

## CEN / TC278

### Road Transport and Telematics

#### Working Group 14

After Theft Systems for Vehicle Recovery

#### Work Item 14.4

#### Short Range Interface/System Requirements

**Document Reference** 14.4 300703

#### Distribution

#### AMENDMENT RECORD

Issue	Amendment Detail	Author	Date
2.9	Format and Grammatical Corrections	WG14 co-ordinators	July 2003
3	Corrections	Tony Scorer	December 2003
4	Corrections wg14 plenary 29/01/2004	Convenor	29 January 2004.

#### DOCUMENT PRODUCTION SOFTWARE

Software	Version
Word for Windows	Word 2000

## Contents

CEN / TC278	1
ROAD TRANSPORT AND TELEMATICS	1
WORKING GROUP 14	1
1 INTRODUCTION	4
1.1 Foreword	4
1.2 Scope	4
1.3 The Conceptual Architecture Model For ATSVR	6
2 REFERENCES	7
2.1 WG14 Documents	7
2.2 Normative References	7
3 DEFINITIONS AND ABBREVIATIONS	10
3.1 Definitions	10
3.1.1 SR Detection by Consulting Function	10
3.1.2 SR Detection by Signalling Function	10
3.1.3 Identification Function	10
3.1.4 Remote Activation Function	10
3.1.5 Remote Degradation Function (Optional)	10
3.2 Abbreviations	11
4 REQUIREMENTS FOR SHORT RANGE OPERATIONS	14
4.1 Detailed Architecture Diagrams and Sequence Diagrams	14
4.1.1 Detection by CONSULTING Architecture Diagram	14
4.1.2 Detection by CONSULTING Sequence Diagram	15
4.1.3 Detection by SIGNALLING Architecture Diagram	16
4.1.4 Detection by SIGNALLING Sequence Diagram	17
4.2 Identification Function	19
4.3 Remote Activation Function	19
4.3.1 Sequence for Remote Activation after Notification of the DE	19
4.4 Remote Deactivation Function	20
4.5 Remote Degradation Function (optional)	21
4.6 Theft Indication Function	22
4.7 Interaction Sequences	22
5 OPERATING CHARACTERISTICS	23
5.1 Characteristics common to both OBE and DE	23
5.1.1 Definition of Telegrams between OBE and DE	23
5.1.2 Collision Capability	23
5.1.3 Collision Capability in Case of Simultaneous Polling and Signalling	23
5.1.4 Frequency, Bandwidth, Modulation, other RF characteristics	24

5.1.5	Usage of DSRC physical layer	25
5.2	Characteristics of On Board Equipment "OBE" in a vehicle	25
5.2.1	RF transmit power	25
5.2.2	Battery	25
5.2.3	DC Current Consumption	25
5.2.4	Data Storage	26
5.2.5	Connection to a Vehicle Internal Bus System	26
5.3	Characteristics of the Detection Equipment "DE"	26
5.3.1	The Communications Networks Interface	26
5.3.2	DE Internal Data Bank	27
5.3.3	Types of Detection Equipment	27
5.4	Communication distance between OBE and DE	27
5.4.1	Case 1: Stationary detection equipment and OBE	27
5.4.2	Case 2: Mobile detection equipment and OBE	28
5.4.3	Case 3: Hand held detection equipment and OBE	28
5.5	Vehicle speed limits	28
5.6	Minimum Number of Activations without Vehicle Battery	28
5.7	Discrimination among Vehicles	28
6	DATA ELEMENTS	30
6.1	Introduction	30
6.1.1	Encryption	30
6.1.2	Reference list	30
6.1.3	Signalling	31
6.2	Data Elements Common to both OBE and DE	31
6.2.1	General Data Elements	31
6.2.2	Specific Data Elements	31
7	REGULATORY ISSUES	33
7.1	Communication Devices	33
7.2	Radio Transmissions	33
7.3	Public Liability Insurance	33
	APPENDIX A	44

# 1 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 done in co-operation with Europol and the European Police Cooperation Working Group (EPCWG).

This 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 Standard will focus on Short Range (SR) Interface / Systems Requirements. SR systems use an interface that allows the Detection Equipment to operate some ATSVR functions in the direct line of sight of vehicles.

SR systems enable LEAs, in a particular country, to permit LEA personnel, using these devices, to perform actions on vehicles that are within their immediate vicinity. Such actions can include identification of vehicle data or remotely influencing the vehicle.

prENV XXX (14.3) describes the structure, bit arrangements, number representation, coding of message elements that are typically transmitted as data. There is no requirement to make the messages as short or as effective as possible. Emphasis has been laid on making them as clear and unambiguous as possible.

For Short Range Communications, where there is very little time available for the transfer of data between passing vehicles and the detection equipment, only a subset of the message elements described in prENV XXX (14.3) can be transmitted. Therefore, in these cases, the data lengths are reduced to an absolute minimum.

Data elements such as times, dates, or geographical coordinates need not be transmitted because the 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 the 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.

Some Short Range devices may be triggered by or may use long range communications and vice versa.

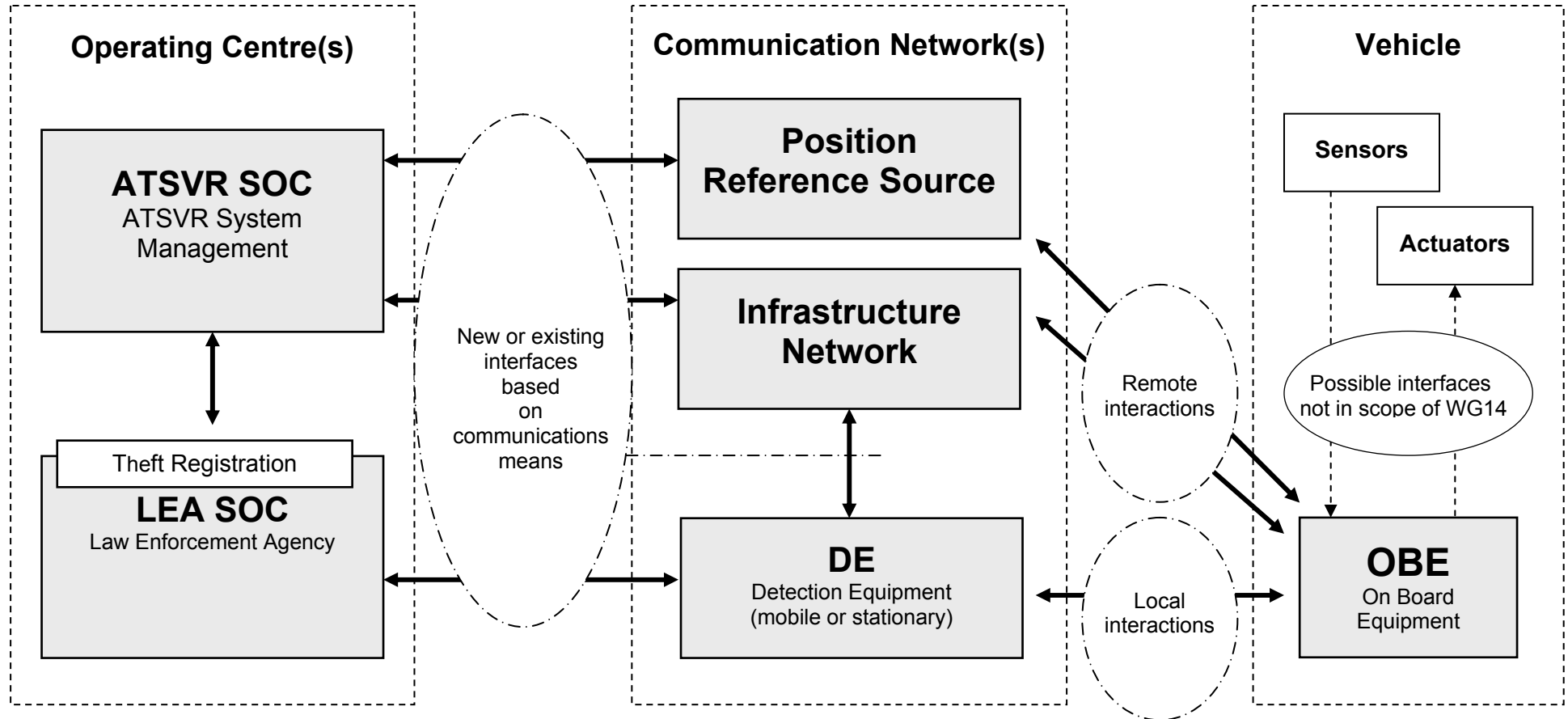
Some Interfaces are not within the scope of this Standard. These comprise interfaces to or from sensors, actuators and human operators; from position reference sources e.g. GPS, LEAs internal interfaces etc.

Detection Equipment "knows" the time, in case of stationary equipment "knows" its coordinates etc. The Detection Equipment may concatenate these data elements to the data coming from the vehicle when sending a complete data set to ATSVR System Operating Centres or to LEA as described in other parts of this Standard.

Wherever possible the same specifications, data structures, contents, and definitions have been used throughout this Standard. 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.

The following diagram is taken from prENV XXX Reference Architecture & Terminology and is repeated for ease of reference.

### 1.3 The Conceptual Architecture Model For ATSVR



## 2 References

### 2.1 WG14 Documents

BN96070 Nov 96	Task Force Report. After Theft Systems for Vehicle Recovery. Investigation into Standardisation Requirements
14N007E Feb 00	WG14 revised work program
14N008U Nov 00	Internal Technical Report WG14.1 Conceptual Architecture & Terminology
14N903E2 Jun 99	WG 14.2 Summary of Users Requirements
WI 00278095	WG 14.3 Common Status Message Elements
WI 00278097	WG 14.5 Long Range Interface / System Requirements
WI00278146	WG 14.6 Messaging Interface
prENV XXX	WG 14.7 Reference Architecture & Terminology
prENV XXX	WG 14.8 Testing Procedures

### 2.2 Normative References

#### Dedicated Short Range Communication (CEN)

ENV12253 equivalent to prENV 278/9/#62	OSI Layer 1 - Physical (Open Systems Interconnections) Physical Layer using 5.8 GHz
ENV12795	OSI Layer 2 – Data Link Layer – Medium access and logical link control
ENV12834	OSI Layer 7 - Applications
ENV13372	DSRC Profiles for RTT applications
ENV12896	Publics Transport reference data model

#### Automatic Vehicle Identification / Automatic Equipment Identification

ENV ISO 14 814	Reference Architectures: Conceptual Architecture, Logical Architecture, Functional Architecture, Control Architecture
ENV ISO 14 815	(Ratified) Automatic vehicle and equipment identification system specification
ENV ISO 14 816	(Ratified) Automatic vehicle and equipment identification numbering and data Structures
ENV (CEN) 12 314.1	(became EN in January 2001) Automatic vehicle and equipment identification reference architectures and terminology

## Short Range Interface/System Requirements

ENV (CEN) 12 314.3	Automatic vehicle and equipment identification system parameters
ENV (CEN) 12 314.4	Automatic vehicle and equipment identification interfaces
ENV (CEN) 12 315.1	TTI Messages via dedicated short range communication Part. 1 - Data specification Downlink (Roadside to vehicle)
ENV (CEN) 12 315.2	Part. 2 – Data specification Uplink (vehicle to roadside)
pr ENV ISO 14 813.1	TICS. Reference model architecture (s) for the TICS sector – Part. 1 TICS fundamental services

pr ENV ISO 14 813.2	TICS – Reference model architecture (s) for the TICS sector – Part. 2 CORE TICS reference architecture
pr ENV ISO 14 813.4	TICS – Reference model architecture (s) for the TICS sector – Part. 4 Reference model TUTORIAL
pr ENV ISO 14 813.5	TICS – Reference architecture (s) for the TICS sector – Part. 5 Requirements for architecture description in TICS standards
pr ENV 14 813.6	TICS – Reference model architecture (s) for the TICS sector – Part. 6 Data presentation in ASN.1
ENV ISO 14906	Application interface definition for dedicated short-range communication EFC application interface (Electronic fee collection)

## Miscellaneous Standards

ANSI x 3.92	DES algorithm (Data Encryption Standard)
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 4 wheeled vehicles
ISO 8730	Int'l standard for message authentication
ISO 8731	Int'l standard for message authentication
ISO 8824	Information processing systems – OSI – Specification of Abstract Syntax Notation One (ASN.1) 1993
ISO 8825	Information processing systems – OSI – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) 1993

Remark: Pr ENV ISO: means that the provisional standard exists both in the European (CEN) and International (ISO) form.

## 3 Definitions and Abbreviations

### 3.1 Definitions

#### 3.1.1 SR Detection by Consulting Function

The Detection Equipment may electronically "consult" passing vehicles. This function is called "Short Range Detection by Consulting".

#### 3.1.2 SR Detection by Signalling Function

The stolen vehicle may "signal" itself, after a wireless activation process, that it is stolen. This function is called "Short Range Detection by Signalling".

#### 3.1.3 Identification Function

Short range communication functions may also be used for unequivocal identification of vehicles, if the vehicle's country of origin or of registration permits this.

#### 3.1.4 Remote Activation Function

An electronic "switch" may be set in the vehicle that can be used to communicate to the vehicle that it is stolen, setting some bits of information in the vehicle. This function is called Remote Activation Function.

#### 3.1.5 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.
- Vehicle tracking and locator 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 SOC must have public liability insurance.

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

### 3.2 Abbreviations

Terminology	Meaning	Explanation or typical use.
A1	an EU project	
AEI	automatic equipment identification	The process of identifying equipment or entities that uses the surface transportation infrastructures by means of OBE's combined with the unambiguous data structure defined in these standards.
AIS	automatic identification system	A system for achieving accurate and unambiguous identification of a data bearing OBE, tag, transponder or a natural / prescribed feature, the data or feature being interrogated by means of a system appropriate source.
ASN.1	abstract syntax notation one	(specified in ISO 8824 and 8825)
AttrID	attribute identifier	
Auth	authenticator	
AVI / AEI	automatic vehicle identification / automatic equipment identification	AVI: the process of identifying vehicles using OBE combined with the unambiguous data structure defined in these standards
carrier signal		an electromagnetic signal that can be modulated to carry lower frequency encoded information across an air interface
CBC	cipher block chaining	
[CEN_AI]	ISO ENV 14906: EFC application interface	
[CEN_L1]	ENV 12253 DSRC layer1 Physical layer using 5.8 GHz	

## Short Range Interface/System Requirements

[CEN_L2]	ENV 12795 DSRC layer2 Data link layer	
[CEN_L7]	ENV 12834 DSRC layer7 Application layer	
[CEN_Pr]	ENV 13372 DSRC Profiles	
constructed identifier		an identification which requires a construct of (more than one) primitive identifiers, as defined in ASN.1 (ISO 8824 / 8825)
Data element structure		a framework comprising a number of data elements in a prescribed form
DE	Detection Equipment	
DES	data encryption standard	(see also TDES)
DSRC	dedicated short range communication	
EDI	electronic data interchange	the passing of a data message, or series of data messages, between computers and/or between different software systems. Within this context, an EDI message is normally compatible with the form specified in ISO 9897 (CEDEX)
EDT	electronic data transfer	the passing of data sets comprising an entire message from one computer to another or from one software system to another
EFC	electronic fee collection	
EID	element ID	
EN	European standard.	(French: Norme Européenne, German: Europäische Norm)
ENV	European pre-standard	
ETSI	European Telecommunications Standards Institute	
GSS	global specs for short range communication	
[GSS 2.0]	global specs for short range communication	(an industry specification)
inductive signals		electromagnetic signals – usually below 30 MHz – characterized by the use of magnetic component of the signals to couple an OBE to a reader by electromagnetic induction
interrogator		a device that performs the functions of a reader (see reader), but in addition has the ability to send new data to the OBE via an air interface
ISO	International Standardisation Organisation	
LEA	Law Enforcement Agency	
LR	Long Range	Long Range Communications Interface
MAC	message authentication code	
manufacturer ID		identifier of manufacturer (2 bytes)
OBE	on board equipment.	A device on board or attached to the vehicle/equipment; (within this context: equipment to perform the functionality of AVI/AEI)

## Short Range Interface/System Requirements

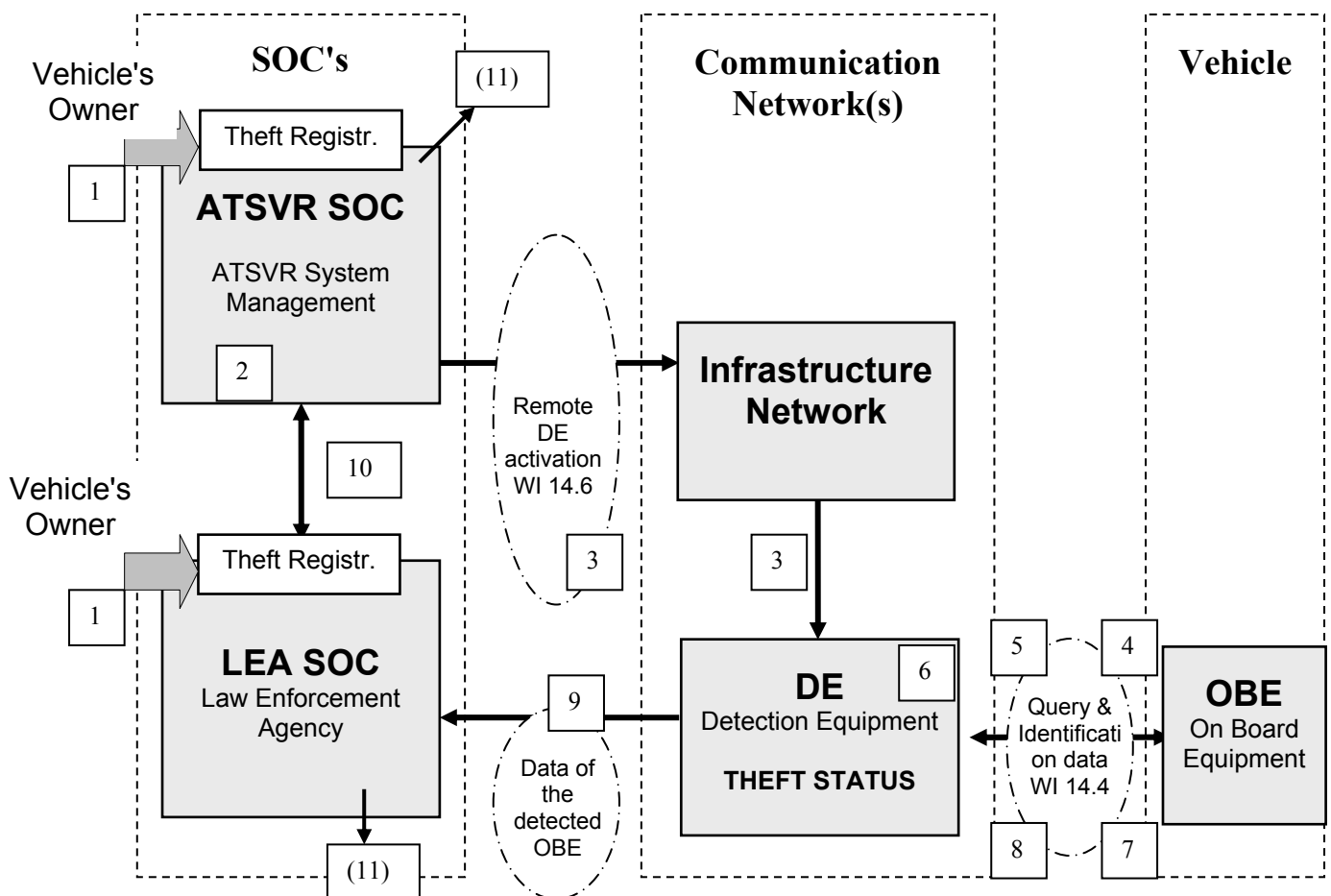
OBESstatus		status of on board equipment (1 byte)
operator		the commercial operator of an AVI/AEI/RTTT system that uses OBEs for the purposes defined in the pre-standard [ENV 12314-1]
primitive identifier		identification as a stand alone identity that does not require any qualifiers such as expiration date etc. All construct identifiers shall be built from (more than one) primitive identifier
RndOBE		random number from OBE to RSE 1
RndRSE		random number from RSE to OBE 1
RSE	road side equipment	
RTI	road traffic informatics	
RTTT	road transport and traffic telematics	
session time		4 bytes; coding defined in ISO 14906
SOC	System Operating Centre	
SR	Short Range	Short Range Communications Interface
Telegram	Short message data	Used at 4.5 and 5.1
TICS	transport information and control systems	
TDES	triple DES	algorithm is performed three times with 2 different keys
VST	vehicle service table	information block from the OBE to the RSE during initialization

## 4 Requirements for Short Range Operations

### 4.1 Detailed Architecture Diagrams and Sequence Diagrams

#### 4.1.1 Detection by CONSULTING Architecture Diagram

This diagram depicts *one* subset of the general ATSVR Architectural Diagram: it shows the Operating Centres, the Communication Network including the Detection Equipment, and the Vehicle with its On Board Equipment together with data streams and interfaces.



1. The theft must be reported to the LEA SOC either directly or via an ATSVR SOC.
2. The "reported to be stolen" information is kept by the ATSVR SOC.
3. When the Theft Registration has been reported, the DE is activated (updating the DE data file) either at LEA SOC before being deployed, or remotely via Long Range Infrastructure Network.
4. The DE interrogates the OBEs of vehicles in the vicinity ("consulting").
5. The OBE sends back the VIN and theft status of the vehicle (or encrypted information from which VIN and status can be derived).
6. The DE compares data from the OBE with its data file of stolen vehicles and determines whether the vehicle is reported as stolen.
7. If the DE has determined that the vehicle status information has to be updated, it sends the appropriate data to the OBE.
8. The acknowledgement of updating the OBE is reported back and logged in the DE.
9. The data of the detected vehicle together with status information is sent to the LEA SOC.
10. This information is subsequently routed to the ATSVR SOC to update their files.
11. (Beyond this *technical* standard: The LEA SOC or the ATSVR SOC may take appropriate action.)

### 4.1.2 Detection by CONSULTING Sequence Diagram

Detection by Consulting is where an external item of Detection Equipment (DE) interrogates the On Board Equipment (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.

This function is especially needed for controls at the roadside, border, harbour, entrance to a parking area etc. using stationary DEs. In order to support these activities a fast identification-function is provided. The transmission of the VIN and the theft-status is sufficient. All other relevant data about the vehicle can be obtained from the vehicles database. . The theft-status in the OBE can be changed via the remote activation function.

Transmission of the theft-status from the OBE to the DE is important because it permits the use of simple DE without connections to a central database of stolen vehicles. It is a pre-requisite that the theft-status of the OBE is up-to-date.

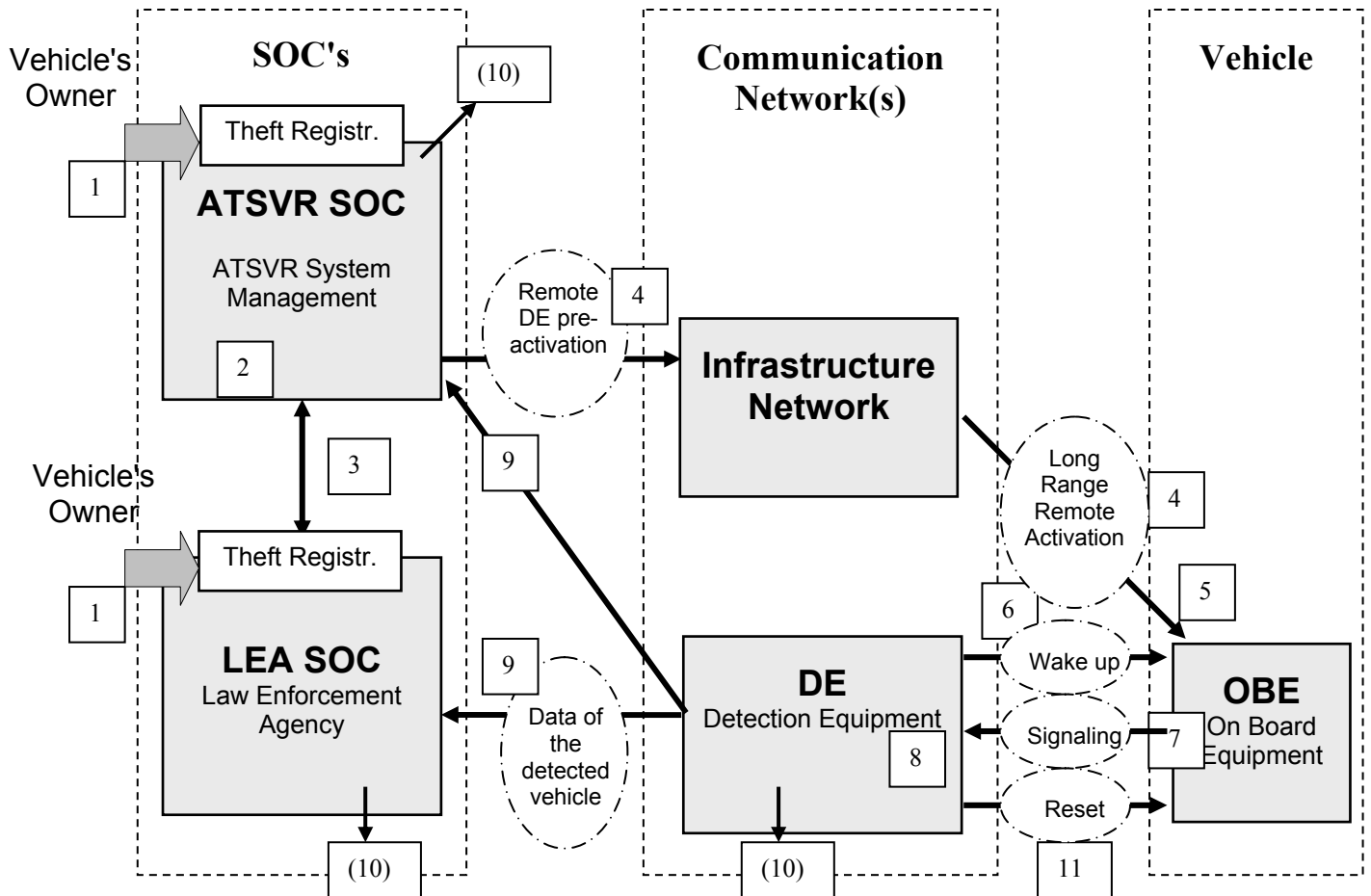
The following table shows the main events for the case of detection by consulting:

Adapted Sequence Diagram for Short Range Detection by Consulting

Main events	LEA SOC	ATSVR SOC	Network	DE	OBE
Theft Registration  Acknowledgement of the vehicle status  Remote DE <b>Notification</b> by updating its file  <b>Polling of Identification elements</b> by the DE from every surrounding OBE  <b>Detection</b> of a vehicle: 1. showing "Theft Status" = ON ; <b>OR</b> , 2. if the vehicle is registered as stolen in the DE's database  Report of detection ; updating of the theft-status in the OBE	<pre> sequenceDiagram     participant LEA as LEA SOC     participant ATSVR as ATSVR SOC     participant Network     participant DE     participant OBE      LEA-&gt;&gt;ATSVR:      ATSVR-&gt;&gt;DE:      DE-&gt;&gt;OBE:      OBE-&gt;&gt;DE:      DE-&gt;&gt;OBE:      OBE-&gt;&gt;LEA:      </pre>				

### 4.1.3 Detection by SIGNALLING Architecture Diagram

This diagram depicts another subset of the general ATSVR Architectural Diagram: it shows the System Operating Centre(s) [SOC's], the Communication Network(s) including the Detection Equipment, and the Vehicle together with data streams and interfaces.



1. The theft must be reported to the LEA SOC either directly or via an ATSVR SOC..
2. The "reported to be stolen" information is kept by the ATSVR SOC.
3. The LEA and some specially authorized organizations have access to this file.
4. The ATSVR SOC pre-activates the OBE through the Long Range Infrastructure Network.
5. The theft status information is set in the OBE.
6. When in the vicinity of a DE sending interrogation telegrams, the OBE interprets them as wake up and:
7. The OBE starts signalling, i.e. sends periodically the VIN and theft status of the vehicle.
8. Hand held DEs display data from the OBE and mark them as coming from a stolen vehicle.
9. Stationary DEs send the appropriate data to the LEA SOC and/or ATSVR SOC.
- 10.(Beyond this *technical* standard: The LEA SOC, the ATSVR SOC or an agent reading the DE information may take appropriate action.)
- 11.In case of recovery of the vehicle, the OBE's stolen status information must be reset. Some special equipment using the same DE-OBE-interface may be used. Excellent cryptography must be used to perform this action.

The various parts of the system work as follows:

- 1 The theft must be reported to the LEA SOC either directly or via an ATSVR SOC.
- 2 This information is put into a file of stolen vehicles, e.g. the stolen vehicle register for the country where the theft takes place and the European central file. The file contains information such as VIN, make of vehicle, type, colour, license plate number, country of registration of the vehicle, date and time of theft, ..
- 3 The LEA and some specially authorised organisations have access to these files.
- 4 The fact that the vehicle is reported to be stolen may be sent to the vehicle in different ways e.g.:
  - by a point-to-point connection via GSM using e.g. short messages
  - by Short Range Communication when the vehicle passes a DE
  - by broadcast messages via FM radio using the traffic message channel.
- 5 This information will "pre-activate" the OBE: The "theft status bit" is set, but transmissions to the outside world ("signalling") do not yet occur. See points -6 and -7.
- 6 When the "pre-activated" vehicle passes a stationary or mobile detection unit, which is sending some short range communication telegrams and if the OBE receives this information, then it interprets it as a wake up command for its signalling device.
- 7 The OBE energises transmissions of the following vehicle information:
  - "stolen" information
  - make, type and colour
  - licence plate number
  - country of registration
  - VIN.
- 8 Hand held readers and/or stationary detection equipment may receive these signals, issue an alarm and may display the signals in an appropriate form in the machine to human interface specifications.
- 9 Stationary equipment reports the detection of the stolen vehicle to the LEA SOC and/or to the ATSVR SOC. Hand held equipment may also have provisions for sending this information to the LEA and/or ATSVR SOC.
- 10 After reception, the agent using the DE or the ATSVR SOCs or the LEA may perform appropriate actions to recover the vehicle. These actions are not within the scope of this technical standard and given only for clarification.
- 11 After recovery of the vehicle, the OBE must be reset to the not-stolen state. If for this purpose the same equipment and interface between the DE and the OBE is used, then very good cryptographic features have to be employed to prevent misuse of this critical resetting.

#### **4.1.4 Detection by SIGNALLING Sequence Diagram**

A prerequisite to Detection by Signalling is that the OBE has been activated by an external source. This activation may come from a mobile or stationary source, which may be local to the vehicle (short-range) or, in most cases, at a distance from the vehicle (transmission via long-range).

Once activated, the OBE will transmit signals (hence "signalling") that are capable of being received by ATSVR Detection Equipment located local to, or at a distance from, the vehicle. The transmitted signal may contain other relevant information.

This table shows the sequence of events for detection by signalling.

Main events	LEA SOC	ATSVR SOC	Network	DE	OBE
Theft Registration					
Acknowledgement of the vehicle status					
Remote OBE Activation "Theft Status" = on					
<b>Detection of the vehicle signalling " Theft Status = on "</b>					
Report of detection					

(Note: in this table the activation of the OBE theft-status is done by *long-range communications*. The beginning of transmitting the signalling telegrams may be dependent upon prior reception of a short range request from a DE in the vicinity of the vehicle. The *short-range activation* is described in Appendix A)

Discrimination is a very important aspect of detecting a stolen vehicle by signalling in situations where the vehicle is surrounded by several other cars. The officer should be able to determine rapidly which of the vehicles is signalling. This should be done through visual observation based on knowledge of the vehicle particulars such as make, model, colour and license-plate.

When operating in the Signalling Mode, the OBE shall not interfere with the operation of Detection by Consulting equipment.

### 4.2 Identification Function

The identification 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, theft status, model, colour.

This function is typically required where an authorised person has to identify a possibly stolen vehicle by using a hand-held scanner.

This table shows the main event for this case:

Sequence for Short Range Identification

Main events	LEA SOC	ATSVR SOC	Network	DE	OBE
Reading of <b>Identification</b> data stored in OBE				• ←	•

### 4.3 Remote Activation Function

This function is part of Detection by Signalling and by Detection by Consulting. The Activation Function switches the OBE Theft Status = ON.

Detection by signalling will only be effective if the theft-status in the OBE is set (OBE Theft Status = ON). Reading the theft-status is essential when the DE has no database of Registered Stolen Vehicles.

It is the Remote Activation Function that switches the theft-status in the OBE to ON . In short-range a vehicle must be detected via the function 'Detection By Consulting': the DE compares the received data with data in its own database of Registered Stolen Vehicles and determines whether the vehicle is reported to be stolen.

The Remote Activation Function is used when the theft-status is 'OFF' (not-stolen) in the OBE and is 'ON' in the DE database. Therefore, the DE must send a signal to the OBE in order to change the OBE-theft-status to 'ON'.

#### 4.3.1 Sequence for Remote Activation after Notification of the DE

Main events	LEA SOC	ATSVR SOC	Network	DE	OBE
Theft Registration	•				
Acknowledgement of the vehicle status	•	•			
Remote DE <b>Notification</b> by updating its file		•	•	•	
Requesting the OBE Theft Status				•	•
Read / Compare OBE Theft Status with data file in the DE				•	•
Remote <b>Short Range Activation</b> of OBE " Theft Status = on "				•	•

### 4.4 Remote Deactivation Function

After recovery of a stolen vehicle, the OBE Theft Status must be reset (OBE Theft Status 'OFF' ). This function is complementary to the "Activation" function as it electronically "converts" a stolen vehicle into a "not stolen" vehicle. The design of this function must be cryptographically well secured. Only specifically accredited personnel may perform this function.

One possibility of securing the necessary data transfers is to use a very secure algorithm (AES) together with a vehicle specific key that is only stored in the vehicle's immobiliser and in the manufacturer's data bank. AES has the feature of selectable key length and runs on small micro-controllers. Also, there is no license fee and the algorithm is freely available.

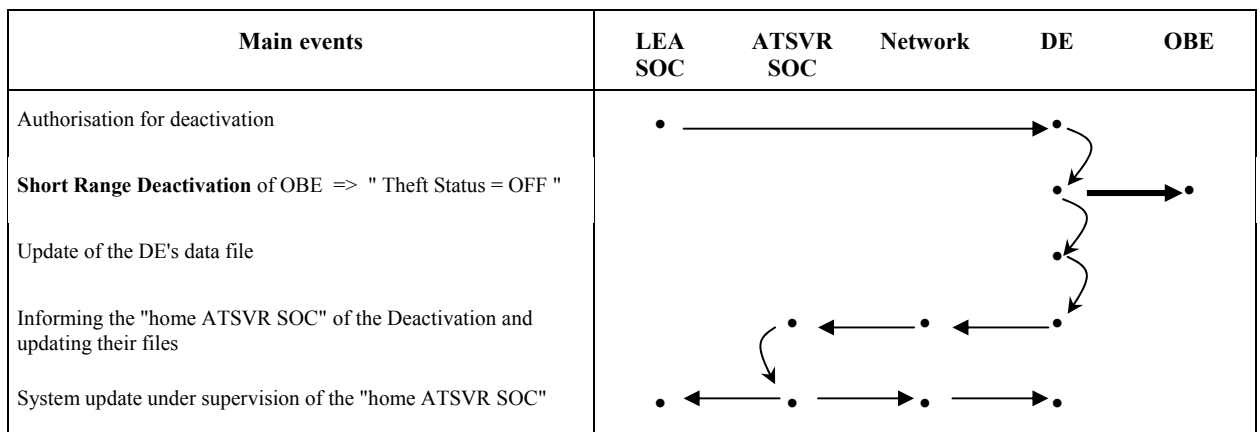
Preferably, the deactivation function should employ short range protocols, and the personnel should be in line of sight of the vehicle.

Before deactivation, the vehicle has to be unequivocally identified (see Identification Function). A bi-directional communication with the LEA SOC results in authorisation for the Deactivation Function. In the Sequence Diagram below it is assumed that the LEA SOC has received the vehicle's unique cryptographic key from a data bank (usually the vehicle manufacturer's data bank).

Besides resetting the OBE Status, the databanks throughout the whole communications net still holding the information "Theft status = ON" have to be reset, accordingly. This should for security reasons be done under supervision of the "home" ATSVR SOC responsible for this vehicle (or a LEA SOC). Again, very secure cryptography must be used to distribute the information "Theft Status = OFF" throughout the communications net.

Hence, the following **Sequence Diagram** applies:

#### Sequence Diagram for Deactivation



#### 4.5 Remote Degradation Function (optional)

This function provides the possibility to remotely degrade the vehicle performance. Although it is feasible that this function uses long range or short-range transmission techniques, short-range communication may be preferable, since some countries require the vehicle to be in direct line of sight of authorised personnel to trigger this function.

Typically, the degrading telegram will be sent from a DE to the OBE. Prerequisites are positive identification of the vehicle and confirmation that it is actually stolen (functions "Detection by Consulting" and "Detection by Signalling").

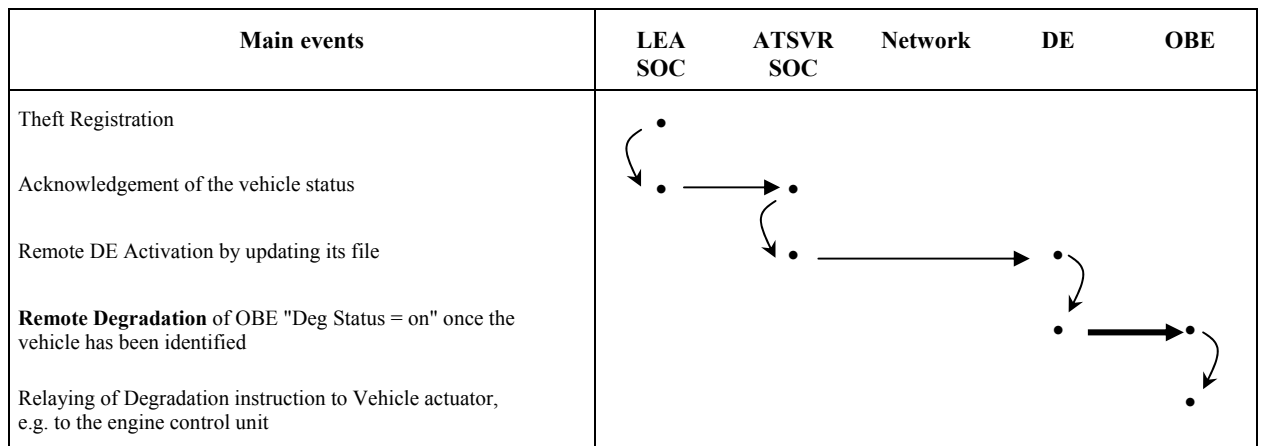
Resolution of safety and legal issues remains paramount for this type of technology. Due to different laws in each country this standard seeks only to establish main principles that should be addressed before such systems are offered to relevant government departments and the LEA.

- a) Unambiguous addressing. The operation of the device must only affect the intended vehicle and no other, irrespective of system or system operator.
- b) Safety. The system shall not compromise safety and in particular shall not stop the engine whilst the vehicle is moving or remove power to vital functions of the vehicle such as brakes, steering or lights.
- c) Legislation. The operation of the system shall not cause a vehicle traffic offence to take place, such as stopping the vehicle in a dangerous place or causing danger to other road users. The list of offences will be different for each country.
- d) Liability. There must be sufficient insurance cover against incidents and claims arising from use of such devices. In particular, where the system is operated by an LEA on behalf of the owner or the SOC, there must be indemnity for the LEA against claims arising from use of the device.
- e) Integrity. The device may only be operated by authorised personnel and should be safeguarded against malicious use on a vehicle that has not been declared stolen.

For safety reasons, the engine must never be switched off. However, 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 enables the vehicle to be parked, minimising danger to passing traffic.

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

### Sequence for Short Range Remote Degradation



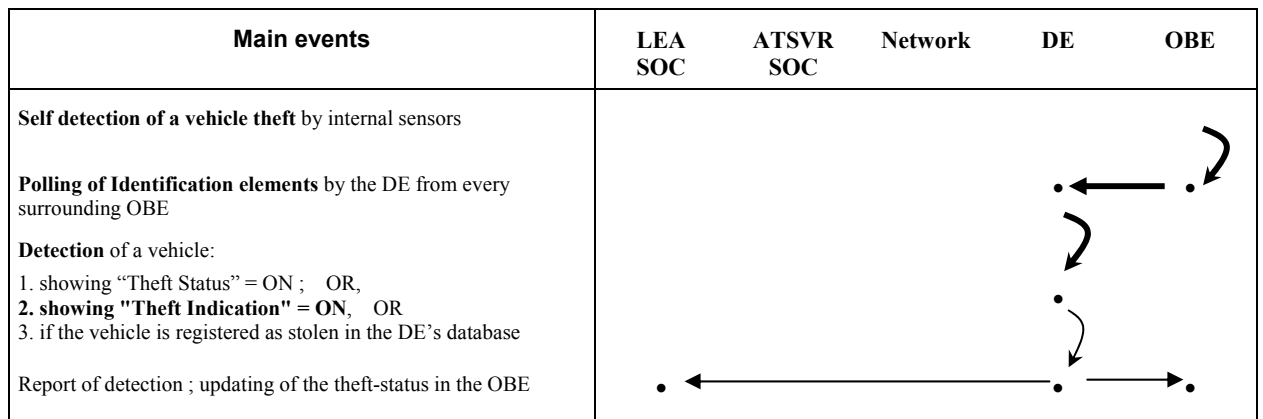
#### 4.6 Theft Indication Function

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

One of the Status bits in the OBE may indicate that the vehicle itself has detected a possible theft state.

As an example, an extract of the Adapted Sequence Diagram for Short Range Detection by Consulting shows the detail incorporating the Theft Indication Function:

Adapted Sequence Diagram for Short Range Detection by Consulting, incorporating the Theft Indication Function



#### 4.7 Interaction Sequences

The After Theft Services take many forms. Each one initiates a set of sequences, which contain sets of operations organised in iterative queries and transactions between each architecture block. The detailed sequencing of various potential short range systems are outlined in **Appendix A**. They are depicted in State Chart Diagrams and Activity Diagrams as appropriate.

## 5 OPERATING CHARACTERISTICS

In this section, the operating characteristics of the Detection Equipment (DE) and the On Board Equipment (OBE) are described.

### 5.1 Characteristics common to both OBE and DE

#### 5.1.1 Definition of Telegrams between OBE and DE

For ATSVR purposes under the conditions of short range communication, at least three different types of telegrams have to be defined:

- Telegram for *fast vehicle identification* together with read/write of the OBE status.
- Telegram for *specific and exhaustive vehicle enquiry*.
- Telegram for *command transmission* to the OBE.

The **fast identification telegram** is specifically designed for very fast data transfer facilitating the identification of all vehicles within range of the reader ("multi lane problem", e.g. on highways).

The **specific and exhaustive identification telegram** will unequivocally identify a vehicle. This results in the transmission of vehicle type, colour, last known license number, etc. In this case the downlink portion of the telegram addresses a specific vehicle, hence no multi lane problem exists.

The **command telegram** is used to execute commands in the OBE; initiated by the DE. This type is used for the Remote Activation and Deactivation Functions and the Remote Degradation Function.

#### 5.1.2 Collision Capability

The short range protocol between OBE and DE must allow for the successful exchange of data even if more than one OBE is within the range of a DE. This can be done using e.g. an Aloha protocol. This protocol is not within the scope of this paper; however, it has to be standardised to guarantee data interchange.

Typically the protocol works as follows:

At the beginning of the data interchange, an individual time slot is assigned to the different OBEs within the range of a DE. (This can be assigned by the DE or can be self-assigned by the participating OBEs using a random process, comparable to casting dice.) Only thereafter the "real" communication begins.

#### 5.1.3 Collision Capability in Case of Simultaneous Polling and Signalling

During "Detection by Signalling", the OBEs which send out signalling telegrams will usually ignore other transmissions. If a signalling vehicle drives into the transmission range of a DE, the signalling telegrams may corrupt the ongoing polling data transfers and vice versa. This would only apply if the same frequency bands are used.

When operating in the Signalling Mode, the OBE shall not interfere with the operation of Detection by Consulting equipment.

Examples of applicable design functions are:

- **Duty cycle:** If the duty cycle (i.e. the ON/OFF time ratio) of the signalling OBE is sufficiently small (say, 1 ...3 %), these collisions will only rarely occur and can be regarded as negligible. Also, polling telegrams detect data corruptions and repeat corrupted telegrams.
- **Muting/Delaying:** When a signalling OBE detects ongoing telegrams immediately before its next signalling time slot, it mutes or delays its transmission.
- **Adapting:** When a signalling OBE detects ongoing telegrams immediately before its next signalling time, it "behaves" like an OBE participating in a Consulting Sequence (cf. section 6.2.1), that means, it fulfils the Consulting Protocol, but declares in its preamble that it is not responding to a Polling Sequence but that it is signalling. This is of course the most intelligent, desirable way of solving the problem. Should this Adapting Procedure be standardised, the DEs must also provide for recognition of the respective Signalling Protocols.

#### 5.1.4 Frequency, Bandwidth, Modulation, other RF characteristics

Frequency, modulation and other RF (radio frequency) characteristics are not within the scope of this standard. However, both DE and OBE equipment must fulfil some fundamental requirements.

- The *frequency* or frequencies used for the purpose of ATSVR systems shall be legally usable in all EU countries. If the system is not usable in all countries then the countries in which it can be used must be clearly stated to the consumer and any relevant LEA. Considering the required bandwidth (see below), a very high carrier frequency must be used. The following frequencies are feasible: (868 MHz), 2.45 or 5.8 GHz.
- The required *bandwidth* can be roughly estimated from the following assumed minimum requirements:

Parameters	Symbol	Speed 80 km/h	Speed 200 km/h	Dim.
		Value	Value	
<b>Number of vehicles within the elliptic transmission lobe</b> of the DE with a length of 50 m: 2 * 3 lanes highway; at speed = 80 km/h: highest density traffic; vehicles have 1 sec intervals at speed = 200 km/h: highest density traffic; vehicles have 2 sec intervals	<b>m</b>	12	3	-
Estimated number of transmitted bytes in the fast identification telegram: Random number, ID for encryption, VIN, OBE status, 2 * authentication bytes, update of OBE status, ...	<b>B</b>	128	128	bytes
Estimated bit-factor for realisation of a collision protocol (Aloha or similar)	<b>f</b>	4	4	-
Number of repetitions to enhance data transmission security	<b>r</b>	2	2	-

## Short Range Interface/System Requirements

Number of bits to be transferred for all vehicles in the transmission lobe <sup>1)</sup>	<b>n</b>	122880	30720	bit
Time for a vehicle to travel thru the transmission lobe	<b>Δ t</b>	2.25	0.9	sec
Minimum required bit rate <sup>2)</sup>	<b>BR</b>	54600	34100	bit / sec
Minimum required bandwidth <sup>3)</sup>	<b>BW</b>	<b>164</b>	<b>102</b>	<b>kHz</b>
<b>Result: minimum required BW</b>	<b>BW</b>	<b>200</b>		<b>kHz</b>

<sup>1)</sup> Number of bits (n) to be transferred for all vehicles in the transmission lobe, with 1 byte = 10 bit because of start and stop bits:

$$n = m * B * 10 \text{ bit/byte} * f * r$$

<sup>2)</sup> Minimum required bit rate (BR) for all vehicles within the transmission lobe =

$$BR = n / \Delta t$$

<sup>3)</sup> Minimum required high frequency bandwidth =

$$BW = 3 * BR \quad (\text{Shannon-Theorem})$$

This sample estimation shows that the required bandwidth is in the range of 200 kHz or higher.

### 5.1.5 Usage of DSRC physical layer

The feasibility to use the same characteristics as specified for DSRC (dedicated short range communication) has to be clarified.

## 5.2 Characteristics of On Board Equipment "OBE" in a vehicle

### 5.2.1 RF transmit power

The CEPT/ERC Recommendation 70/03 must be fulfilled.

### 5.2.2 Battery

The OBE must be capable of working without being continuously connected to the vehicle battery. A back-up battery (e.g. primary cell or an own accumulator) may be used at the manufacturer's discretion. The back up battery may be recharged when the ignition is switched on.

### 5.2.3 DC Current Consumption

The DC current consumption is dependent on the mode of operation:

- **Active mode:** When the ignition is ON, the power consumption is not critical.
- **Sleeping mode:** When the ignition is off (e.g. parked vehicle), and if the DE electronics are in a sleeping mode, it is desirable that the current consumption be < 1 mA. Alternatively, if the OBE has a primary cell for back up, the life time of this primary cell must be more than 5 years under normal operating conditions.
- **Wake up mode:** When the vehicle is standing with ignition off and the OBE has been woken up by an appropriate wake up signal, the necessary current

may be drawn from the vehicle's battery. Should the cable be disconnected, the OBE must be capable of working from the internal battery for at least five days.

#### **5.2.4 Data Storage**

The OBE contains different types of data storage: permanent data storage (e.g. for the VIN) and over-writeable data storage (e.g. OBE status).

##### **5.2.4.1 Permanent Storage Space**

The storage space for permanent data (e.g. for the VIN, manufacturer and type of vehicle, cryptographic keys) is written into the appropriate storage space of the OBE and can thereafter never be erased (this type is called WORM = Write Once Read Many Times). This is an important security measure as an attacker must be unable to change this data.

(If no special WORM hardware is used, an appropriate operating system may implement this feature together with conventional flash or EEPROM hardware located on the micro-controller chip).

##### **5.2.4.2 Over-writeable Storage Space**

The over-writeable storage space contains important data like OBE status, last known license plate number, colour, country of origin, registration date, ... This storage space for over-writeable data must be non-volatile, i.e., it must not lose its contents when the power is switched off.

Since most of this data is security relevant, extreme care must be taken that an attacker is unable to read and modify the data. This can be realised, if readout and overwriting of this data are under the control of the operating system.

For accessing this data, appropriate authorisation techniques must be used: this may include encryption [only data encrypted with the correct algorithm and key are usable], use of MACs [message authentication codes: only data being authenticated correctly will be accepted].

#### **5.2.5 Connection to a Vehicle Internal Bus System**

The connection to a vehicle internal bus could greatly enhance the performance of an OBE, with regard to security, attack reporting and remote degradation. This is beyond the scope of this Standard.

### **5.3 Characteristics of the Detection Equipment "DE"**

The DE has two interfaces: the connection to the Communications Networks and the short range radio interface to OBEs.

#### **5.3.1 The Communications Networks Interface**

Where Long Range Communications systems are used as part of a Short Range system, the following should be borne in mind.

- The security of the communications network cannot be made dependent upon the communications network being a "private" network. With thousands of

DEs connected to the communications network there are unavoidable weaknesses where the network can be tapped and compromised.

- Only effective encryption methods can guarantee secure data transmissions and storage.
- The communications network does not need to be fast. If a theft occurs, it may be over one hour before a report is made which then has to be confirmed. The data will then have to be transmitted to the DEs. Therefore, response times in the range of, say, 10 minutes are acceptable.

### **5.3.2 DE Internal Data Bank**

During Short Range Communications between a DE and OBEs, which usually last less than 1 second, there is no possibility for the DE to build up a communication chain with an ATSVR SOC or a LEA SOC in order to find out whether the vehicle just passing by is reported to be stolen or not. Consequently, it is imperative that a DE contains a list (data bank) of vehicles that are reported to be stolen.

Where local regulation requires it, techniques such as "Hashing Functions" may be used for information storage and use.

(See further explanations under the topic "Security Considerations; Encryption".)

### **5.3.3 Types of Detection Equipment**

- **Stationary DEs with Data Bank:**

Updating of new information should take place as soon as the information is available, latest after 1 hour, because in the first hours after a theft has taken place, the recovery is most easily attained.

- **Mobile DEs with Data Bank:**

Mobile DEs with data bank should also be updated as soon as the information is available, however if unavoidable, at the latest after 24 hours. Such devices can easily be updated when the personnel carrying it is able to connect it to the appropriate communications point.

- **Hand Held DEs without Data Bank:**

Hand held DEs without data bank cannot be updated; they are only able to display the information coming from the vehicle(s) they are just examining, e.g. VIN (the legislation of some countries may forbid this), stolen status, make and type of vehicle.

## **5.4 Communication distance between OBE and DE**

### **5.4.1 Case 1: Stationary detection equipment and OBE**

The short range communication distance between stationary DE and an OBE shall be up to 100 m in unobstructed line of sight for the maximum specified vehicle speed.

#### 5.4.2 Case 2: Mobile detection equipment and OBE

The short range communication distance between a mobile DE (e.g. on board a LEA vehicle) and an OBE shall be up to 100 m in unobstructed line of sight for the maximum specified vehicle speed if optimised vehicle antennas are used (usually antennas being fixed in the LEA or ATSVR vehicle).

#### 5.4.3 Case 3: Hand held detection equipment and OBE

If hand held detection equipment is used to interrogate a vehicle whose engine is ON, then the short range communication distance between this DE and an OBE shall be up to 30 m in unobstructed line of sight for the maximum specified vehicle speed .

If however when some hand held detection equipment is used to interrogate a vehicle whose engine is cut off then the short range communication distance between this DE and the OBE shall be up to 5 m in unobstructed line of sight. Usually, the OBE will be in a sleeping mode that results in a very low power consumption. When woken up, the sensitivity of the RF components of the OBE will be increased, the transmitter is powered up, and the communication will (over a short period of time) be equal to the power up mode of the first paragraph of this section (30 m).

#### 5.5 Vehicle speed limits

The maximum specified vehicle speed for this kind of short range communication is 250 km/h. That means, the short range communication must work between 0 km/h and 250 km/h.

#### 5.6 Minimum Number of Activations without Vehicle Battery

The minimum number of activations which the OBE must be able to perform without backup from the vehicle battery is 5,000.

Note: This number can be achieved with simple NiCd accumulators or with standard alkaline batteries. (Assumptions: wake up duration  $\leq 10$  sec., medium current consumption during these 10 seconds  $\leq 100$  mA, battery capacity  $\geq 1.500$  mA h.)

#### 5.7 Discrimination among Vehicles

Discrimination is the process that enables authorised personnel unambiguously to differentiate the detected vehicle from other surrounding vehicles. It may take place when the handheld detection equipment is set to this mode.

Physically, it is very similar to short range *detection*; however, in the transmission telegram header this mode tells the OBE that it shall respond in the "discrimination mode". The handheld DE addresses the specific OBE which it has detected as being stolen (either by comparison in its data bank or by reading only the OBE status = "stolen" or both.)

In that case, the vehicle responds by sending its VIN, together with identifying parameters like make and type of the vehicle, the (original) colour of the vehicle, date of fabrication, special equipment (sliding roof, fog lights,...) etc.

The transmission process can take some time (e. g. 1 second), as there is no data contention problem, because the vehicle is addressed individually, and simple long ASCII strings may be used. Even the headers of the data fields may be transmitted.

**As an example:**

**Vehicle VIN:** WDB2101231A123456

**Manufacturer:** Mercedes Benz

**Model/Type:** W 210

**vehicle Colour:** black metallic

**Other descriptive information:** Colour of upholstery dark blue

**Date of Manufacture:** 02. February 1999

**Vehicle Engine size:** 2.0 Litre

**Vehicle Engine Number:** 1234567890

**Country of registration:** D (Deutschland)

**Licence / number plate:** B - XY 1234"

The headers of each item (e.g. VIN, Make, ...) may alternatively be transmitted as numbers, e.g.

**"01:** WDB2101231A123456

**02:** Mercedes Benz

**03:** W 210...etc."

and the DE converts these defined items into the set language that is used by the authorised personnel.

Also, the problem of identifying e.g. plant can be solved in this way. In this transmission application, any long fully transparent data string may be transmitted.

The exact description of the data fields is described in 14.3, "Common status Message Elements".

## 6 DATA ELEMENTS

### 6.1 Introduction

For the purpose of Short Range Communication, only the data elements that reside in the OBE and in the DE and those which are transferred between them are specified in this section.

The data structures in this section show the inner representation ("reference structure") of data and their identifiers. If encryption is used (e.g. when transferring the information through the internet), these structures are, of course, no longer visible and appear only after decryption, when they are safely stored in the appropriate storage media. They give a hint to the necessary storage space e.g. of the data banks or data lists. In Europe, there are about 2 million vehicles on the stolen vehicle database. This figure together with the required data lengths plus organising space result in the approximate required data storage space.

The legislation of some countries does not allow the "external" storage of certain sensitive data (like VINs of stolen vehicles). There are at least three methods of solving this problem:

#### 6.1.1 Encryption

If the sensitive data like VINs ("plain text") is encrypted resulting in unintelligible "cipher text", and if only this encrypted data is used both for external storage and for data transfers over every single wire or radio interface, the attacker may well read the encrypted data but be unable to interpret it.

The encryption process only allows the deciphering of the data if the algorithm and the appropriate key is used.

#### 6.1.2 Reference list

In a similar approach, instead of encryption, only a reference list is transferred to and stored in the DEs. For this case, the vehicles (licensed in the countries not allowing external data storage) have to know their reference number in addition to their VIN. When interrogated, those vehicles transmit their reference number, the data bank in the DE compares it with the stored reference number list and can by comparison find out whether the vehicle is reported to be stolen or not.

Even the algorithm in a (e. g. hand held) reader only compares the reference numbers and the result of the search is only a

- "yes, vehicle is reported to be stolen" or a
- "no, vehicle is not reported to be stolen".

The data bank has no means of finding out the VIN. At discretion of the country of origin, additional identifying parameters may be added to the reference number list like make and type of vehicle, colour and the like to facilitate discrimination.

### 6.1.3 Signalling

When using the signalling method of detection of stolen vehicles, there is no necessity to store a list of VINs in the DEs. The procedure is as follows:

After report of a theft, the ATSVR SOC uses long range individual addressing (e. g. by GSM SMS) or broadcast messages to activate the stolen vehicle OBE. After activation, the OBE listens to "reading" emissions from stationary, mobile or handheld readers, and the OBE answers only upon reception of such interrogation signals by transmitting periodically its VIN, license plate No. etc.

## 6.2 Data Elements Common to both OBE and DE

### 6.2.1 General Data Elements

The General Data Elements serve for organising the data transfers, whereas the Specific Data Elements convey the necessary information.

- **Header**

The header defines which type of Short Range transmission will follow:

Header	1 byte	binary unsigned number
--------	--------	------------------------

Header Definition	Hex code	meaning
Fast identification sequence	01 <sub>16</sub>	The following data transfers are optimized for minimum transfer time and convey only the VIN
Extended identification sequence	02 <sub>16</sub>	The following data transfers convey complete vehicle identification elements: VIN, last known license plate, country of origin, make and type of vehicle, colour, known special equipment (like side airbags, glass lift-up-and-slide-back sunroof, automatic transmission, ), stolen status.  The suitable codes are selected "Common Status Message Elements"

- **Random Number**

The random number is used during encrypted sessions in order to guarantee that any new encryption of the same plain text results in totally different cipher text.

Designation	size	Code
Random Number	4 bytes	binary unsigned number

### 6.2.2 Specific Data Elements

The Theft Specific Data Elements

- **VIN Vehicle Identification Number**

The Vehicle Identification Number is an alpha numeric field which defines a

worldwide unique vehicle identifier. The field definition is taken from Common Status Message Elements, Annex A:

<b>Designation</b>	<b>size</b>	<b>Code</b>
VIN	17 bytes	ASCII

- **Incident, Stolen Status**

The field definition is taken from Common Status Message Elements, Annex A.

<b>Designation</b>	<b>size</b>	<b>Code</b>
Stolen status	1 byte	binary coded,

## **7 Regulatory Issues**

### **7.1 Communication Devices**

Equipment must be type-approved and must comply with European EMC directives, CE and appropriate radio type approvals.

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.

### **7.2 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. 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.

UNECE Reg. 21 [5] has been quoted

EC Directive 95/54/EEC has been quoted

EC Directive 89/336/EEC has been quoted

EC Directive 74/60/EEC (as amended) [5] has been quoted

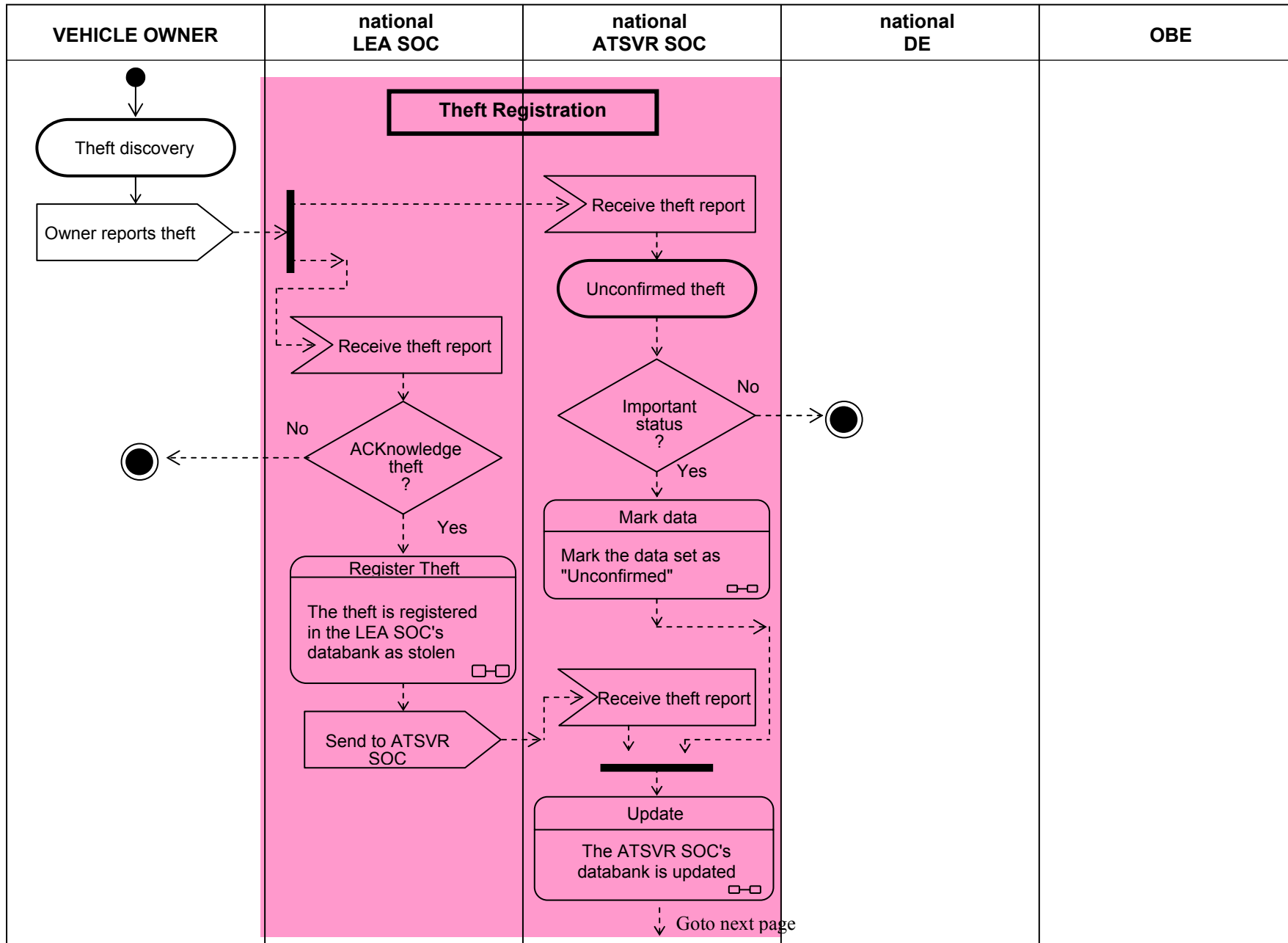
CEPT Recommendation 70-03 emitted radiated power of active devices

### **7.3 Public Liability Insurance**

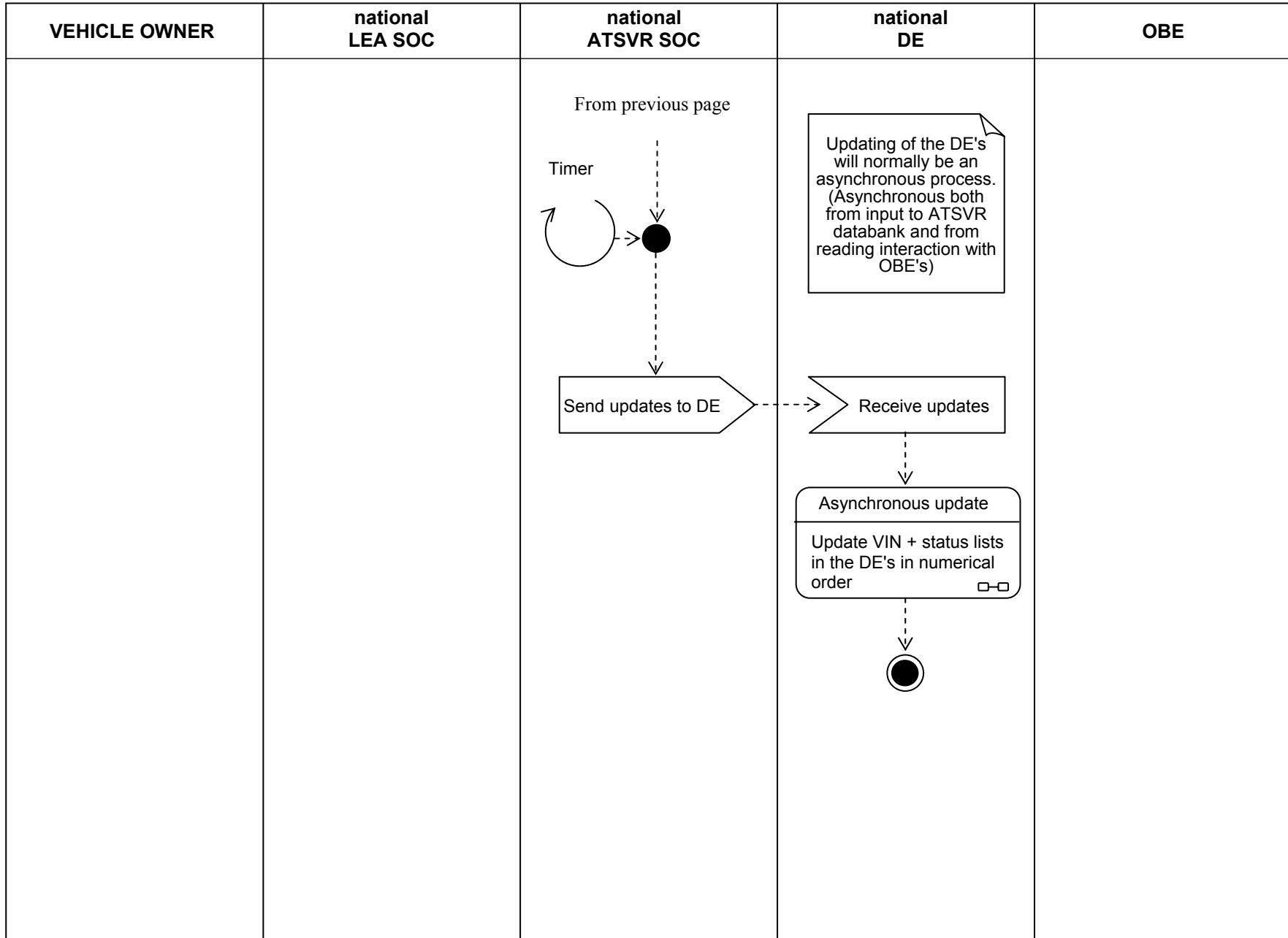
The ATSVR service provider must have public liability insurance.

## Appendix A STATE CHART DIAGRAMS OF THE ATSVR PROCESSES

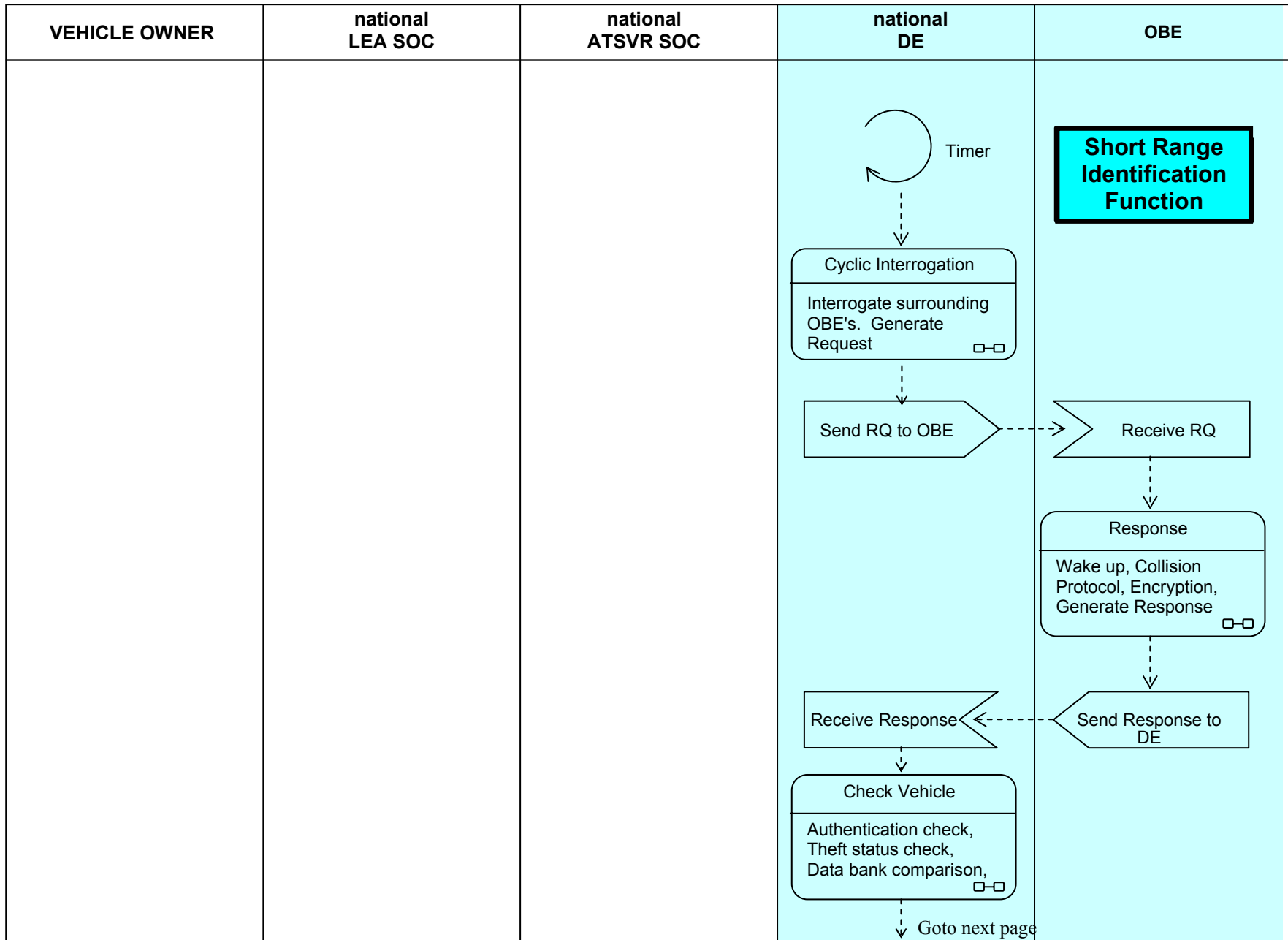
**Detection by Consulting**



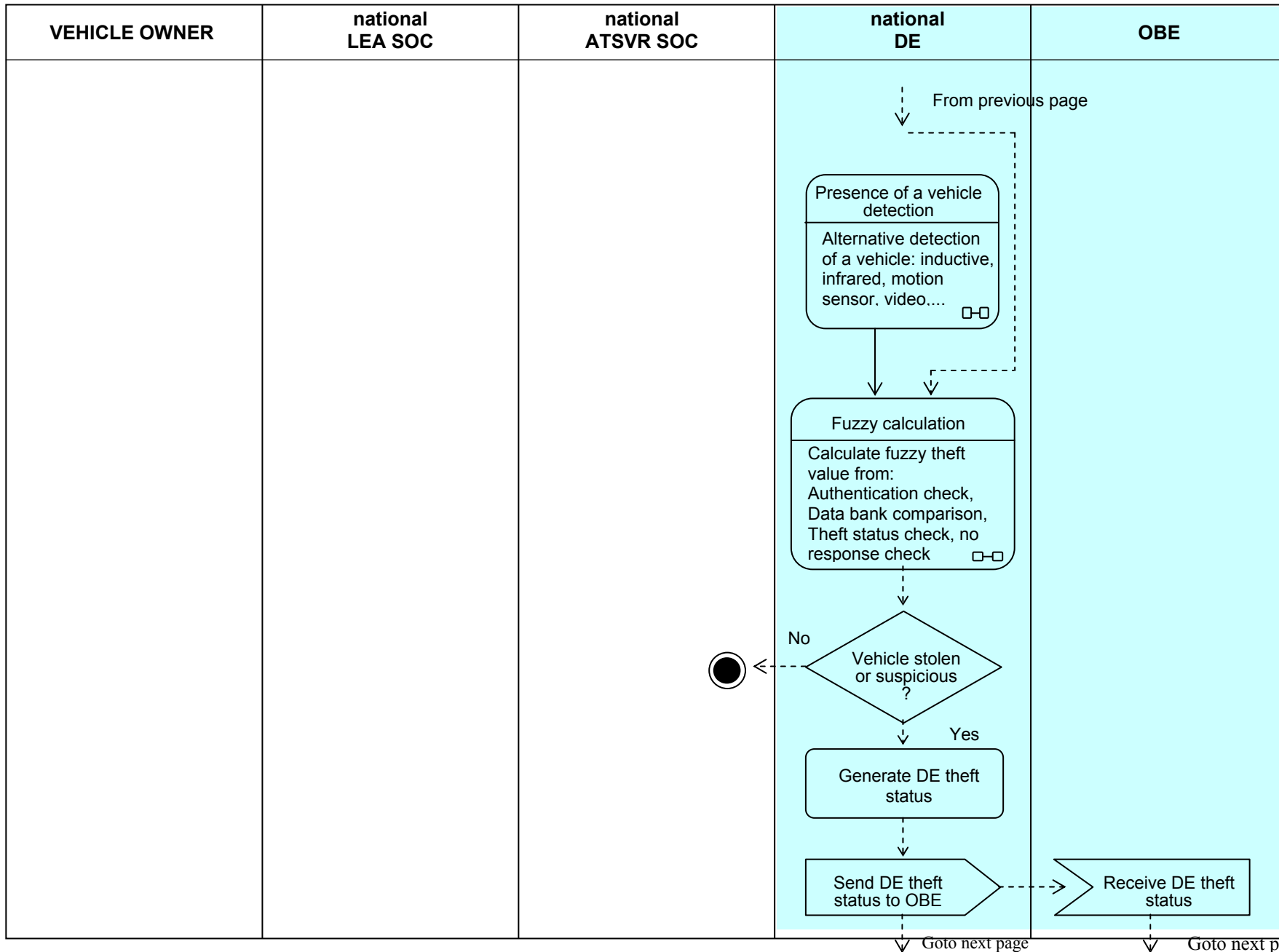
Detection by Consulting



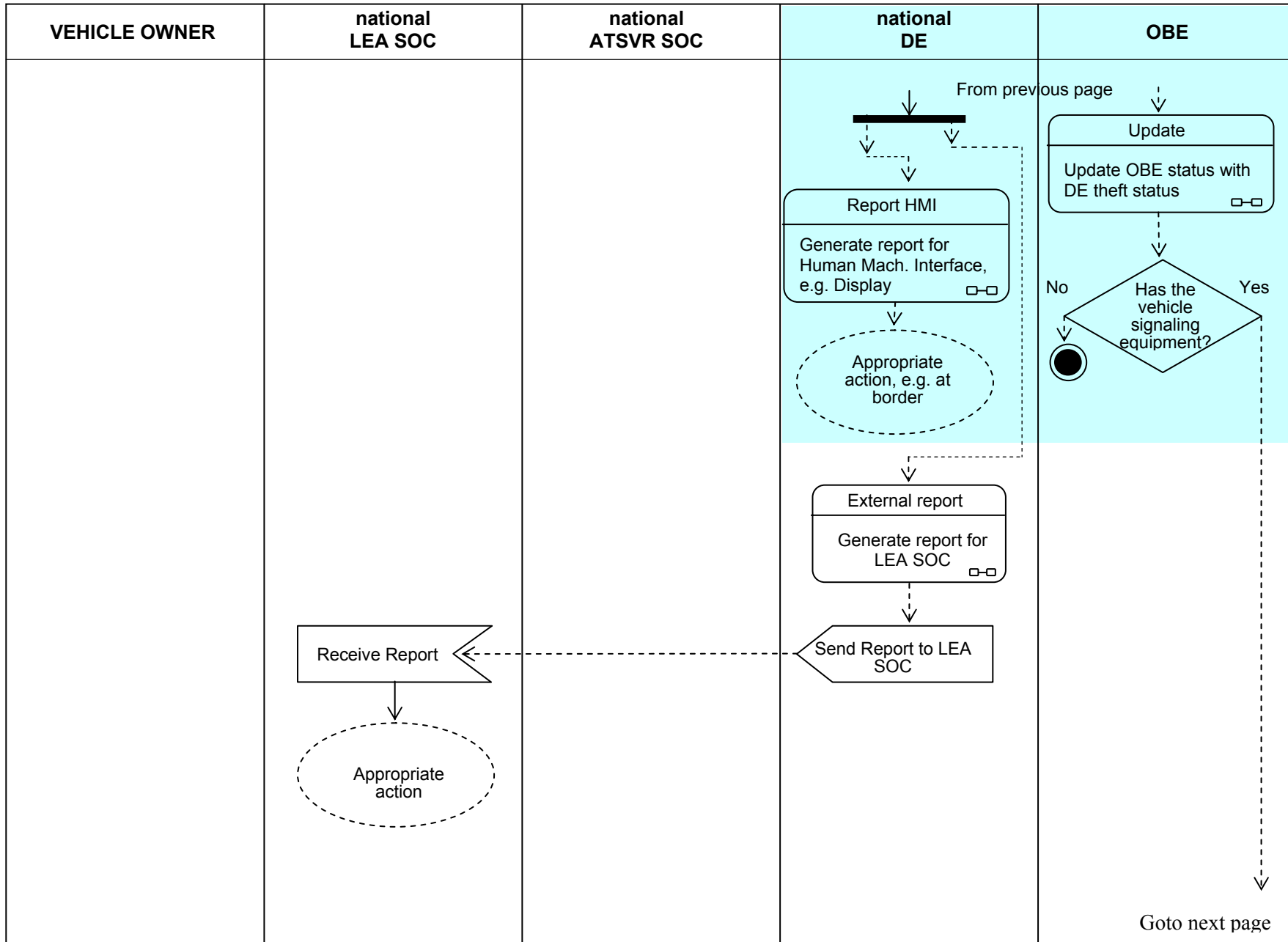
Detection by Consulting



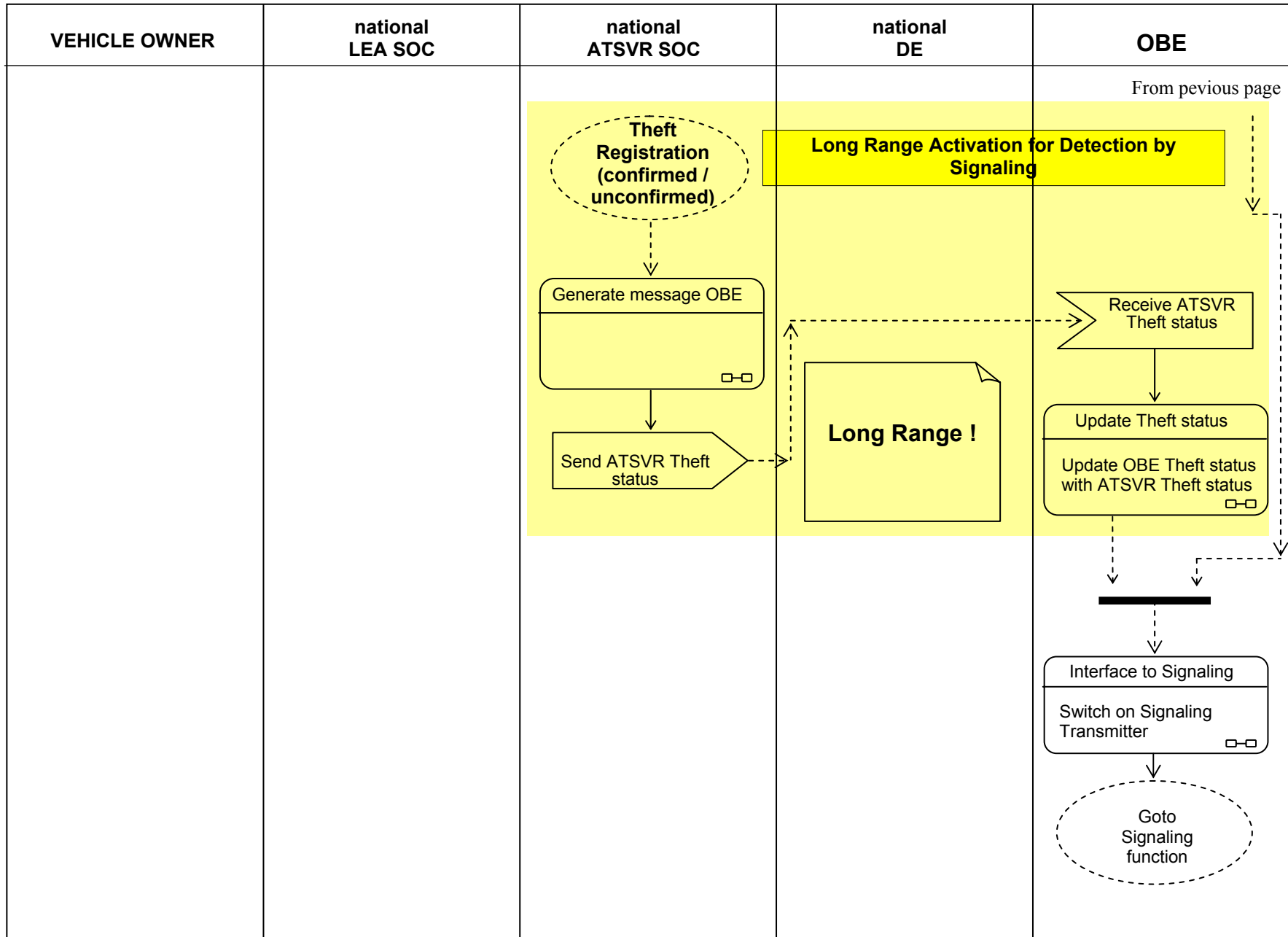
Detection by Consulting



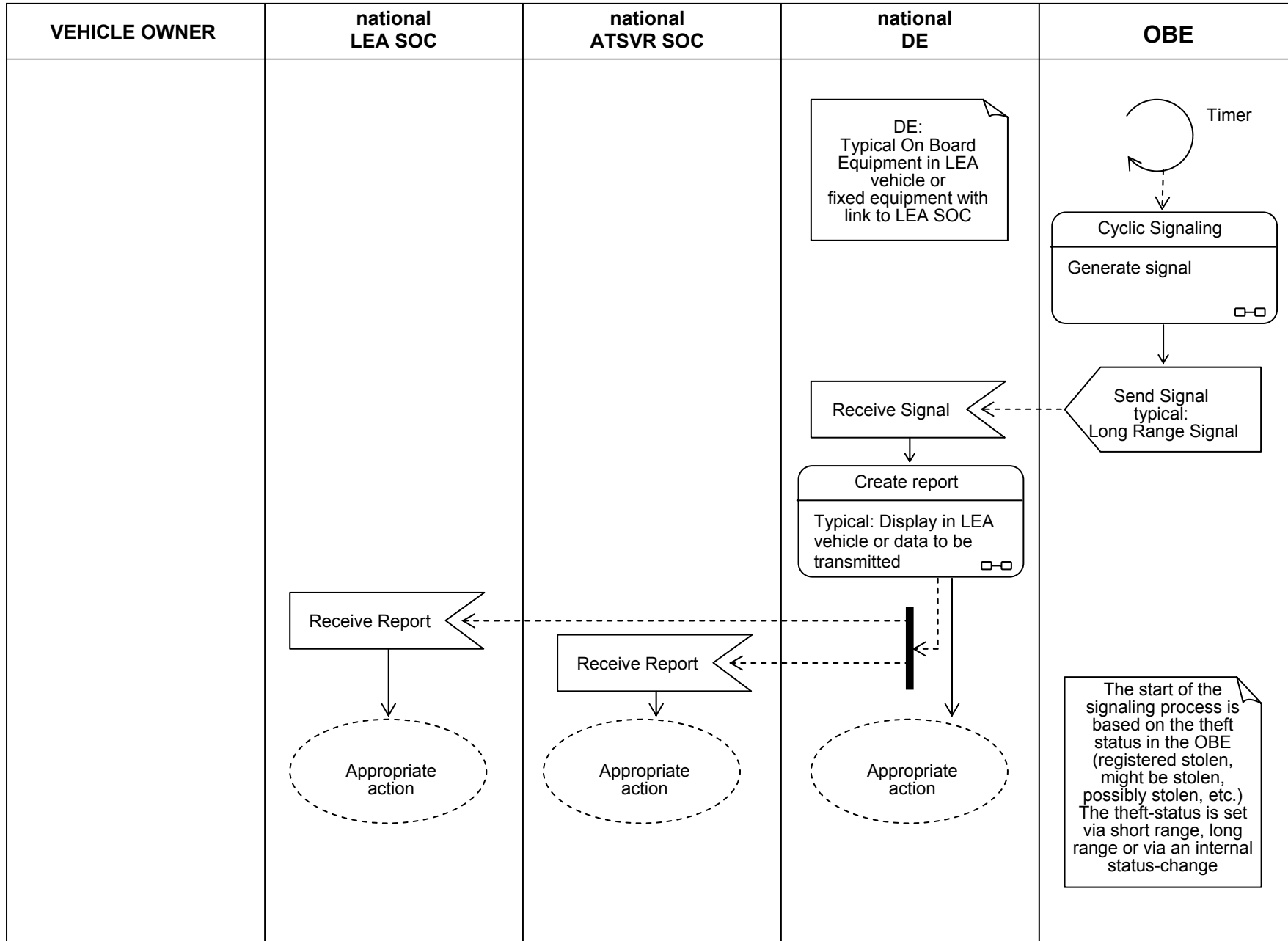
Detection by Consulting



Remote activation OBE



Signaling



This page is intentionally left blank

End of document