

## CEN / TC278

### Road Transport and Telematics

#### Working Group 14

After Theft Systems for Vehicle Recovery

#### Work Item 14.5

#### Long Range Interface/System Requirements

#### Document Reference

WG14.5 LR interface 2004.  
Agrred at WG14 meeting The Hague 29/01/04

#### Distribution

Working Group 14 & CEN TC 278

#### AMENDMENT RECORD

Issue	Amendment Detail	Author	Date
A	Preliminary Draft of Working Paper Distributed to WG14.5 members	Tim Terrebonne	June 2001
B	Draft Working Paper Distributed to WG14.3, WG14.4, WG14.6	"	July 16, 2001
C	Draft Working Paper Distributed to WG14 coordinators meeting	WG14.5	8 Nov, 2001
D	Revised issue following Amsterdam co-ordinators meeting 4/9/2	Ralph Kanter; Tony Scorer	5 Sept. 02
E	Minor changes	Tony Scorer	10 Sept 02
F	Format and Grammatical Changes	co-ordinators	30 July 2003
G	Corrections	Tony Scorer	December 03
H	Corrections	Convenor	January 2004

#### DOCUMENT PRODUCTION SOFTWARE

Software	Version
Word for Windows	Word 2000

Index

Introduction.....	3
1.1 Foreword .....	3
1.2 Scope .....	3
1.3 The Conceptual Architecture Model for ATSVR.....	5
2 References .....	6
2.1 WG14 Documents .....	6
2.2 Normative References.....	6
2.3 Other References .....	6
3 Definitions and Abbreviations .....	7
3.1 After Theft System for Vehicle Recovery .....	7
3.2 Abbreviations.....	7
4 Requirements for Long Range Operations. ....	8
4.1 LR ATSVR Architecture.....	8
4.2 The LR ATSVR Process.....	8
4.3 The LR ATSVR Functions .....	8
4.3.1 LR Detection Function.....	8
4.3.2 LR Location Function .....	9
4.3.3 LR Identification Function.....	9
4.3.4 Remote Degradation Function (optional) .....	10
4.3.5 LR Theft Indication Function .....	11
5 Examples of Long Range Systems.....	12
5.1 Detection by Signalling with Location Function by Communication Network .	12
5.2 Detection by Signalling with Location Function by Homing .....	13
5.3 Detection by Signalling with Location Function by Geographic Positioning ...	14
5.4 Detection by Signalling with Location Function by Communication Network .	15
6 Vehicle Tracking System Parameters.....	16
6.1 Attack Resistance.....	16
6.2 Technical Specification.....	16
6.3 Activation of the ATSVR Process .....	16
6.4 Deactivation of the ATSVR Process.....	16
6.5 Functional Specification .....	16
6.6 Detection .....	17
6.7 Information Protocol .....	17
6.8 Tests.....	17
6.9 Integrity of Response .....	18
6.10 Incorrect Operations .....	18
6.11 Management of False Alarms .....	18
6.12 Quality of Process.....	19
6.13 Quality of Information.....	19
6.14 Quality of Equipment .....	19
6.15 Quality of Manufacturing.....	19
6.16 Quality of Installation .....	19
6.17 Transmitted Power.....	20
6.18 Safety of Vehicle User .....	20
6.19 Safety of Operators of Mobile Equipment.....	20
7 Security Considerations in LR Systems.....	20
7.1 Communications security .....	20
7.2 Stored Data Security .....	20
7.3 Personnel Security .....	21
7.4 Radio Transmissions.....	21
7.5 Data Protection requirements.....	21

## Introduction

### 1.1 Foreword

This document was developed by CEN TC 278 Road Transport & Traffic Telematics Working Group 14 (WG14) on the subject of After Theft Systems for Vehicle Recovery (ATSVR).

WG14 comprised representatives and experts from police, insurance associations (CEA), car manufacturers, transport associations, vehicle rental associations and ATSVR system and product providers. The work was also in cooperation with Europol and the European Police Cooperation Working Group (EPCWG).

The standard was developed to define an architecture within guidelines from CEN TC 278 through which a level of interoperability can be achieved between Systems Operating Centres (SOC) and law enforcement agencies (LEA), both nationally and internationally.

This will provide minimum standards of information and assurance to users as to the functionality of systems, thereby enabling the recovery of vehicles, detection of offenders and a reduction in crime.

This document should be read in conjunction with prENVXXX Reference Architecture and Terminology which provides the preliminary framework for ATSVR concepts.

### 1.2 Scope

This document specifies the characteristics required to operate the Long Range ATSVR Architecture

An ATSVR consists of various equipment elements that communicate and interact through various interfaces in accordance with standard procedures and protocols in order to facilitate the recovery of a stolen vehicle. These processes may involve a human operator.

ATSVR elements include the OBE installed in the vehicles, a range of Detecting Equipment and one or more System Operating Centres. One or more supporting Infrastructure Networks provide the communications to support the ATSVR. The ATSVR location function may also include one or more supporting Position Reference Sources.

The LR systems use an interface that allows the Detection Equipment to operate some ATSVR Functions at distances normally greater than direct line of sight. These LR systems are generally operated with ATSVR Location Functions using long-range communications.

This Standard permits existing proprietary systems to operate using these interface specifications at ATSVR application level.

The main subject areas are:

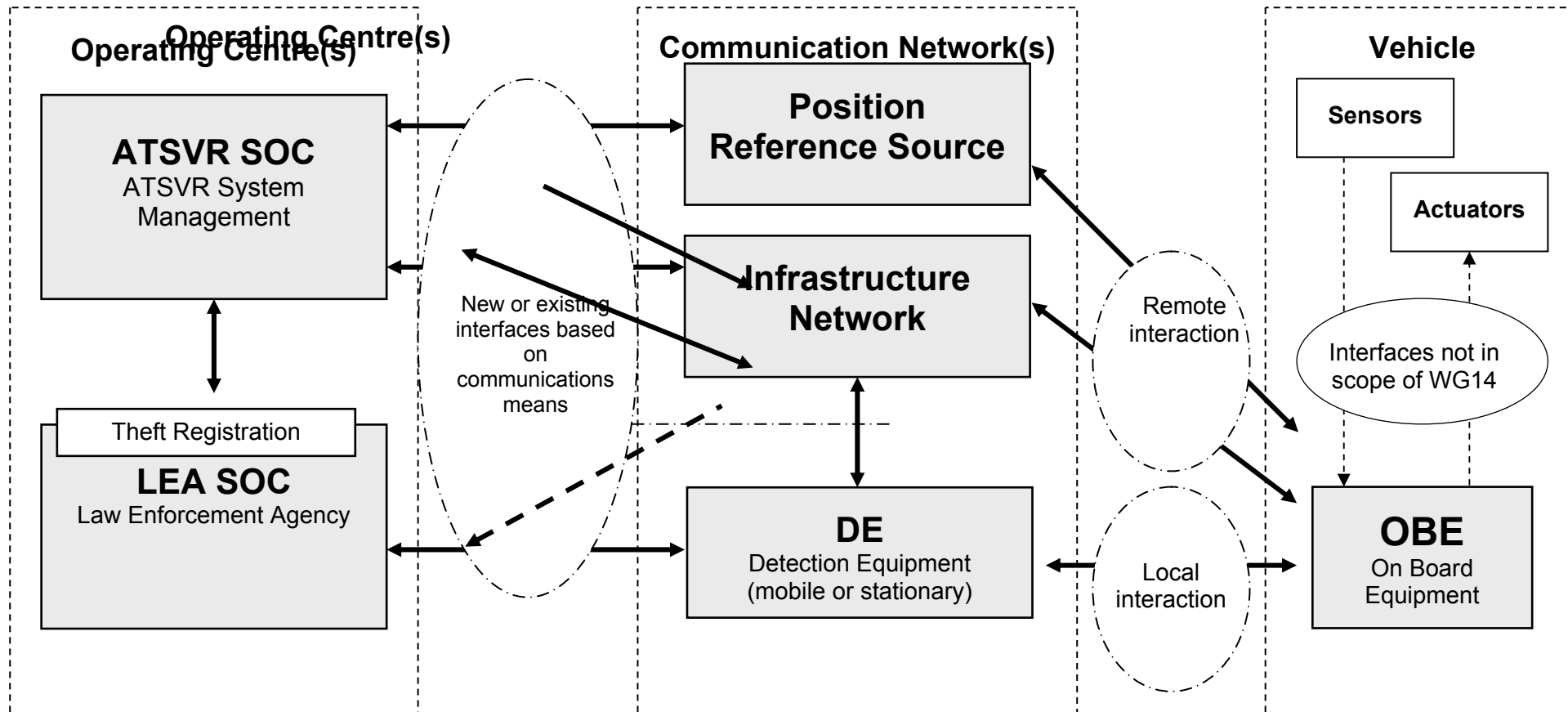
- Definition of classes and categories
- Interoperability and compatibility of systems at;
  - Functional level
  - Information level

Performance level

- Identification of communications supporting infrastructures
- Specification of compatible interfaces for ATSVR applications
- Restriction of specifications to;
  - Application level
  - Operating level
  - User level

The following Diagram is taken from prENV XXXX Reference Architecture & Terminology and is repeated here for ease of reference.

### 1.3 The Conceptual Architecture Model for ATSVR



## 2 References

### 2.1 WG14 Documents

BN9607028 Nov 96	Task Force Report "After Theft Systems for Vehicle Recovery Investigation into Standardisation requirements
14N903E2 Jun 99	14.2 "Summary of Users Requirements"
14N007E Feb 00	WG14 revised work program
14N009E Feb 00	14.6 "Messaging Interface"
14N008U Nov 00	Internal Technical Report WG14.1 "Conceptual Architecture & Terminology "

### 2.2 Normative References

ENV12253	OSI Layer 1 - Physical (Open Systems Interconnections)
ENV12795	OSI Layer 2 - Link
ENV12834	OSI Layer 7 - Applications
ENV13372	Profiles
UTE C 70-201	EMC - Part 1 (transmission)
UTE C 70-202	EMC -Part 2 (immunity)
ETSI (EN 300 220-1/2)	
ETS 300 113	Technical characteristics and test conditions for radio equipment intended for the transmission of data (and speech) and having an antenna connector
EN 300 279	Electromagnetic Compatibility (EMC) standard for Private Land Mobile Radio (PMR) and Ancillary Equipment (speech and/or non-speech)
EU 95/54	Automotive type approval for Suppression of Radio Interference (i.e. EMC) for 4 wheeled vehicles

### 2.3 Other References

VSIB Code of Practice (UK)

### **3 Definitions and Abbreviations**

#### **3.1 After Theft System for Vehicle Recovery**

An After Theft System for Vehicle Recovery (ATSVR) is a system that comprises various elements that communicate and interact through various interfaces in accordance with standard procedures and transmission protocols in order to facilitate the recovery of a Registered Stolen Vehicle.

This Standard does not seek to define the requirements or actions of the various human elements of the ATSVR, but it does aim to identify the interactions and interfaces that exist amongst the equipment and human elements operating within the system.

#### **3.2 Abbreviations**

ATSVR	After Theft Systems for Vehicle Recovery
LEA	Law Enforcement Agency
SOC	System Operating Centre
OBE	On Board Equipment
DE	Detection Equipment
LR	Long Range (Communications Interface)
SR	Short Range (Communications Interface)
ETSI	European Telecommunications Standards Institute

## 4 Requirements for Long Range Operations.

### 4.1 LR ATSVR Architecture

A LR ATSVR consists of various equipment elements that communicate and interact through communication network interfaces in accordance with standard procedures and protocols in order to facilitate the recovery of a stolen vehicle. These processes may involve the human operator.

ATSVR elements include the OBE installed in the vehicles, a range of Detecting Equipment and one or more SOC's. One or more supporting communications network interfaces facilitate the interactions that support the various ATSVR functions. The ATSVR location function may also include one or more supporting Position Reference Sources.

### 4.2 The LR ATSVR Process

The process necessarily begins with the theft of the vehicle. Following theft or suspected theft, the first possible function is to **indicate** that a theft of a vehicle has occurred. Following this, the status of the target vehicle, i.e., whether the target vehicle has been stolen or not, shall be confirmed by the user or by other appropriate personnel and this status shall then be **acknowledged** by a LEA. This then becomes a Registered Stolen Vehicle.

The vehicle should then be **located** by the ATSVR, and if moving, **tracked** or homed onto by the system in order to facilitate LEA or ATSVR service personnel to close range with the target vehicle. By closing range with the target vehicle, they will more easily be able to **recognise** the vehicle. Once recognised, the target vehicle shall be accurately **discriminated as the target vehicle** from other surrounding vehicles.

This process facilitates the selection of the target vehicle for closer examination by LEA or ATSVR personnel in order to confirm the **identity** of the target vehicle as the stolen vehicle. The process of establishing **identity** may require an additional query and response through ATSVR databases.

This process can, under controlled circumstances, be assisted by the degradation of the capabilities of the target vehicle.

### 4.3 The LR ATSVR Functions

There are three basic ATSVR functions of detection, location and identification of a Registered Stolen Vehicle.

#### 4.3.1 LR Detection Function

Automatically or semi-automatically to detect the location of a Registered Stolen Vehicle. This may be done by Signalling or by Consulting.

Detection by Signalling is where the OBE has been activated by a signal from an external source. This activation may come from a mobile or stationary source, which may be local to the vehicle (Short Range) or at a distance from the vehicle (Long Range). Once activated the OBE will transmit a signal that is capable of being picked up by ATSVR Detection

Equipment located locally to the vehicle or at a distance from the vehicle. The transmitted signal may contain other relevant information.

Detection by Consulting is where an external item of Detection Equipment interrogates the OBE and the OBE responds by transmitting data to the DE. The DE then compares the received data with a database of Registered Stolen Vehicles, a data match confirms that a Registered Stolen vehicle is present and further action can take place.

#### 4.3.2 LR Location Function

Once the Registered Stolen vehicle has been detected the location can be established by one of the following functions:

- Location by using direct geographic co-ordinates;
- Location by using indirect geographical co-ordinates or
- Location by using homing techniques.

**Location by direct or indirect geographic co-ordinates** is the process that establishes the general or precise location of the vehicle at a given point in time. This allows entitled persons to carry out their defined tasks.

**Homing** (also known as Tracing or Relative Positioning) is the process that periodically updates the range and direction of the detected vehicle from an intercepting vehicle over a period of time. Thus allowing entitled personnel to approach or intercept the detected vehicle without the necessary use of landmarks or absolute geographic references.

**Tracking** is the process that periodically updates location and other information on the detected vehicle over a period of time and allows entitled personnel to monitor, approach or intercept the detected vehicle.

#### 4.3.3 LR Identification Function

This function allows 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. VIN, registration number, and other data, e.g. theft status, model, colour and if relevant, position.

**Discrimination** is the process that enables entitled personnel unambiguously to differentiate the detected vehicle from other surrounding vehicles.

**Recognition** is the process that enables entitled personnel correctly to select the detected vehicle through visual observation based on knowledge of the vehicle particulars such as make, model, colour and other specific observable features.

**Indirect Identification** results from data coming from a central or remote data bank, whilst Direct Identification is that resulting from data coming from the OBE.

#### 4.3.4 Remote Degradation Function (optional)

This function provides the possibility to degrade remotely the vehicle's performance using either long or short-range transmission techniques. Short-range communication may be preferable as some countries require the vehicle to be in direct line of sight of authorised personnel to trigger this function.

Regulations for these devices will be developed according to the laws in each country. However, this standard seeks to establish main principles as currently requested by the LEA's. These are:

- Use of the system and the resulting engine degradation must not lead to the contravention of vehicle or road transport legislation in the country where it is to be operated. Differences in legislation in different countries must be taken into account.
- The system must not compromise the safety of the vehicle, or any other vehicle. It must only influence the intended vehicle and no other, irrespective of system or system operator (anti-collision protection).
- For safety reasons the device must not switch off the engine or have any influence on the braking, steering or safety of the vehicle. Subject to these requirements a slow degradation of power that the engine can generate is permissible. The degradation time may be as long as 30 to 60 minutes until a steady low power state is reached. This would permit the driver to park the vehicle safely without endangering passing traffic.
- There must be a positive identification of the vehicle and a confirmation that it is actually stolen.
- The systems may only be activated by a person authorised by the LEA or a relevant government department. Some countries may require the vehicle to be in direct line of sight of such an authorised person to trigger this function.
- ATSVR companies will indemnify, in writing, each LEA where it is intended that the system will operate. The indemnity shall cover the LEA, and their officers and servants, against any claim under any course of action made by any person in respect of:
  - (a) personal injury (including death) directly caused as a result of the use of the tracking/ remote engine degradation system,
  - (b) any loss, damage, expense, personal injury (including death), wrongful arrest, prosecution or charge caused by the negligent operation of the system by the SOC, or by any malfunction of the system which results in a vehicle being wrongly identified as stolen.
- The ATSVR operators and SOC's must have international public liability insurance.

This section does not inhibit the use of Prohibit Engine Start function when the vehicle is in Engine Off mode.

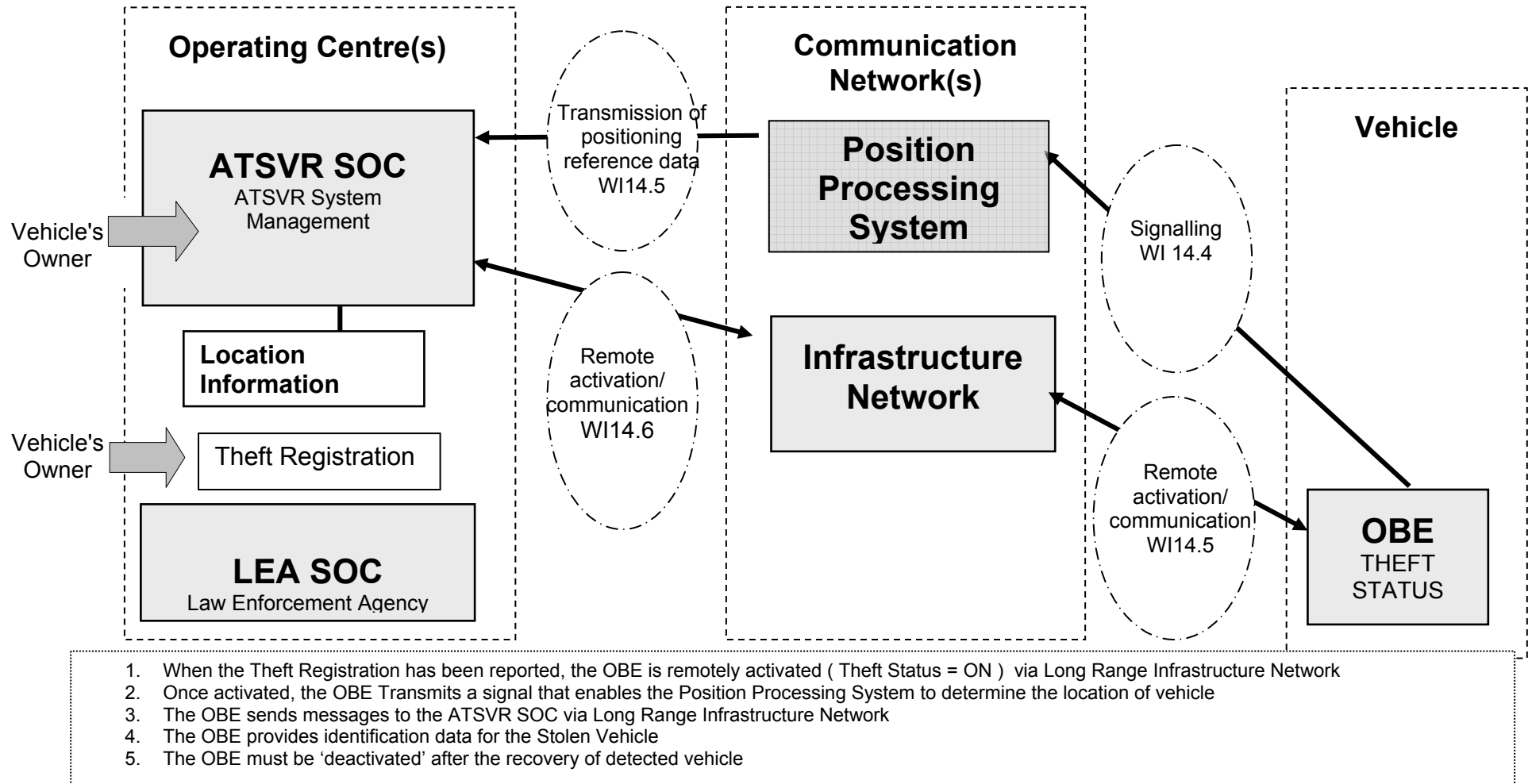
#### **4.3.5 LR Theft Indication Function**

The transmission of a warning or alert from the OBE to an SOC, the indication in a DE, that the transmitting vehicle may have been stolen.

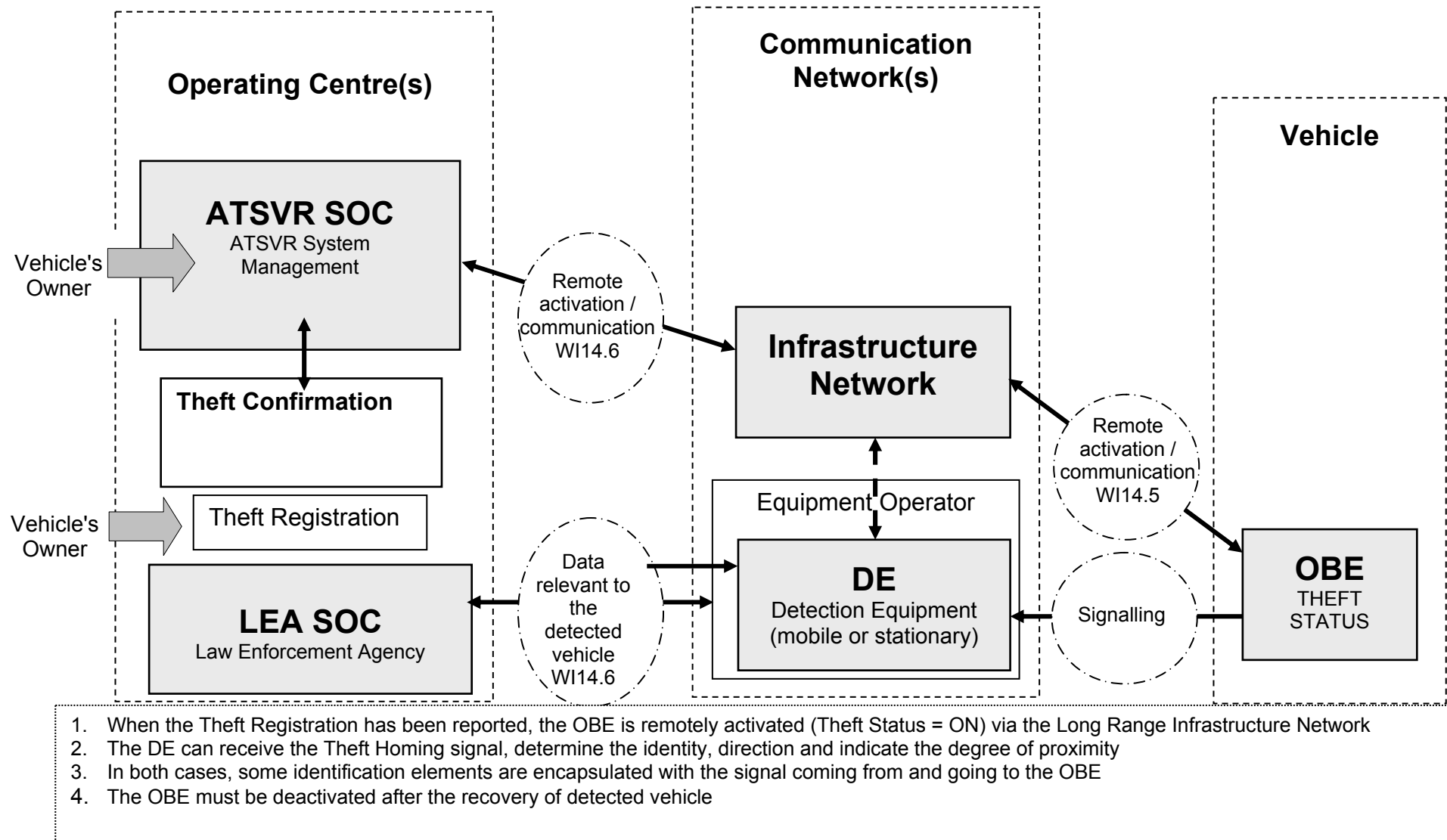
## 5 Examples of Long Range Systems

### 5.1 LR Detection by Signalling with Location Function by Communication Network

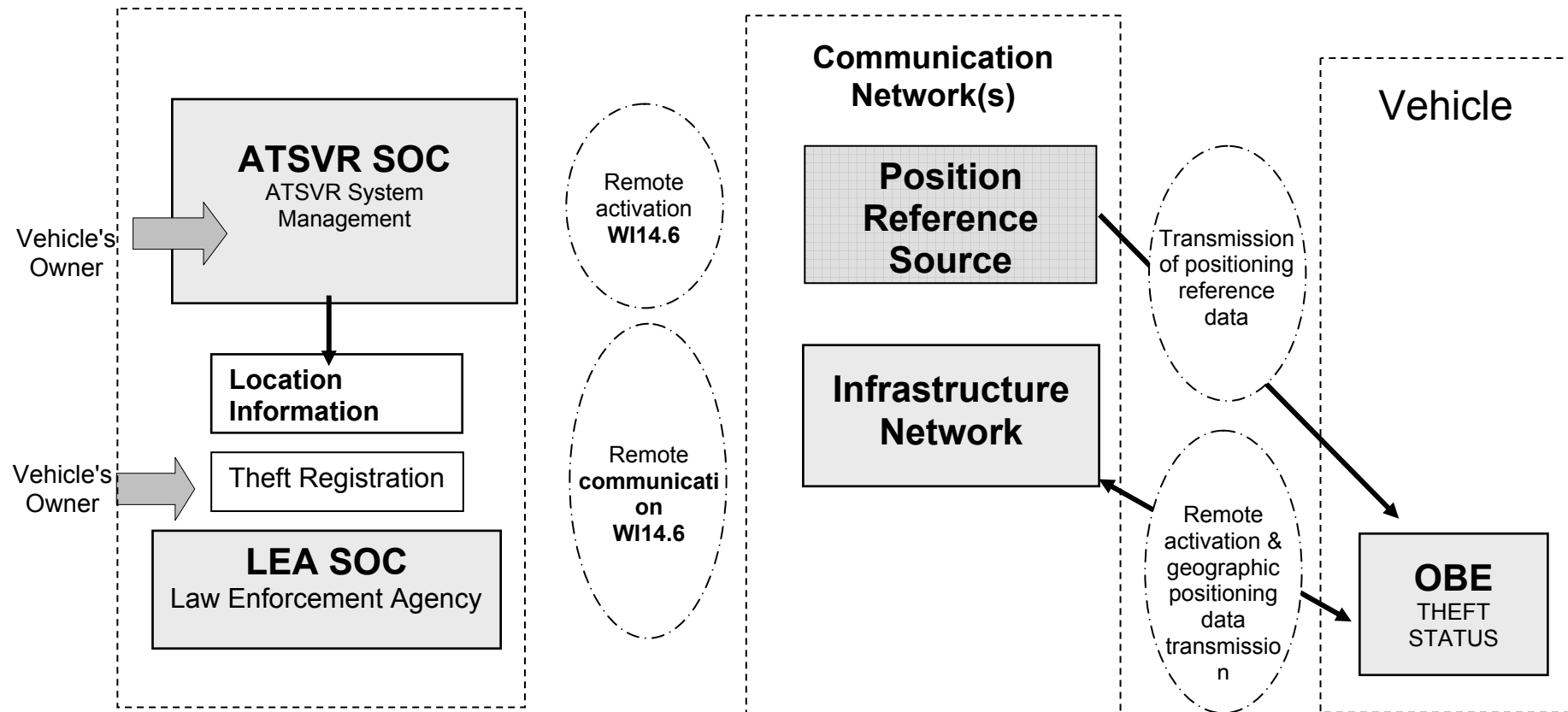
(e.g. Enhanced Observed Time Difference)



## 5.2 LR Detection by Signalling with Location Function by Homing

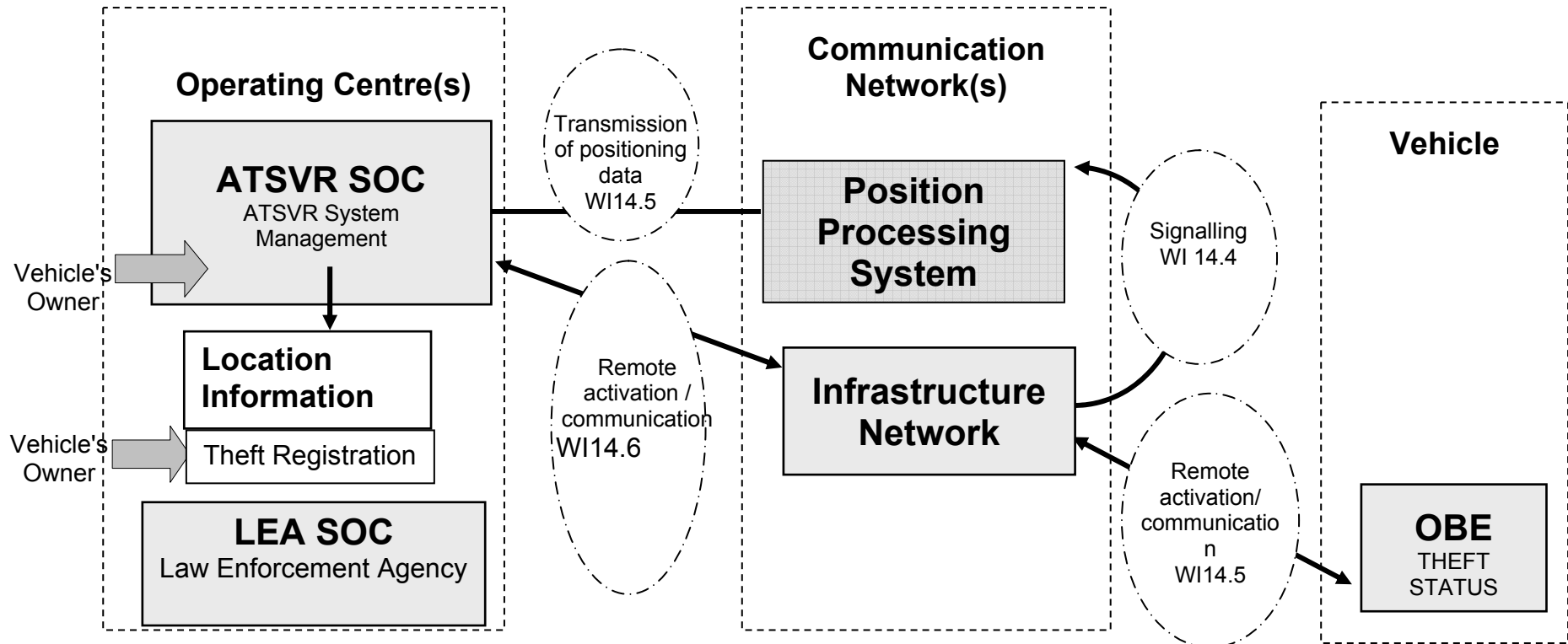


### 5.3 LR Detection by Signalling with Location Function by Geographic Positioning



1. When the Theft Registration has been reported, the OBE is remotely activated (Theft Status = ON) via Long Range Infrastructure Network
2. Once activated, the OBE determines the location of vehicle with the Position Reference data received from Position Reference Source
3. The OBE sends messages to the ATSVR SOC (and possibly LEA SOC) via Long Range Infrastructure Network
4. The OBE provides identification and the Geographic position data for the Stolen Vehicle
5. The OBE must be 'deactivated' after the recovery of detected vehicle

**5.4 LR Detection by Signalling with Location Function by Communication Network**  
(e.g. Spread Spectrum)



1. When the Theft Registration has been reported, the OBE is remotely activated (Theft Status = ON) via Long Range Infrastructure Network
2. Once activated, any signals that the OBE transmits to the Infrastructure Network enables the Position Processing System to determine the location of the vehicle
3. The OBE sends messages to the ATSVR SOC via Long Range Infrastructure Network
4. The OBE provides identification data for the Stolen Vehicle

## **6 Vehicle Tracking System Parameters**

### **6.1 Attack Resistance**

The system including the antenna shall be capable of being covertly installed.

### **6.2 Technical Specification**

The vehicle battery shall normally power the system.

The system shall have its own back up battery

The back up battery (a device that powers up the device in the event that the main vehicle supply is interrupted) shall be capable of maintaining the system for 5 hours in active mode.

The back up battery shall be capable of maintaining the system for at least 48 hours in power saving mode.

The quiescent current drain of the system must be less than 20 milliamps when the OBE is inactive.

### **6.3 Activation of the ATSVR Process**

The ATSVR Process may only be initiated by an SOC for the purpose of ATSVR where that SOC has an agreement with an LEA or another SOC that has such an agreement.

A SOC shall only initiate the ATSVR Process when:

It has been confirmed with a LEA that the vehicle has been stolen.

The standard operational procedures of the SOC have been followed.

A SOC may initiate the ATSVR Process for testing purposes with the prior agreement of the appropriate LEA.

### **6.4 Deactivation of the ATSVR Process**

The ATSVR Process may only be stopped by a duly *authorised* SOC.

A SOC shall only deactivate the ATSVR Process when

Requested by a LEA for valid operational reasons

Following the standard operational procedures of the SOC.

Or

Following successful recovery of the stolen vehicle

### **6.5 Functional Specification**

Where the system is capable of providing its position to the SOC:

The time of the position report must be known.

The system must continue to update its position at regular intervals or as required by the LEA.

The system's operational area shall be clearly identified (for the purposes of clarification this does not refer to radio coverage map but rather

restrictions on operational area due to policy e.g. restriction of operation to an individual country).

## **6.6 Detection**

Any of the following events, among others, shall initiate the ATSVR process:

Report of theft by Authorised User

Request by the LEA (such request must be from a suitably senior officer and relate to a real and present danger to an individual or the public)

Detection of unauthorised movement:

Change in inclination

Irregular movement

Change of location.

## **6.7 Information Protocol**

The SOC must maintain a database containing the following information for each vehicle:

Make

Model

Vehicle Registration Mark (if applicable)

VIN (if applicable)

Colour

Status (i.e. whether active or not)

For all communications between SOC and the LEA all ATSVR's must provide the SOC with a unique code to avoid operational errors.

The minimum detection accuracy shall be twenty five metres RMS.

## **6.8 Tests**

The Test House shall assess the system for compliance with the mandatory requirements of this standard.

The Test House shall validate the claims made by the ATSVR Supplier.

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

The Test House shall determine the location of the test in accordance with the Supplier's installation and operational instructions. Any special test requirements imposed by the Supplier must be in accordance with normal installations.

During each test all system components shall function normally and not cause any unintended alarms or change of status.

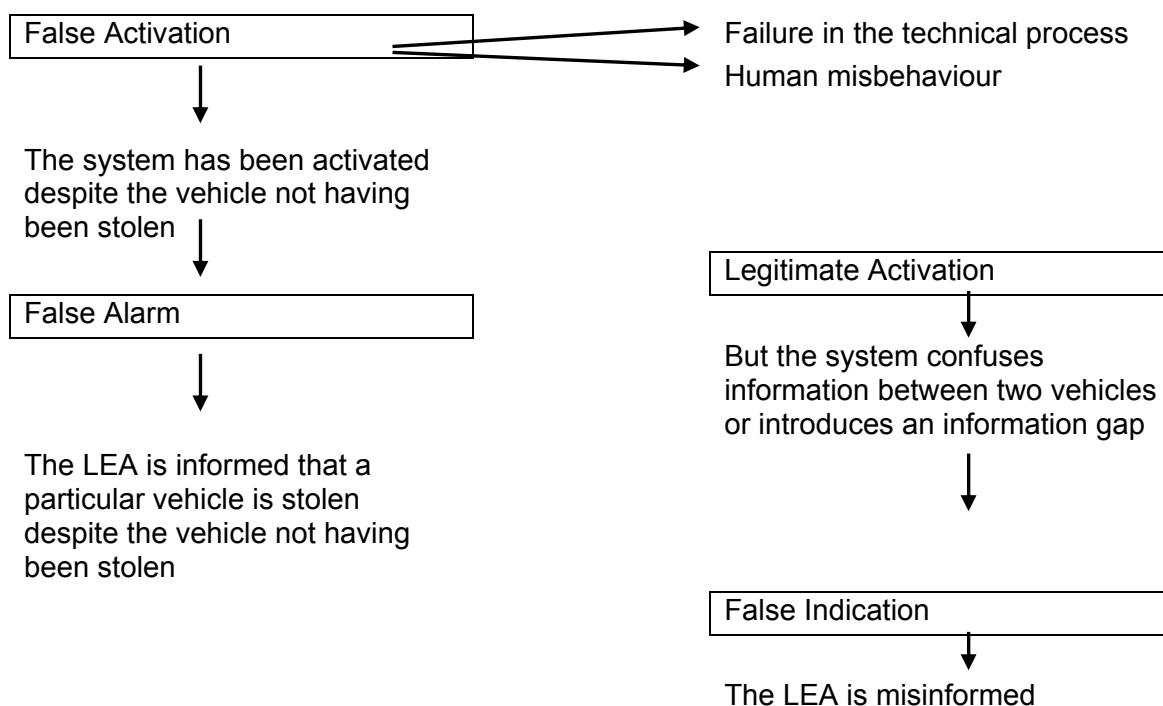
On completion of the test, the system shall continue to function according to the Supplier's specifications.

## 6.9 Integrity of Response

Any request for data, whether manual or automatic, should always yield the same results when applied to the same database.

## 6.10 Incorrect Operations

There are a number of ways in which an ATSVR system can be misused or operated incorrectly. An incorrect operation is one that misleads the ATSVR users. The different types of incorrect operation may be defined according to the result of such incorrect operation as follows:



## 6.11 Management of False Alarms

Management of False Alarms needs to be agreed with the LEA. A False Alarm is an alarm generated by the ATSVR system where the LEA has been informed by the SOC or the OBE, despite no vehicle theft having taken place. An Activation of an ATSVR system that results from use of the vehicle by an Authorized Vehicle Operator that is reported to an LEA by the SOC or OBE is a False Alarm.

A SOC must be capable of providing management information on their system to the LEA to enable an assessment of false alarms in each jurisdiction. The information supplied must give details of the number of calls received by the SOC and passed to the LEA, the number of recoveries and the number of false alarms.

If the level of false alarms is unacceptable this may result in a written warning or sanctions from the LEA to the SOC involved. If the level of false alarms remains unacceptable, LEA response to the SOC requests to track vehicles can be withdrawn.

To restore response the LEA may require the SOC to demonstrate that the level of false activations are not excessive and show what corrective action has been taken. False alarms include malicious calls and matters

that are not a LEA responsibility; for example debt recovery may not be a LEA responsibility.

It will, therefore, be the responsibility of the SOC to limit false alarms by the early identification of problem installations and subsequent withdrawal of service for such installations.

The LEA must be satisfied with the system(s) being operated by the SOC. Each system must be capable of being demonstrated to the LEA. The LEA will determine the acceptable false alarm rate.

### **6.12 Quality of Process**

Any SOC providing services for use in monitoring or activation of vehicle tracking or location systems should be able to demonstrate internal and external procedures that are designed to comply with ISO 9000 quality assurance requirements or equivalent.

Any SOC used in monitoring or recovery of 'high risk loads' belonging to third parties should also comply with the security requirements of the national security standard. This standard should define SOC response times.

Compliance with this document does not in itself confer immunity from any legal obligations applicable to organisations involved in running and / or supporting ATSVR services

### **6.13 Quality of Information**

The SOC supplying information to the LEA must:

Operate 24 hours a day, 365 days a year

Provide full backup monitoring systems in the event of down time

Have a full disaster recovery plan to enable continuation of service within a few hours.

Adhere to the data protection and Human Rights laws of the country in whose jurisdiction they operate.

### **6.14 Quality of Equipment**

The ATSVR equipment manufacturer must be certified ISO 9002 or equivalent.

### **6.15 Quality of Manufacturing**

All ATSVR equipment must be of good build quality and be fit for purpose. It must have a CE mark; and appropriate EMC certification (EU 95/54) and any necessary radio Type Approval certificate. It shall, where appropriate, comply with the relevant criteria of EU 95/56.

### **6.16 Quality of Installation**

Installation of the equipment must be of a high standard, in accordance with best common practice as laid down in the VSIB Code of Practice or other similar national standards.

Detailed installation instructions provided by the supplier shall be such that when followed by a competent installer, the safety and reliability of the vehicle is not affected.

### **6.17 Transmitted Power**

The transmitted power levels of radio equipment will be such as not to cause harm or damage and be compliant with the specified legal limits for the device.

### **6.18 Safety of Vehicle User**

The ATSVR equipment must not adversely affect the design function and safe operation of any vehicle, even in the case of malfunction, especially with regard to steering, brakes and electromagnetic compatibility. Antennas must be installed in a safe manner and in accordance with manufacturer's instructions if available.

### **6.19 Safety of Operators of Mobile Equipment**

Mobile ATSVR equipment must be suitable for vehicle use and when installed in LEA vehicles must meet the defined standards of safe equipment operation for that LEA.

Any ATSVR display must be suitable for operation in all normal lighting conditions and must refresh at an appropriate frequency to enable the operator to effectively use the equipment.

## **7 Security Considerations in LR Systems**

### **7.1 Communications security**

It is accepted that all radio devices can be jammed. However, the ATSVR equipment operators should have a method of detecting that jamming is occurring and if possible identifying the source of the jamming signal. If this jamming results from un-authorized transmissions then the ATSVR operator can report that to the relevant territories radio licensing body. This is outside the scope of this standard.

The Transmission protocols must include error correction and require the use of codes to provide a secure and high integrity means of communication with the vehicle and ATSVR devices.

It is accepted that given knowledge, the relevant technology and time, a criminal attack on any device may be successful. To provide realistic protection the device shall be installed in a covert manner such that normally non user-removable items of trim or other fabric of the vehicle must be removed in order to gain access to the system, including the antenna.

### **7.2 Stored Data Security**

Whilst this is not within the scope of this Standard, any operator of ATSVR equipment must ensure that data held is backed up, is not corrupted nor interfered with by any third party. They must take steps to ensure the integrity and protection of any sensitive data held or processed.

### **7.3 Personnel Security**

Whilst this is not within the scope of this Standard, any ATSVR system operators shall undertake such measures and investigations as permitted in the host country to ensure that staff employed on ATSVR systems does not have criminal convictions that would pose a risk to security.

ATSVR Service Personnel employed by an ATSVR SOC dealing with vehicles carrying High Value Goods must be security cleared to the recognised national standard.

### **7.4 Radio Transmissions**

Radio transmitting devices must operate on a legal frequency and be licensed for the country of operation. The equipment supplier should take steps to ensure that equipment does not transmit outside of the licensed area whilst in control of the authorised user. This may require equipment to be able to select a different frequency for each country of operation. Manufacturers of such a device must ensure a list of the countries for which the device is licensed accompanies the sale of the device.

### **7.5 Data Protection requirements**

All data shall be accurate, up to date and secure, particularly where this relates to personal data. All data shall be kept in accordance with the data protection principles set out by the Council of Europe Convention on 28<sup>th</sup> January 1981 and shall take account of Recommendation R(87)15 of the Committee of Ministers of the Council of Europe 17<sup>th</sup> September 1987 concerning the use of personal data in the police sector.

There are some variations in requirements across EU member states. Therefore the data shall also be kept in accordance with the national data protection requirements of the country where the data originates and the country where the data is stored

End of document