

# Specifications of Roadside ITS Stations

---

## Deliverable 2.4.2.1

**Activity 2 : Studies**

Sub-activity 2.4 > Specifications

Version 3.00

Publication date: 21/01/2019



Co-financed by the Connecting Europe  
Facility of the European Union

## Information on the document

Document: Specifications of Roadside ITS Stations

Date of publication: 21/01/2019

Responsible, Entity: Emilie PETIT, Cerema

Status: Version 3.00 – Approved

## Publication history

Date	Version	Author(s)	Main updates & changes	Distribution
21/01/2019	3.00	Marie-Christine ESPOSITO and Emilie PETIT	Final version for official release	Release 3

### Reference to the version administration

Version number to be composed of 3 digits > vR.XY

- R corresponds to the release number: it is upgraded each time SC Studies validates the diffusion of a new release,
- X is the major version number: it is upgraded each time SC Studies validates the deliverable,
- Y is the minor version number: it is upgraded each time a contributor changes anything.

Once the deliverable is approved, its version number is upgraded from vR.XY to vR.(X+1)0

Once the deliverable is release, its version number is upgraded from vR.XY to v(R+1).00

As illustration:

- 0.03 > Work in progress version
- 0.10 > Del. Approved by SC Studies but not released
- 2.00 > Del. approved & released (in release 2)
- 2.05 > Del. Updated - in progress version

# Table of Contents

1 Introduction .....	6
1.1 Document contents .....	6
1.2 Standards and related references .....	6
2 General Points .....	8
2.1 Definitions .....	8
2.2 Environment .....	8
2.3 Main R-ITS-S Functionalities .....	9
3 Equipment .....	11
3.1 Main unit .....	11
3.1.1 Power supply module (if present) .....	11
3.1.2 Hardware Security Module (HSM) (mandatory) .....	12
3.1.3 Memory (mandatory) .....	13
3.1.4 Computing unit (mandatory) .....	13
3.2 Telecommunication components .....	14
3.2.1 ITS-G5 .....	14
3.2.2 Cellular network .....	16
3.2.3 Satellite network .....	16
3.3 Connections and sensors .....	17
3.3.1 External connection .....	17
3.3.2 Monitoring sensors .....	17
3.4 R-ITS-S Case .....	18
4 Installation specifications .....	19
5 Software .....	20
5.1 Process received messages .....	21
5.1.1 Process received CAM .....	21
5.1.2 Process DENM received from the ITS stations .....	27
5.1.3 Forward received DENM messages .....	30
5.2 Distribute messages to users of the road network .....	31
5.2.1 DENM from the platform .....	31
5.2.2 [optional] DENM from the HMI (local or remote) .....	33

---

5.2.3 CAM-I .....	33
5.2.4 Secure sent messages .....	33
5.3 Security of the R-ITS-S.....	33
5.4 Facilities for the Vru-ITS-S.....	34
5.4.1 Relay security messages between Vru-ITS-S and PKI.....	34
5.4.2 Upload T-log/U-log from Vru-ITS-S.....	34
5.4.3 Send road tolling positions to Vru-ITS-S and Vro-ITS-S.....	35
5.5 Internal R-ITS-S management:.....	35
5.5.1 R-ITS-S Start-up.....	35
5.5.2 R-ITS-S Shut-down.....	35
5.5.3 Data management .....	36
5.5.4 Data protection .....	36
5.5.5 Connection .....	36
5.5.6 Supervision (local and remote access).....	37
5.5.7 Configuration, (remote and local access.) .....	37
5.5.8 T-log .....	40
5.5.9 Fail-soft modes .....	40
5.5.10 Validation of the system.....	42

## List of figures

Illustration 1: Architecture of the SCOOP project, from the point of view of R-ITS-S .....	8
Illustration 2: Different functionalities between fixed and mobile R-ITS-S .....	10
Illustration 3: ITS Station Architecture .....	20
Illustration 4: Functions implemented through the A1 use-case .....	22
Illustration 5: Description of a zone .....	24
Illustration 6: R-ITS-S functions about DENM .....	27

# 1 Introduction

## 1.1 Document contents

This document compiles the technical specifications for the road-side communication equipment designated hereafter by Road-Side Unit (RSU) or R-ITS-S, which has to be installed as part of the SCOOP project.

The specifications in this document describe the hardware and software aspects of this equipment. These are the minimum established requirements recommended to serve as a common base for all project partners likely to acquire R-ITS-S. These recommendations make it possible in principle for the system to run. The second underlying objective is to ensure that the equipment is compatible between all the partner sites. Most of the requirements were chosen to involve few constraints so different technical solutions can be used to comply with them.

However, the specific implementation characteristics at each deployment site may require adding other requirements to, and/or exceptions from, the specifications formulated in this document. These modifications shall be explained in each partner's R-ITS-S acquisition specifications.

## 1.2 Standards and related references

This document calls on the standards and references described in the SCOOP deliverable [2.4.1.bis: Applicable standards for SCOOP]. Some supplementary standards have to be respected :

Ce marking for Electromagnetic compatibility :

- EN 61000-6-2 : 2005 (Electromagnetic compatibility (EMC). Generic standards. Immunity for industrial environments )
- Draft ETSI EN 301 489-1 V2.2.0 : 2017 : ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements; Harmonised Standard covering the essential requirements of article 3.1(b) of Directive 2014/53/EU and the essential requirements of article 6 of Directive 2014/30/EU
- Final Draft ETSI EN 301 489-3 V2.1.1 : 2017 ; ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 246 GHz; Harmonised Standard covering the essential requirements of article 3.1(b) of Directive 2014/53/EU
- Final draft ETSI EN 301 489-52 V1.1.0 : 2016 : Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for Cellular Communication Mobile and portable (UE) radio and ancillary equipment; Harmonised Standard covering the essential requirements of article 3.1(b) of Directive 2014/53/EU

- EN 62479 : 2010 : Assessment of the compliance of low-power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

CE marking for radio :

- ETSI EN 302 571 V2.1.1 : Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- Draft ETSI EN 303 413 V1.1.1 : 2017 : Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) receivers; Radio equipment operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz frequency bands; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- ETSI EN 301 511 V.12.5.1 : 2017 : Global System for Mobile communications (GSM); Mobile Stations (MS) equipment; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- ETSI EN 301 908-2 V11.1.1 : 2016 : IMT cellular networks; Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE)

CE marking for safety electrical :

- 1 EN/CEI 61010-1 : Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements

## 2 General Points

### 2.1 Definitions

In this document, the following terms are used:

- RSU: Road Side Unit, also called R-ITS-S, it is a C-ITS station deployed on the side of the road network, called “UBR” in French in SCOOP.
- OBU: on board unit, also called V-ITS-S: C-ITS station in a vehicle. Vru-ITS-S is in any User vehicle, and Vro-ITS-S is in a Road Operator Vehicle.

R-ITS-S have different functional types:

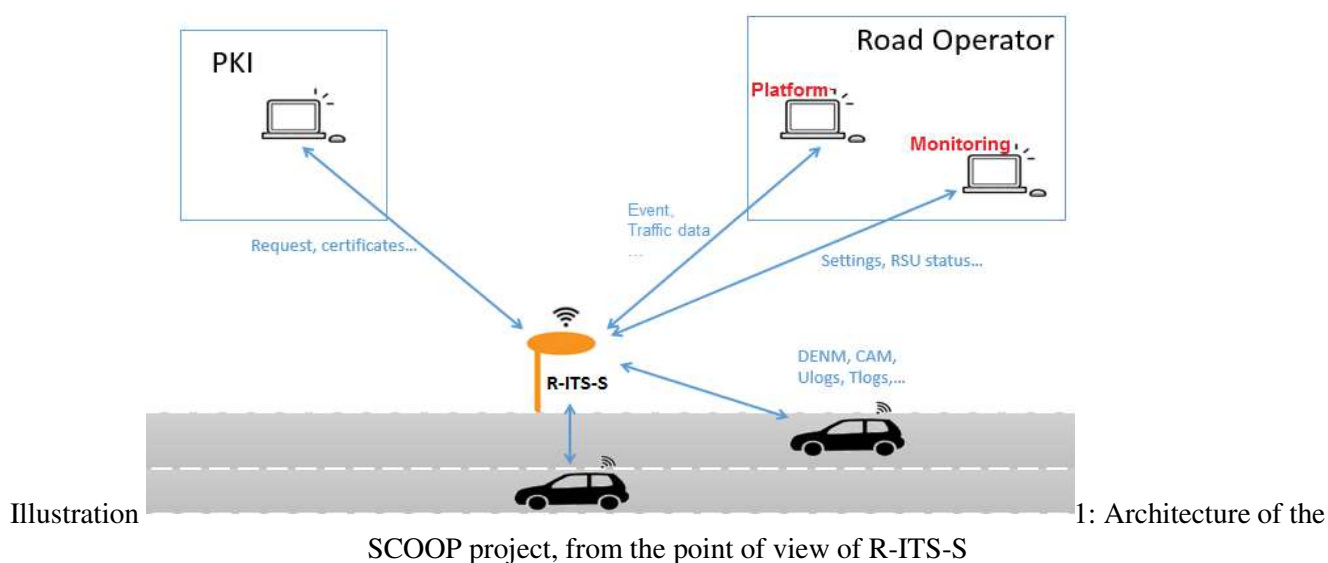
- Fixed R-ITS-S: (“UBR fixe”): R-ITS-S on the side of the road. All the functions described in this document are implemented inside.
- Mobile R-ITS-S: Function of a Vro-ITS-S, that only have some of the functions described in this document (See Chapter 2.3 Main R-ITS-S Functionalities).

### 2.2 Environment

The architecture of the SCOOP project, from the point of view of a R-ITS-S, is presented in the figure below. A R-ITS-S communicates with 4 different main entities: the SCOOP platform, the PKI, the monitoring server and C-ITS vehicles.



Illustration 1: Architecture of the SCOOP project, from the point of view of R-ITS-S



Note: The R-ITS-S on the illustration can be fixed, or mobile, or moveable. See chapter Installation.

Note: Not all the SCOOP messages are described on this schema. And, for example, the Ulogs and Tlogs messages are not treated by a mobile R-ITS-S.

## 2.3 Main R-ITS-S Functionalities

As indicated in the definitions, the R-ITS-S is a road ITS station based on the ETSI definition. It can be used simultaneously to:

- process received messages:
  - receive CAM or DENM messages from the ITS stations on the road network (especially V-ITS-S)
  - process them
  - transmit information to the SCOOP platform
  - forward messages to the ITS stations on the road network
- distribute messages to users of the road network:
  - from the platform
  - from the HMI (local or central)
- offer services to the V-ITS-S:
  - relay “security messages” between Vru-ITS-S and PKI
  - download T-log/U-log from Vru-ITS-S to special server
  - send positions of the tolls to V-ITS-S

Necessarily, the R-ITS-S has others functions to maintain itself:

- security management
  - download and management of the R-ITS-S certificates
  - update
- internal management:
  - protection of data (HSM, ...)
  - supervision and log file (local / remote)
  - configuration (local / remote)
  - update (local / remote)
  - T-log (local / remote)
  - management of degraded modes
  - functions or software to enable the validation of the R-ITS-S software (HMI, specific commands, upper tester, etc.)

The mobile R-ITS-S have mostly the same functions as fixed R-ITS-S, except for some specific functions that are not provided or are dealt with differently. This is summarised in illustration 2.

	Fixed R-ITS-S	Mobile R-ITS-S
receive CAM, process them, transmit information to the SCOOP platform,	X	
receive DENM, process them, transmit information to the SCOOP platform, forward messages to the ITS stations on the road network	X	Note X
from the platform	X	X
from the HMI (local or central)	X	Note X
relay security messages between Vru-ITS-S and PKI	X	
download T-log/U-log from Vru-ITS-S to special server	X	
send positions of the tolls to the V-ITS-S	X	
download and management of the R-ITS-S certificates	X	Note X
update	X	Note X
protection of data (HSM, ...)	X	Note X
supervision and log file (local / remote)	X	Note X
configuration (local / remote)	X	Note X
update (local / remote)	X	Note X
T-log (local / remote)	X	Note X
management of degraded modes	X	Note X
functions or software to enable the validation of the R-ITS-S software (HMI, command, diary, etc.)	X	Note X

Illustration 2: Different functionalities between fixed and mobile R-ITS-S

X means “Shall be done by the R-ITS-S”

---

Note: The process is not the same for Mobile and Fixed R-ITS-S. See all the SCOOP Deliverables [2.4.2.2 Vro-ITS-S Specifications] for more information.

## 3 Equipment

The R-ITS-S includes:

- a power supply,
- the main unit,
- the communication modules (including the Datex II translation software that could be supplied to the platform),
- the antennas (GNSS, ITS-G5, cellular...)
  - the antennas can be gathered in the same protective physical case
- the external connections (located inside the R-ITS-S case)
- and the R-ITS-S case (which can potentially be comprised of two cases depending on the defined installation).

All R-ITS-S components must be easy to maintain and to replace.

In some types of installations, some elements can be removed. For example, the power supply can be removed in the presence of an already existent power supply.

The G5 unit can be either partially remote (only the antenna - see §3.2.1.6 ) or totally remote (antenna and communication module).

### 3.1 Main unit

The main unit is determined, among other things, by its internal memory and its computing unit. It is powered by the power supply module.

#### 3.1.1 Power supply module (if present)

The power supply module must comply with the NF C15-100 standard.

The power supply can operate via Ethernet (Power over Ethernet (PoE)) or operate directly on the operator's electrical network. An independent power supply shall operate one quarter of an hour in case of a power outage.

Depending on the electrical connection and the R-ITS-S support, the power supply module can also be adapted to the following situations (based on each pilot site):

- connection on a lamppost: it shall be able to recharge the additional power supply module at night, so that it can operate during the day,
- connection on a solar panel or with wind turbine: it shall be able to recharge the additional power supply module during the day (solar panel) or night (wind turbine) ; the consumption calculation will be based on the most unfavourable periods of the year on the pilot site,
- autonomous operation: it shall be able to operate via an autonomous power supply the entire day without any power supply (e.g. battery or electric generator),

The battery charging circuit must include a charge regulator so that the battery is not

damaged. The batteries shall be waterproof.  
It shall be easy to replace the entire power supply module.

The R-ITS-S shall be powered between 12 and 48V from this optional power supply module included in the R-ITS-S equipment or from an existing module in the field.

### 3.1.2 Hardware Security Module (HSM) (mandatory)

#### 3.1.2.1 Description

The Hardware Security Module is a physical computing device that is highly secure. It generates, stores, protects cryptographic keys and provides cryptoprocessing. If it is handled physically, it can self-destruct its data. The Hardware Security Modules meet international security standards like EAL4+ Common Criteria and can support cryptographic APIs.

#### 3.1.2.2 Mandatory Functions

The HSM shall:

- store the critical security components like private keys,
- perform cryptographic operations with the stored keys,
- support Cryptography algorithms (cited in ETSI TS 103 097 V1.2.1: "Intelligent Transport Systems (ITS); Intelligent Transport Systems (ITS); Security; Security header and certificate formats")

#### 3.1.2.3 Optional Functions

The HSM can:

- verify the certificates
- compute the signature of the received messages (LTC verification key pair, based on the algorithm ECDSA NIST P-256)
- secure the messages sent, with the certificates of the R-ITS-S (TSK (technical secret key), based on the algorithm ECDSA NIST P-256 idem)
- contain securely the certificates and the public keys of the certificate authorities used to perform the cryptographic operations.

Nevertheless, if the HSM does not perform these processes, the R-ITS-S must perform them.

### 3.1.2.4 Functions not covered by the HSM

This module does not perform all of the PKI related processes. See Deliverables [2.4.4.X : Security in SCOOP] for more information on the HSM and on the PKI related processes. For example, the HSM does not:

- create a certificate
- connect to the PKI server
- generate TPK (technical public key)
- ...

### 3.1.2.5 Data self-erasure

The HSM can self-erase its data in the following cases:

- wrongful handling, detected by an accelerometer for example
- wrongful opening,
- connection with an unauthorized drive, either on the USB port or via Ethernet cable...

Note: An operator can enable or disable the erasure when this operator is authorized (for example, when an authorized dongle is set in the USB port, or a recognized computer is connected to the Ethernet port...). To allow an operator to authenticate himself, the self-erasure is done after a configurable time, by default 60sec.

Note: The erasure can be deactivated for the tests on the prototypes.

## 3.1.3 Memory (mandatory)

An internal storage memory will be integrated in the module and will contain at least 16 Gb of memory. The used partitions will also be encrypted for security reasons. For reasons of environmental resistance, rotary hard disks are not recommended.

At least 256 Mb of RAM shall be integrated in the system. The RAM can be larger if necessary, because it must absolutely have 30% of unused capacity when all the services detailed in this document are deployed and active.

The memories shall be easy to replace, thus removable.

## 3.1.4 Computing unit (mandatory)

The computing unit must be able to process all operations, uses cases or information, defined in the SCOOP specifications, in accordance with the contextual conditions requested by the operators. (See chapter §5 Software for details).

The Computing unit must be able to simultaneously compute all the operations described in the software part. Thus, an acceptable size of the processor can be 900 MIPS.

Note: It is more or less equivalent to a single processor with a 900Mhz frequency.

## 3.2 Telecommunication components

The telecommunication components include an ITS-G5 communication module for I2V and V2I communications, and it can include a cellular communication module, for the platform communications.

### 3.2.1 ITS-G5

#### 3.2.1.1 Frequency range

The harmonized frequency range in Europe is from 5855 MHz to 5905 MHz. This range is divided into two sub-bands, the first from 5855 MHz to 5875 MHz called G5B and the second from 5875 MHz to 5905 MHz called G5A.

ARCEP (French telecommunications and postal regulatory body) decision No. 2010-0852 dated 2 September 2010 sets the operating conditions for wireless frequencies that intelligent transportation system applications can use as the 5875-5905 MHz band (G5A).

This last sub-band is dedicated to road security and breaks down into 3 channels, each 10 MHz wide:

- the 180 channel centred on 5900 MHz, called CCH (reference channel);
- the 178 channel centred on 5890 MHz, called SCH2 (service channel 2), not used in the project; and
- the 176 channel centred on 5880 MHz, called SCH1 (service channel 1);

Communications are established in simplex (i.e., the transmission frequency and the receiving frequency are identical) and comply with the standards used in SCOOP (See [2.4.1.bis: Applicable standards for SCOOP]).

#### 3.2.1.2 Transmit power

The appendix to decision No. 2010-0852, titled "spécification d'interface radioélectrique" (wireless interface specification) defines the Equivalent Isotropically Radiated Power (EIRP) authorized by ARCEP and in compliance with the European Commission decision 2008/671/EC. This EIRP is 33 dBm for channels 176 and 180. The EIRP takes into account the transmit power, the antenna gain and the loss in the antenna's coaxial cable. The transmit power should be adapted to each R-ITS-S based on the antenna and related cable in order to get as close as possible to the 33 dBm without exceeding it.

Moreover, this appendix specifies the access and occupancy rules (i.e., the interference attenuation techniques that should be used). They imply that the transmitter has a "TPC" (Transmit Power Control) system.

The transmitters do not have to be declared with the "Agence Nationale des Fréquences" (ANFR) (French National Frequency Agency), but in exchange they cannot claim any protection against interference.



### 3.2.1.3 Range

The range of the transmitters depends largely on the installation site because the waves in this range of frequencies are quickly attenuated, even stopped, depending on the density of natural obstacles in the vicinity.

The theoretical average range should be estimated at approximately 1000 metres based on the relief and nature of the ground surface, under rather favourable weather conditions, for a R-ITS-S antenna installed on a pole 10 metres above the ground.

Practically, the messages sent by a R-ITS-S, must be received at a rate of at least 90% by the SCOOP Vru-ITS-S, positioned in free space 500m from the R-ITS-S, and driving at a normal speed, adapted to the road.

### 3.2.1.4 Receiver sensitivity

Depending on the modulation schema of the subcarrier OFDM, the maximum theoretical throughput varies. As a minimum, with the OFDM modulation (currently used in the 5 GHz band), the R-ITS-S receivers should have greater than -90 dBm sensitivity, corresponding to a throughput of 10 messages per second.

The R-ITS-S is comprised of two transmitter-receiver (transducer) units operating simultaneously.

### 3.2.1.5 Type of antenna

The antenna installed in the R-ITS-S and dedicated to the ITS G5 networks must comply with the following requirements:

- A) Electric data
  - can either be omnidirectional (most probably the majority of cases) or directional in specific cases where it will be necessary to give priority to a very specific coverage sector of a few dozen degrees
  - impedance 50 Ohms;
  - vertical polarisation;
  - N Jack female termination;
  - gain between 5 dBi and 12 dBi; the antenna must have a minimum gain of 5 dBi to offset the losses in the coaxial cable.
  - acceptable power > 5 Watts;
  - SWR < 2,1
- B) Mechanical data
  - radome type in anti-UV treated fibreglass or PVC;
  - height or length < 0.5 m;
  - weight < 1 Kg;
  - with mounting flange for pole
- C) Environmental data
  - maximum admissible wind 200 km/h;
  - operating temperature -40°C to + 60°C;
  - impermeability IP67.

### 3.2.1.6 Antenna cable

The coaxial cables used for the R-ITS-S, that make it possible to position the antenna remotely from the transmitter, must have attenuation characteristics less than 40 dB at 100 m at the frequency of 5900 MHz.

If there are two cases (G5 and the computing unit), power can be supplied to the G5 module by PoE and by traditional cables.

Note: the road operator must try to minimise the length of the cable to minimise the signal attenuation. The acceptable length depends on the installation, on the type of cables, antennas, and of the characteristics of the R-ITS-S,

## 3.2.2 Cellular network

The cellular connections can be integrated with a SIM location in a modem integrated in the R-ITS-S.

The antenna installed in the R-ITS-S and dedicated to the connection to the cellular networks must comply with the following requirements:

- A) Electric data
  - omnidirectional type radiation;
  - multi-bands 2G/3G/4G;
  - impedance 50 Ohms;
  - vertical polarisation;
  - N female termination;
  - gain between 2 dBi and 5 dBi;
  - acceptable power > 5 Watts;
  - SWR < 1.6.
- B) Mechanical data
  - radome type in anti-UV treated fibreglass or PVC;
  - height or length < 0.5 m;
  - weight < 1 Kg;
  - with mounting flange for pole
- C) Environmental data
  - maximum admissible wind 200 km/h;
  - operating temperature -40°C to + 60°C;
  - impermeability IP67.

### 3.2.3 Satellite network

A GNSS receiver can also be installed to accommodate:

- a time synchronisation in relation to the satellite network see chapter 5.5.5.1 for software time synchronisation;
- a differential position calculation.

This GNSS system can be GPS, GLONASS or GALILEO. It can also improve its reliability using more than one of these systems.

Consequently, the GNSS module can be remote if needed.

## 3.3 Connections and sensors

The external connections, located in the R-ITS-S case (see 3.4 ), can be used to position the R-ITS-S in the operator's network and to ensure it is in good working order (power supply, communication and monitoring). The monitoring is also provided by the presence of monitoring sensors that are then processed by the monitoring tool.

Note: This monitoring shall be accessed by the HMI (See chapter 5.5.6 Supervision)

### 3.3.1 External connection

The external connection is protected by the R-ITS-S case and includes at least:

- one power outlet;
- one connection that can be used to communicate with the R-ITS-S for local monitoring (RJ45, USB 2.0, etc.);
- one level 3 switch (4-port Ethernet flexible lead connector) with access switching between Ethernet and optical fibre or a router with at least one RJ45 input/output and an optical outlet.

### 3.3.2 Monitoring sensors

The operator must be able to remotely control the R-ITS-S and have access to the same monitoring items that the R-ITS-S's local monitoring could display on a connected terminal:

- the status of the battery,
- the status of the antenna connection and the state of the antenna itself,
- the status of connections (Cellular modem, G5 modem, GNSS, other connections),
- the status of the memory,
- the calculation resources, and
- the status of the processors.

In order to do so, all the previously mentioned equipments must be equipped with the relevant sensors.

## 3.4 R-ITS-S Case

The R-ITS-S case can be mounted on a gantry or a mast (in which case the appropriate fasteners shall be included) or mounted directly on the ground. All fasteners shall be made in stainless steel for difficult environments (storms, salt, etc.).

The electric and data cables shall run through cable glands to ensure they are mechanically protected and also to ensure the equipment they are connected to is impermeable.

The case cannot be opened without the use of one (or more) specific key(s).

The case shall ensure operability:

- for outside temperatures ranging from -25°C to +55°C,
- for a level of humidity ranging from 10% to 80%, and
- in compliance with the IP65 and IK8 indexes (CEI 60529 standard) related respectively to the protection against the penetration of foreign solid bodies and water and against external mechanical impacts.

If the antenna and the communication modules in G5 are remote, two cases can be used.

## 4 Installation specifications

Fixed R-ITS-S can be installed in different ways:

- Fixed R-ITS-S (term by default): This station can't be simply removed once it is installed.
- Autonomous R-ITS-S ("UBR autonome"): A station fully autonomous in terms of networks and light enough to be moved by a human operator (for example: the R-ITS-S + a battery + a solar panel + a cellular connection + a movable antenna on a light mast).

For example, an autonomous R-ITS-S will be left on the roadside during temporary roadworks for a few days;

- Moveable R-ITS-S ("UBR déplaçable"): A station partially autonomous in terms of networks and light enough to be moved by a human operator (for example: the R-ITS-S + a cellular connection + a movable antenna on a light mast + electrical connections)

For example, a moveable R-ITS-S will be brought for a specific test session for a few hours and directly managed by an operator.

The installation guidance is available in deliverable 2.4.2.1\_annex.

## 5 Software

The software part of the R-ITS-S includes different layers, the ITS station reference architecture is shown in the figure below:

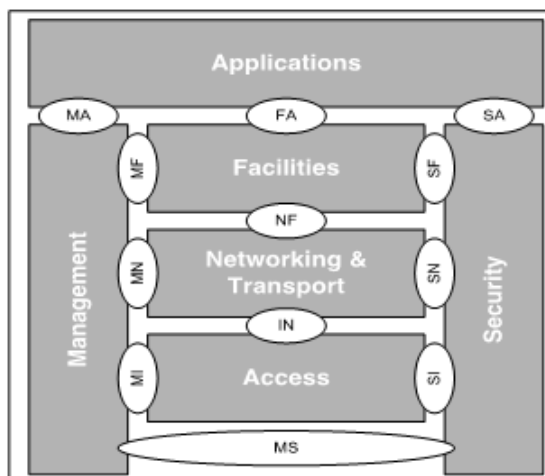


Illustration 3: ITS Station Architecture

- Applications layer:
  - R-ITS-S configuration,
  - applications for use-cases,
  - part of the Local Dynamic Map (LDM),
  - translation between DENM and DATEX (can also be done in the facilities layer).
- Facilities layer
  - part of the Local Dynamic Map (LDM); it must be possible to update it in real time, the information in the CAM and DENM messages are processed and stored in the LDM type module, based on the dictionary of messages by use-case.
- Transport and network layer
  - A TCP/IP is required with the operator's required compatibilities. The TCP ensures that the connection between the R-ITS-S and the platform is reliable, it supports the PKI requests and the logs upload.
  - Communications are transported between the Vru-ITS-S and R-ITS-S by the Geo-Networking Basic Transport Protocol (GNBTP).
  - The PKI traffic flows through HTTP.
  - The log files from the Vru-ITS-S flow through sftp.
- Access layer
  - The access layer of the ITS station reference architecture includes both the physical layer and the data link layer of the OSI model, in order to define access technologies used: ITS-G5, cellular, ethernet, ... or several of them.
  - R-ITS-S - platform: via a wire-based Ethernet link or via a cellular link, in full-duplex.
  - R-ITS-S – Vru-ITS-S : in ITS-G5

- R-ITS-S – PKI : via Ethernet or cellular link.
- Security Layer
  - requests and responses to the PKI for the R-ITS-S needs,
  - management of the R-ITS-S personal certificates
  - other security rules for the different interfaces (e.g. VPN for 3G/4G connections)
- Management Layer
  - R-ITS-S Configuration
  - Supervision
  - Creation of R-ITS-S T-logs

## 5.1 Process received messages

### 5.1.1 Process received CAM

This process concerns only the fixed R-ITS-S.

#### 5.1.1.1 Situation

A CAM is sent by any V-ITS-S.

The R-ITS-S receives all CAM and processes them.

The R-ITS-S sends calculated information to the SCOP platform, when it is relevant.

This function refers to receiving and understanding the CAM messages transmitted by the vehicles. It also involves knowing what to do with the information contained in each message and apply the rules accordingly to the received CAMs.

#### 5.1.1.2 Functions

The UML type diagram hereafter explains the functions implemented through the A1 use-case.

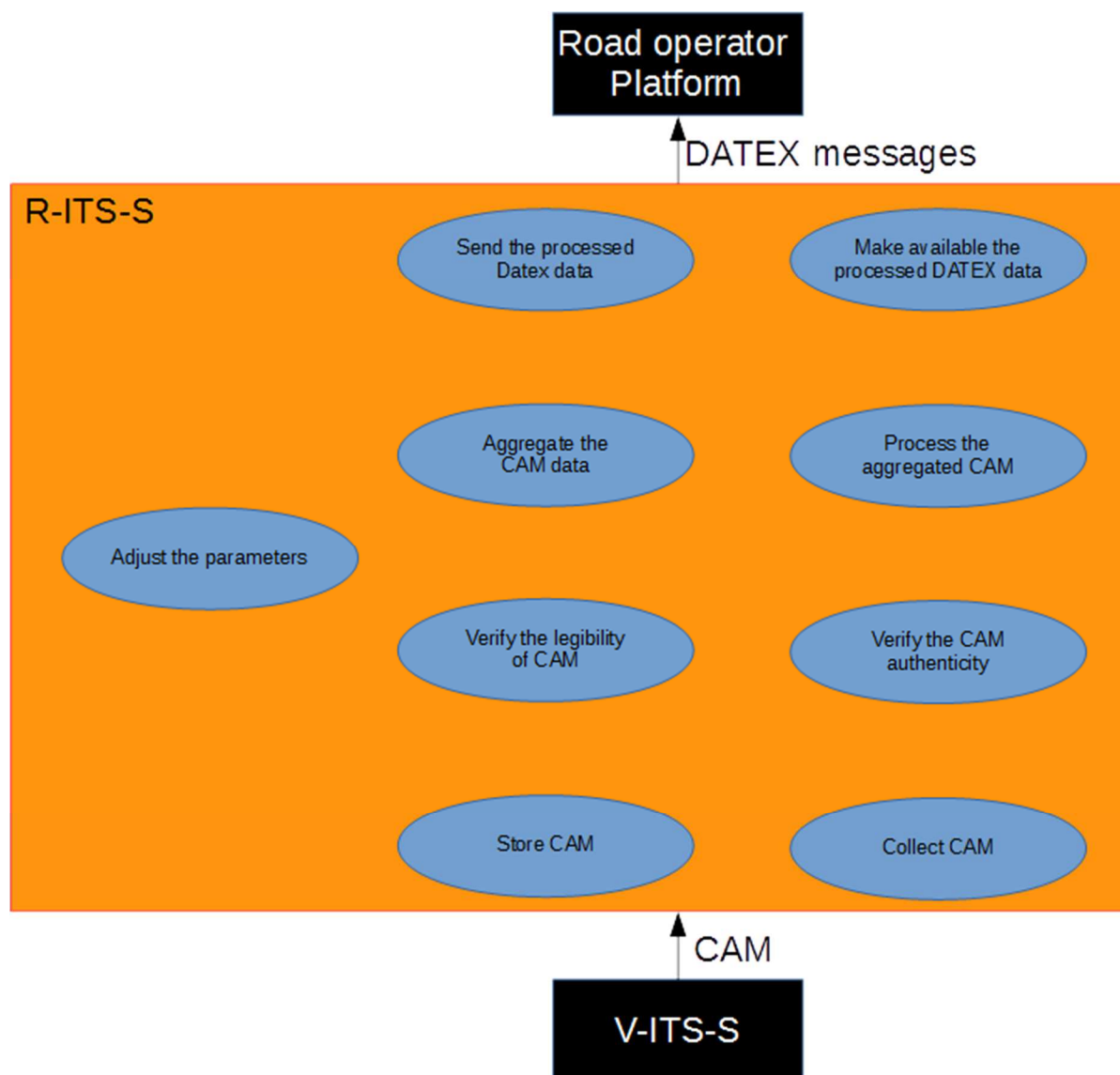


Illustration 4: Functions implemented through the A1 use-case

#### 5.1.1.2.1 COLLECT CAMS

This function consists in receiving CAM messages, and understanding the CAM messages transmitted by the vehicles.

For example:

- check that the messageID in the header is set to 2.

#### 5.1.1.2.2 STORE CAMS

This function stores the CAM information, according to a configurable storage time, with a configurable storage space constraint.

The R-ITS-S will store all received CAMs during a customizable period (which should be greater than the aggregation period), in a storage space reserved for real-time processing.



If the number of messages received exceeds a storage limit defined by the operator, the oldest CAMs will be deleted and replaced by the more recent CAMs. A message shall also be sent to the operator in order to inform him of the problem. Moreover, the log files will be completed with the information.

The storage space reserved for post-processing will also store all the processed received CAMs, from the last transmission of aggregated post-processing information to the platform.

The storage space reserved for project validation can also store all received CAMs.

When a CAM message contains a certificate, the R-ITS-S must store the certificate for a configurable time in order to verify the next CAM messages received without certificates.

#### Parameters

- CAM storage limit
- time of storage of a certificate (Default value: 1 second)

#### **5.1.1.2.3 VERIFY THE LEGIBILITY OF CAMs**

This function concerns verifying the legibility of the message received, which corresponds to the transmission of a CAM message. The function consolidates the ability to identify an incomplete or invalid CAM that can not be processed and to know how to process it.

In particular, the R-ITS-S shall check the messages based on their completeness according to the deliverable 2.4.1 mandatory data elements.

#### **5.1.1.2.4 AGGREGATE THE CAM DATA**

This function is to create data with the relevant received CAM. This involves consolidating and aggregating the information collected from several CAMs in order to produce usable data for the SCOOP - A1 service.

The CAM is relevant for the aggregation considered:

- if the message has been received in one of the zones of a virtual sensor.
- if the date-times of the message are in the aggregation duration.

The R-ITS-S must offer the ability to create from 1 to 10 virtual "sensors" which are geographic rectangles, per direction for the CAMs, determined by a specific identifier attached to the R-ITS-S identifier. The sensors can cover the same space: they are not necessarily disjoint. These zones shall be configurable in the R-ITS-S.

A sensor is a rectangle, with a heading, associated to a precision value. Only the vehicles in the same heading, regard to the precision set, shall be taken into account.

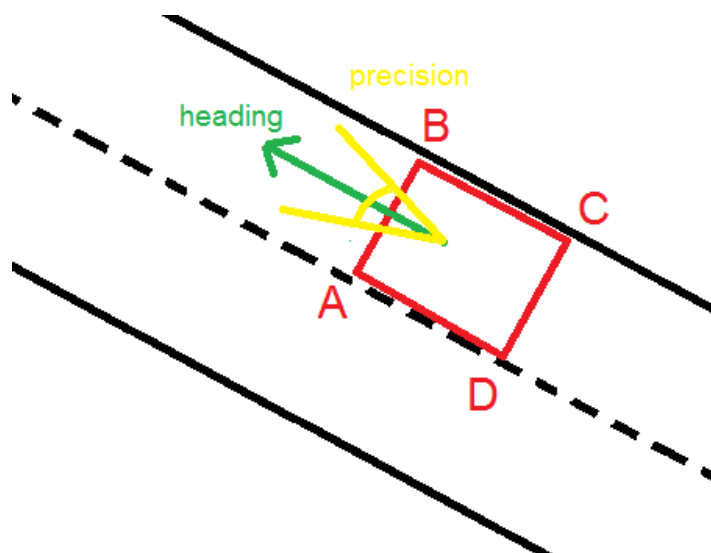


Illustration 5: Description of a zone

For each aggregation period, the software will calculate for each virtual sensor, using only the CAM:

- number of vehicles present,
- a harmonic speed mean of a vehicle,
- a harmonic speed mean of all the individual harmonic speed means (previously mentioned),
- a harmonic speed mean of all the speeds in each first CAM received from a vehicle
- an average length of the vehicles,
- the harmonic speed means of all the vehicles in a class (The class is a gathering of vehicles by length or other characteristics present in a CAM message.)
- the number of vehicles in a class (The number of vehicles per class will be stored by aggregation time steps. The length intervals can contain more classes, with a maximum of 6 classes that the software can configure by the necessary 5 thresholds.)

The aggregations will also show the number of vehicles concerned by each time aggregation and by virtual sensor.

These processes can be disabled and modified independently from each other.

Note: There may be several types of aggregation in parallel. For example: aggregation of speed and length every 20 sec (real time) and aggregation of classified data every hour (deferred time). There shall be at least two types available.

Note: the deliverable 2.4.1.4 describes the Datex II message that constitutes the results of those computations.

Note: some C-ITS stations can be excluded from the computation, based on the station type ; this shall be configurable

#### Parameters:

- the spatial aggregation zone (virtual sensor)

Note: the precision of the GPS is between 1 and 20 m, so the distance AB (see Illustration 5) must be larger than 20 m. The CAM generation frequency is inferior to 1000 ms, therefore, the distance BC shall be higher than:

25 m at 90 km/h

36 m at 130 km/h

Note: in the future, the parameters of these zones could be sent in a Datex format, by a central server (platform, or other...) - see deliverable 2.4.1.4

- the aggregation period,
- activation or not for each calculation (boolean)
- the configuration for the data processing algorithms that will be performed by the R-ITS-S
- the class of vehicles length. For example, the length classes are defined on the SIREDO system (French computerized data retrieval system) into 4 classes with the limits: 0; 6; 7; 9; 25.5. The length intervals can contain more classes, with a maximum of 6 classes that the software can define by the necessary 5 thresholds.

Note: All the parameters can be different from one aggregation to another.

- types of station that shall be excluded from the computation (e.g. stationType = 15 to exclude R-ITS-S; stationType = 0 to exclude unknown stations ; stationType = 9 or 10 to exclude Vro-ITS-S, that might have driving manoeuvres different than regular vehicles)

#### 5.1.1.2.5 VERIFY THE CAM AUTHENTICITY

This function corresponds to verifying the trusted authority's certificate and the message signature.

It should be taken into account that this verification will be done based on the complete certificate received in some CAM.

Every received CAM is verified.

Note: The security systems in SCOOP, is described in the deliverables [2.4.4.1 to 2.4.4.8]. The deliverables [2.4.4.6bis] and [2.4.4.8] describe the process of the message's signature verification by using TSL and CRL.

#### 5.1.1.2.6 PROCESS THE AGGREGATED CAM DATA

This involves applying any kind of process to the already aggregated data, based on the operator's desire, in order to produce the necessary information to operate the SCOOP - A1 service.

The R-ITS-S will translate into a DATEX II v2.3 message the aggregated data, and encapsulate it into a SOAP envelope. See deliverables 2.4.1.4.

#### 5.1.1.2.7 MAKE AVAILABLE THE PROCESSED DATEX II DATA

The processed data used to produce the SCOOP - A1 service are made available to third party systems (especially the platform) for subsequent use (real time, batch mode, studies, archiving, etc.) through this function.

This directory must be accessible by remote or local access. (For example, the data can be stored in a file directory in the R-ITS-S)

#### 5.1.1.2.8 SEND THE PROCESSED DATEX II DATA

The function sends the aggregate information in a Datex II v2.3 format directly to the platform. In this case, the web-service (with a SOAP envelope) will be used in the “push on occurrence” mode with acknowledgement of receipt.

In the case of useful real-time information for the operator, the information is sent directly to the platform on a regular basis. By default, the period can be set to 6 minutes. There shall be two upload frequency parameters, that will be configured for each type of aggregation (see 5.1.1.2.4 ). Mostly, one will be dedicated to real-time uploads, one to deferred uploads.

Note: In the case of statistical post-processing, the operator may choose between storing and providing this data via an occasional direct request from the platform and sending the information regularly to the platform (by default, every night at 1:00 am).

#### 5.1.1.2.9 ADJUST THE PARAMETERS

This function makes it possible to modify the rules and algorithms used to consolidate and aggregate the data collected via the CAM messages received by a R-ITS-S. This adjustment conditions the type of data transmitted subsequently to the Platform. This function also lets the operator choose the settings that will be applied to the aggregated traffic data retrieved from the road-side equipment in order to produce the relevant information in the context of the SCOOP - A1 service.

The parameters shall be modified remotely or in a local way.

The parameters should be at least:

- number of aggregations
- for each aggregation type
- period of aggregation
- spatial aggregation zones (virtual sensor) concerned:
  - size,
  - position (3 (or 4) points to define a rectangle)
  - heading of the zone
  - precision of the heading
- data to aggregate,
- number and terminals of length classes; (defaults values: number: 4 classes, terminals: 0; 6; 7; 9; 25.5),
- Boolean: filter the stationTypes to exclude in the CAM aggregation
- frequencies of data retrieval (Default value = 6 minutes)
- period of data disposal (Default value = 24h)
- Hour of data disposal (Default value = 01:00 am)
- Datex II settings
- period of storage of CAM in LDM (seconds)
- limit of storage of CAM (default value 16Mb)
- others filters
- SOAP parameters

- IP addresses

## 5.1.2 Process DENM received from the ITS stations

### 5.1.2.1 Situation

A DENM is sent from a user or operator V-ITS-S.

The R-ITS-S receives the DENM.

If it is relevant, the R-ITS-S sends the information to the platform in a Datex II v2,3 format.

This function refers to receiving and understanding the DENM messages transmitted by the vehicles. It also involves knowing what to do with the information contained in each message and to apply the rules accordingly to the received DENMs.

### 5.1.2.2 Functions

The UML type diagram hereafter explains the functions implemented through the A2 and A3 SCOOP use-cases.

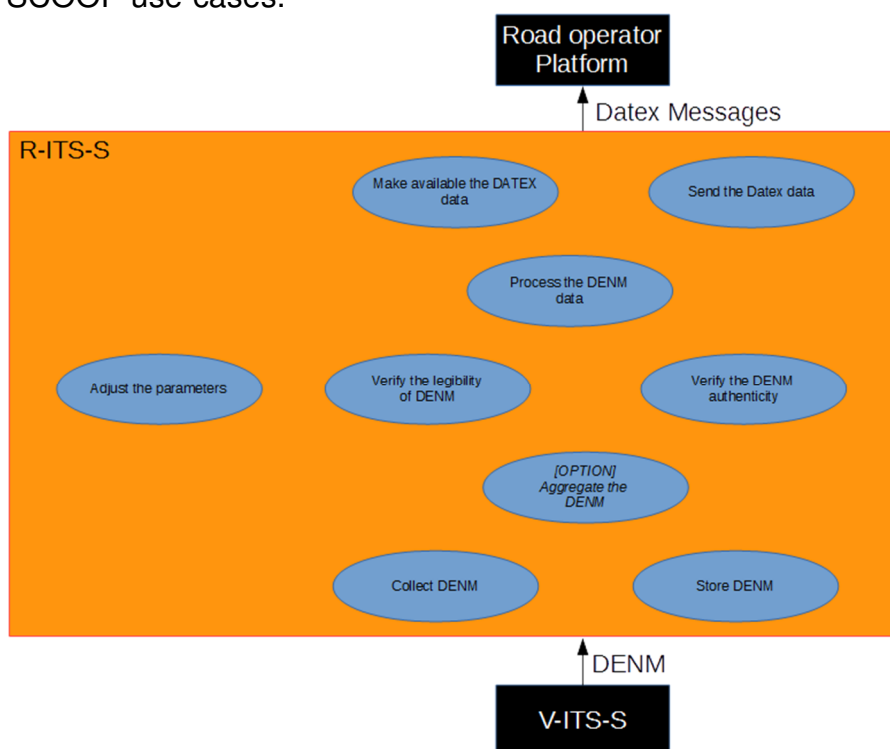


Illustration 6: R-ITS-S functions about DENM

#### 5.1.2.2.1 COLLECT DENMs

This function refers to receiving and understanding the DENMs transmitted by the vehicles. It also involves knowing what to do with the information contained in each message and to apply the rules accordingly to the received DENMs.

The specific characteristics of the contents of DENMs and their transmission frequency and conditions depend on the vehicle's situation and the configuration of its communication system. See SCOOP deliverable [2.4.1.2: DENM Parameters].

#### 5.1.2.2.2 **STORE DENMs**

This function stores the relevant DENM information, according to a configurable storage time, with a configurable storage space constraint.

The storage of a DENM consists in adding a new entry in the database for the DENM.

In some cases it can consist in modifying an already present entry:

- If the received DENM is a cancellation of a DENM already in the database, the DENM is deleted from the database.
- If the received DENM is a cancellation of an unknown DENM, the received DENM is ignored.
- If the same DENM is already present in the LDM, the message is ignored (same actionID, same DetectionTime)
- If the same DENM is already present in the LDM, but some data are updated, the message is updated in the LDM (same actionID, same eventype, different detectionTime, different referenceTime, different termination, different eventPosition...)

Note: the negation DENMs shall not be taken into account.

The expired DENM messages in the database can be deleted.

If the number of messages in the database exceeds a storage limit defined by the operator, the oldest or the less important DENMs will be deleted and replaced by the more recent DENMs. A message shall also be sent to the operator in order to inform him of the problem. Moreover, the log files will be completed with the information.

The storage space reserved for post-processing will also store all the processed received DENM, from the last transmission of aggregated post-processing information to the platform.

The storage space reserved for project validation can also store all received DENM.

#### 5.1.2.2.3 **VERIFY THE LEGIBILITY OF DENM**

This function concerns verifying the legibility of the messages received, which corresponds to the transmission of a DENM message. The function consolidates the ability to identify an incomplete DENM that can not be processed and to know how to process it. If the DENM message has already expired, ( $\text{detectionTime} + \text{validityDuration} < \text{Now}$ ) the message is ignored.

This function is included in the preceding one - the consolidation of information from the DENMs - and involves in particular verifying redundancy: several DENMs sent by the same vehicle and related to the same event should only be taken into account once.

By default, the Local Dynamic Map (LDM) type module, via the "Information Management" module, can filter the messages:

- based on their legibility/completeness; in particular, the R-ITS-S shall check the messages based on their completeness according to the deliverable 2.4.1 mandatory data elements.
- based on their uniqueness (thanks to the actionID block of the container Management, if the message isn't a cancellation or termination);

#### 5.1.2.2.4 [OPTION] AGGREGATE THE DENM DATA

This involves consolidating and aggregating the information collected from the DENMs transmitted by different vehicles to produce usable event-based information for the SCOOP - A2 or A3 service.

By default, upon receiving a DENM message, the data could be consolidated depending on the eventType as follows:

- if two DENMs are in the same geographical area, with the same causeCode/subCauseCode, they can be considered as the same.
- wait for a certain number of message before sending it to the platform.

This functionality will not be implemented in the R-ITS-S for the SCOOP project.

#### 5.1.2.2.5 VERIFY THE DENM AUTHENTICITY

This function corresponds to verifying the certificate used to sign the DENM message sent by the vehicle, in order to ensure the authenticity of the source of these data.

The authentication of messages makes it possible to then verify the validity of the DENM message, by following two security steps:

- the trusted authority that generated the vehicle's certificate passes the verification process and is accepted, and
- the message authenticity and integrity pass the verification process: its signature is verified using the authority's public key, verified in the preceding step.

Note: The security systems in SCOOP, is described in the deliverables [2.4.4.1 to 2.4.4.8]. The deliverables [2.4.4.6bis] and [2.4.4.8] describe the process of the message's signature verification by using TSL and CRL.

#### 5.1.2.2.6 PROCESS THE DENM DATA

This involves applying any kind of process to the already consolidated event-based information, based on the operator's desire, in order to produce the necessary information to operate the SCOOP – A2 and A3 services.

The R-ITS-S will translate into a DATEX II v2.3 message the data, and encapsulate it into a SOAP envelope. See deliverable 2.4.1.4.

#### 5.1.2.2.7 MAKE AVAILABLE THE PROCESSED DATEX II DATA

The processed information used to produce the SCOOP – A2 and A3 services are made available to third party systems (especially the platform) for subsequent use (real time, batch mode, studies, archiving, etc.) through this use-case.

This directory must be accessible by remote or local access. (For example, the data can be stored in a file directory in the R-ITS-S.



#### 5.1.2.2.8 SEND THE PROCESSED DATEX II DATA

The function sends the information in a Datex II v2.3 format directly to the platform. In this case, the web-service (with a SOAP envelope) will be used in the “push on occurrence” mode with acknowledgement of receipt.

Note: on request by the road operator platform, the R-ITS-S can also send a snapshot of all the stored events

#### 5.1.2.2.9 ADJUST THE PARAMETERS

This function makes it possible to modify the rules and algorithms used to consolidate and aggregate the data collected via the DENM messages received by a R-ITS-S. This adjustment conditions the type of data transmitted subsequently to the Platform.

The parameters should be at least:

- eventTypes of the DENM to collect
- Setting for storage: period of storage of DENM (seconds) or priority in informationQuality or priority causeCode/subCauseCode
- Limit of storage of DENM (default value 16Mb)
- period of data disposal (Default value = 24h)
- Datex II settings

### 5.1.3 Forward received DENM messages

#### 5.1.3.1 Mechanism

The Forwarding mechanism is to send a received message automatically to other C-ITS stations. Several algorithms coexist and are described in the DENM and GeoNetWorking standards.

The R-ITS-S must use the algorithm “Simple Geonet forwarding”, in the network and transport layer.

Note: The R-ITS-S can implement other algorithms mentioned in the standards, but it is not mandatory in SCOOP project (, CBF, Advanced Forwarding...)

Note: as mentioned in deliverable 2.4.1, the Keep Alive Forwarding shall not be in use.

#### 5.1.3.2 Parameters

Parameters at least:

- Activate/deactivate the forwarding in the application layer
- Optional: Choose the algorithms used by the R-ITS-S



## 5.2 Distribute messages to users of the road network

### 5.2.1 DENM from the platform

#### 5.2.1.1 Situation

This function produces the necessary information to operate the SCOOP – B, D, E services based on the DENM.

A situation or an event is sent by the platform to the R-ITS-S in a DATEX II format, which, if it's relevant, sends the processed information as a DENM to the C-ITS stations on the road.

See Deliverable 2.4.1.4 for more information about Datex syntax and translation.  
See Deliverable 2.4.3.2 for more information about the platform.

#### 5.2.1.2 Functions

##### 5.2.1.2.1 COLLECT A DATEX II MESSAGE

This involves receiving the data and, for each, recognizing and extracting the DATEX II message.

(For example, remove the soap envelope)

The R-ITS-S should check the value "SOURCE" or < nationalIdentifier> in its database, to be sure of the source of the message.

##### 5.2.1.2.2 TRANSLATE THE DATEX INFORMATION IN DENM

This use-case involves transforming the information contained in the DATEX II message and cross-tabulating it with the R-ITS-S's settings (position, SCOOP services activated, time, configuration according to deliverable 2.4.1.2, etc.) in order to develop the corresponding DENM message that should be sent to users.

This shall be done according to the SCOOP Deliverable 2.4.1.4. Some extracts mentioning some vigilance points are mentioned below :

- *The "Linear" elements inside the "GroupofLocation" in the DATEX message sent by the platform will contain enough coordinates points for the R-ITS-S to send complete "trace" and "eventHistory" attributes in the DENM*
- *The units used are different (tenth of a micro-degree for DENM, decimal degree for DATEX II).*
- *Whereas the different geographic locations, which are part of a trace or an event history, are defined in DENM by difference with the previous location ("deltas"), DATEX II defines point locations by geodetic coordinates (latitude and longitude) separately.*

##### 5.2.1.2.3 STORE THE DENM

This function is the same as in 5.1.2.2.2 .Store DENMs.

It consists in adding or removing the relevant information in the LDM.

#### 5.2.1.2.4 SIGN A DENM

The sent messages must be signed before transmission, it means that the R-ITS-S must add an encrypted certificate to the message and sign with it.

Note: The security systems in SCOOP, is described in the deliverables [2.4.4.1 to 2.4.4.8]. The deliverables [2.4.4.6bis] and [2.4.4.8] describe the process of the message's signatures.

#### 5.2.1.2.5 SEND A DENM

This involves, for each road-side equipment, transmitting the signed DENM when it is relevant, to the others users via ITS-G5. For each eventType, frequency and duration are set in the parameters, along with the parameters mentioned in deliverable 2.4.1.2.

#### 5.2.1.2.6 OTHER FUNCTIONS

For the R-ITS-S and platform exchanges, the web-service (with a SOAP envelope) will be used in the "push on occurrence" mode with acknowledgement of receipt.

Furthermore, regularly, R-ITS-S or platform can request a snapshot to the other. It means requesting a Datex II message that contains all the situation present in the database. For this exchange, the web-service (with a SOAP envelope) will be used in the "pull" mode.

If the exchange fails or if there is no answer, the requester must request again.

For example, Platform and R-ITS-S must request a snapshot at a regular period, or at a start-up.

Note: The platform must know the state of the R-ITS-S: status, URL, position. Those data are settings in the platform.

#### 5.2.1.2.7 ADJUST THE PARAMETERS

These functions let the operator adjust the translation modalities for event-based information entering the road-side equipment as DENM to be broadcast to users.

Parameters:

- URL of the platform
- Datex II settings ("nationalIdentifier", ...)
- Frequency and time of the snapshot to the platform (default value = 24h at 01:00 am)
- Frequency of request after failure

### 5.2.2 [optional] DENM from the HMI (local or remote)

The R-ITS-S can have a HMI accessible for an authorised operator by local (Ethernet or USB connection) or by remote access (on the supervision centre for example).

With this HMI, the operator can create any message (DENM, ...) provided in the SCOOP specifications. Any element of the DENM Data Frame mentioned in deliverable 2.4.1.2 could be changeable, along with the eventposition, traces and eventhistory.

### 5.2.3 CAM-I

The R-ITS-S does not send CAM, but CAM-I to others C-ITS stations.

The data-frames of CAM-I are specified in the following deliverables:

- SCOOP Deliverable 2.4.1: Common specifications,
- SCOOP Deliverable 2.4.1\_Appendix1 Renewal of pseudonym certificates and upload of Logs (T-Logs and U-Logs)

The CAM-I must be sent to a configurable frequency (default value = 2 messages in a second, one for each proposed service – see chapter 5.4 )

### 5.2.4 Secure sent messages

#### 5.2.4.1 Sign a sent message

See DENM standards and SCOOP deliverables [2.4.4.6bis] and [2.4.4.8] for the exact explanation. Some parts are reproduced below.

- *Secured messages are built in Geonet Layer and transmitted to the security layer.*
- *Different cryptographic algorithms are used. Among, the Elliptic Curve Digital Signature Algorithm (ECDSA) which is used for the signature of messages (CAM, DENM, CAM-I) with keys of size 32/64 bytes.*
- *A certificate indicates its holder's permissions, i.e. what statements the holder is allowed to make or privileges it is allowed to assert in a message signed by that certificate. The format for the certificates is specified in ETSI TS 103 097 [i.17].*

#### 5.2.4.2 Add the R-ITS-S certificate to some messages

The R-ITS-S must add its certificate to all CAM-I messages.

The R-ITS-S must add its certificate to all DENM.

## 5.3 Security of the R-ITS-S

The R-ITS-S must be able to

- download its certificates from the PKI servers
- manage the certificates pool and change from one pool to another
- manage the certificates, and change from one certificate to another

See chapter HSM for more information about the process in the HSM  
See deliverable [2.4.4.8] for details on the certificate management.

## 5.4 Facilities for the Vru-ITS-S

All the facilities offered to Vru-ITS-S by a R-ITS-S are announced in its CAM-I.

Note: it is possible that a R-ITS-S offers no such facility (for example a R-ITS-S connected with a 3G connection to the servers) ; it should be configurable for the functions of relay of security messages and logs download.

### 5.4.1 Relay security messages between Vru-ITS-S and PKI

If the facility is available for the R-ITS-S, the requests for certificates for the Vru-ITS-S will flow through the R-ITS-S. See Deliverable [2.4.4.8] for more information. Some extracts of the processes are presented below:

- *The R-ITS-S relays the LTC request from the Vru-ITS-S to the PKI server and response from the PKI to the Vru-ITS-S.*
- *The R-ITS-S relays the PC request from the Vru-ITS-S to the PKI server and response from the PKI to the Vru-ITS-S.*
- *The R-ITS-S relays the Get CRL request and the response.*
- *The R-ITS-S relays the Get TSL to the DC and the response.*

The availability will be declared in the Service Advertisement Container: the Advertised Service ID is set to 0 if PKI service is supported.

### 5.4.2 Upload T-log/U-log from Vru-ITS-S

If the facility is available for the R-ITS-S, the T-log and U-log will flow to the R-ITS-S. The Vru-ITS-S will upload its log file on the R-ITS-S, through the address presented in the CAM-I. The R-ITS-S stores the information.

The R-ITS-S makes it available for the logs server or sends it to a specific server at a configurable frequency.

The R-ITS-S does not modify or open these files.

The availability will be declared in the Service Advertisement Container: the Advertised Service ID is set to 1 if upload log service is supported.

The process is specified in SCOOP Deliverable [2.4.1\_appendix\_1: Renewal of pseudonym certificates and upload of Logs (T-Logs and U-Logs)]

### 5.4.3 Send road tolling positions to Vru-ITS-S and Vro-ITS-S

These CAM-I messages are also used for advertisement of DSRC road tolling.

The road operator can inform of its own road tolling positions in its CAM-I. The filling-up for the R-ITS-S is left up to the discretion of each road operator.

The V-ITS-S will implement the reception mitigation techniques after the reception of the message. When the V-ITS-S passes in an area presented in the CAM-I, the V-ITS-S must reduce its power transmission.

The R-ITS-S shall be able to send up to the maximum number of toll positions that the CAM-I message allows. It shall be configurable

Note: it is not an obligation for the road operator but he can also indicate other road tolls than his own.

The availability will be declared in the data-frame: Protected Communication Zone R-ITS-S: Data elements for Toll collect protection (See details in the mitigation standards and in SCOOP Deliverables 2.4.1 and 2.4.1.1)

## 5.5 Internal R-ITS-S management:

### 5.5.1 R-ITS-S Start-up

When the R-ITS-S starts, it shall:

- launch all the internal processes (BIOS, OS, check memory, supervision ...)
- launch the security processes (check/update certificates...)
- launch all the C-ITS processes (send/receive CAM/DENM/CAM-I...)
- signal its presence to the platform with a keep-alive message
- request a snapshot of the events to the platform

### 5.5.2 R-ITS-S Shut-down

When the R-ITS-S stops, it shall:

- wait for the end of the ongoing processes (during a maximum configurable time) and stop all the C-ITS processes (send/receive CAM/DENM/...)
- archive and store data
- send all the data to the platform:
  1. the processing of still valid DENM messages,

2. the real-time CAM processing,
  3. the processing of expired DENM messages,
  4. the T-logs,
  5. the U-logs,
  6. the batch-mode CAM processing,
  7. the message history
- wait for the end of the ongoing processes (during a maximum configurable time) and stop all the internal processes (BIOS, OS, check memory, supervision ...)

### 5.5.3 Data management

The databases (and especially the LDM) delete the expired events regularly. If the number of data received exceeds a storage limit defined by the operator, but that can be taken by default as 16 Mb, the least important events starting with the oldest will be deleted. The problem will be stored in the R-ITS-S log files to be sent to the supervision server.

### 5.5.4 Data protection

The Hardware Security Module is a case that self-erases its data if it is handled physically. (See chapter 3.1.2. Hardware Security Module).

### 5.5.5 Connection

#### 5.5.5.1 With the platform

Regularly (in a configurable way), the platform will send messages called “keep-alive” to ensure the connection of the R-ITS-S to the platform.

Parameter:

- the frequency at which the R-ITS-S will ask a snapshot from the platform (24h);

#### 5.5.5.2 With the PKI system

See SCOOP Deliverables [2.4.4] for details.

#### 5.5.5.3 IPV4/IPV6

The communication between On Board Units over ITS-G5 is specified over Geonetworking and over IPv6, not for IPv4. However, road operators' networks used IPv4 technology. The Road Side Units shall then mount TLS tunnels over IPv4 networks of road operators to reach a hosting company. The latter has two connections to the Internet, one in IPv4, another in IPv6. Thus, the TLS tunnel can be used to transport IPv6 traffic over IPv4 networks.

See SCOOP Deliverable [2.5.3.2.1]

## 5.5.6 Supervision (local and remote access)

### 5.5.6.1 Real time monitoring

Real time monitoring of malfunctions of the different components and modules must be done remotely, and by local access.

Remotely, it should be done via the SNMP v3 for managing a Management Information Base (MIB). It must also be possible to monitor the R-ITS-S's own module as a web page.

It should be possible to connect directly to the external connectors provided for this purpose and to access the same HMI or web page access. This will be used, for example, in case there are communication problems with the supervision server, or during the first installation of the R-ITS-S.

The list of the components to monitor is, at least, each material systems described in 3.3.2 . Monitoring sensors. The operator must see the status of each element, and the monitoring shall also provide an alarm system for all sensor states for a certain time. It should be possible to parameter those alarms. By default, only the battery status can trigger an alert at the monitoring level.

### 5.5.6.2 Maintenance and debug

Moreover, all the malfunctions and all the different operating states of the components must be traced in a log file, generated and stored in the R-ITS-S:

- time and date,
- component identifier,
- component name/function,
- component state (no response, defective, OK); for the process, the "OK" state will be replaced by the use of hardware resources as a percentage,

This log file shall be readable remotely, and by local access.

## 5.5.7 Configuration, (remote and local access.)

### 5.5.7.1 Time consideration

The time synchronisation is very important in the ITS projects.

The R-ITS-S shall be timed synchronised.

- For this purpose, it can use an NTP server, which will broadcast the temporal synchronisation in client-server mode to the NTP client installed in the R-ITS-S.
- The R-ITS-S can also use the GPS timer to do this synchronization.

This synchronisation must be done regularly by the R-ITS-S.

Whatever the way the R-ITS-S time is synchronized, R-ITS-S shall communicate to the vehicle with the timestampITS, and to the platform with the UTC time.



The algorithm is like this:

- $\text{timestampITS} = \text{UTC}(\text{system}) - \text{UTC}(01/01/2004) + \text{_(intercalary seconds since 01/01/2004)}$

The intercalary seconds since 01/01/2004, are computed using the best way possible: from the GNSS, or by manual configuration,

Note: The time to use in the Datex messages is set in SCOOP Deliverable 2.4.1.4

Note: A tolerance on times (3 seconds on the CAM and 60 seconds on the DENM) is required to make it possible to compensate the possible delays of integration of the leap seconds by the different partners. The R-ITS-S must manage this tolerance for input messages.

### 5.5.7.2 Parameters

When the R-ITS-S is installed at a new site, the R-ITS-S's initial configurations have to be set. This configuration can only be done with a local access.

This configuration includes at least:

- the connection and addressing options (IP addresses, gateway, selected ports, etc.) for all the servers:
  - the Long-Term Certificate Authority (LTCA),
  - the Pseudonym Certificate Authority (PCA), in charge of transmitting the certificates for the R-ITS-S,
  - the platform,
  - the supervisory system,
- the RCA (root certificate authority), LTCA and PCA certificates and public keys,
- the pseudonym certificate and the related public and private keys,
- the pair of Public and Private Tracing Keys (TPK/TSK) and related user interface, and the R-ITS-S's long-term certificate (LTC) and the related public and private keys
- the identification of the R-ITS-S, including a user name (set by the operator, it can be the Datex "nationalIdentifier", or it can be part of it.),
- the 3 parts of the Datex "nationalIdentifier" (see deliverables 2.4.1.4 for the details)
- the leap seconds.

A software for back-up must be installed: this will make it possible (upon a special command from the R-ITS-S monitoring) to independently perform at any time the following actions:

- manage a new identifier, and
- reset all parameters to default (but not the initial configurations);



Once this first configuration is done, all the others configurations should be available remotely and on a local access.

The R-ITS-S customization for the processes depends on the use-cases installed in the R-ITS-S.

All the parameters described above could be accessible for the configuration process and should be set to their default value during the first installation:

- 5.1.1.2.9 CAM parameters
- 5.1.2.2.9 DENM parameters
- 5.1.3.2 Forwarding DENM parameters
- 5.2.1.2.5 Platform parameters
- 5.2.3 CAM-I parameters
- Validation parameters:
  - [validation]: the frequency of LOG files (monitoring file, user log and technical log) for the R-ITS-S on the platform;
- Supervision parameters:
  - [supervision]: for each component the level to trigger the monitoring alarm; (default value: activated for the battery at 25%. deactivated for the others components)
- General parameters:
  - [general]: sizes (or proportions of total storage space) of storage space reserved for real time and post-processing;
- Fail-soft modes see 5.5.9 :
  - [fail-soft mode]: the number of messages not included over a defined period, also configurable;
  - [fail-soft mode]: the number of new messages included over a defined period, also configurable;
  - [fail-soft mode]: the battery's low charge; (25%)
  - [fail-soft mode]: the battery's very low charge; (10%)
  - [fail-soft mode]: the time per use-case during which the DENM transmission is kept; (10 min)
  - [hsm] boolean: Activate/deactivate the self-destruction (activate)
  - [hsm] Time before self-destruction after an unsecured event is detected. (0 sec)

The configurations will be modifiable from the supervisory system and then stored locally in the R-ITS-S.

A tool shall be able to modify these parameters directly in the R-ITS-S. The modifications will then be sent to the supervisory system for back-up.

### 5.5.7.3 Software updates

All pieces of software must be able to be updated remotely and on a local access, independently from each other.

## 5.5.8 T-log

The R-ITS-S shall create its own T-logs.

All the log files must be accessible remotely and on a local access.

T-log are described in the SCOOP deliverable: [2.4.1.3: Road Operator Tlogs], [2.4.1.3-LOGGestionnairesASN1] and in [2.4.1.3-CataOfDataTlog]. Some parts are reproduced below:

- *The R-ITS-S detects a new event. Its generated a record, and encoded it in an UPER format.*
- *The record is set in the R-ITS-S T-log file.*
- *At a certain period, or at a certain T-log file size, the file is closed.*
- *The T-log file is sent to a server.*

Some T-logs contains personal data. The others T-logs can be used for statistics, or supervision by the road operator. It implies two different processes for the two types of T-logs. For example, the first must be removed as soon as they have been sent to the analyst server, whereas the others can be stored a long time and accessible for the road operator.

The up-to-date list of T-logs accessible by the road operator owner, is:

- TLog-RSU-CAMI
- TLog-RSU-DENM-Sent
- TLog-RSU-NetworkAccessPerformances
- TLog-RSU-Datex2Reception
- TLog-RSU-Datex2Sending
- TLog-RSU-GeneralWorking
- TLog-RSU-ModulesWorking
- TLog-RSU-Radio
- TLog-RSU-Configuration
- TLog-RSU-ObjetsPKI
- Tlog-RSU-Faulty message

The T-Logs shall be regularly sent at a configurable frequency to the appropriate repositories (public or private) on the supervision server.

The activation of each T-Log shall be configurable.

## 5.5.9 Fail-soft modes

### 5.5.9.1 General points

The SCOOP platform does not include a road-side equipment monitoring tool. Consequently, technical alert and fault messages are sent to a monitoring tool dedicated to the R-ITS-S.

For each fault, a record is entered in the monitoring logs and maybe in a T-log file.

All reported messages and alerts are saved as new entries in the monitoring logs.

#### 5.5.9.1.1 MEMORY

The internal memory is organized such that the real-time traffic information (event messages, and recent traffic messages) and the post-processed traffic information (deferred time traffic messages) are stored in two different spaces. Consequently, the saturation of the first storage space will not impact the second storage space.

If one of the storage spaces becomes saturated, the oldest information will be erased first in order to free up the necessary memory to store the new incoming data.

#### 5.5.9.1.2 RETURN FROM FAIL-SOFT MODE

The messages processed and stored by the R-ITS-S will be sent to the platform based on the following order:

1. the processing of still valid DENM messages,
2. the real-time CAM processing,
3. the processing of expired DENM messages,
4. the T-logs,
5. the U-logs,
6. the batch-mode CAM processing,
7. the message history.

The return from fail-soft mode will then be affected by sending a keep alive, then a Datex II snapshot request that can restore the entire map of events, i.e. snapshot (and thereby update all the information to send).

Upon return from the fail-soft mode, the R-ITS-S downloads all of its configuration parameters

### 5.5.9.2 Internal problems

#### 5.5.9.2.1 RECEIVER FAULT

If the transceiver receives non-understood signals continuously (number of messages over a lapse of time - configurable), the R-ITS-S continues to transmit, but no processing is carried out until the signals are once again understood continuously (number of messages over a lapse of time - configurable). This may be due to interference around the R-ITS-S.

On demand from the monitoring, the dual antenna can also manage the message transmissions based on one or the other of the antennas, either reserved for the CCH (for the CAM and DENM) or for the SCH1 (for all other information).

#### 5.5.9.2.2 TRANSMITTER FAULT

If a transmitter is non-functional, the second transmitter can supersede it, while respecting the R-ITS-S' priority of functionalities.

In the event of a technical fault on one of the transmitters preventing the transmission of signals, the second transmitter must be able to take over.

If no transmission is possible, all of the information that should normally be transmitted is stored until it is no longer pertinent : in all cases it is recorded in the log file containing all of the CAMs and DENMs as well as the reason they were not sent, if known.

#### 5.5.9.2.3 POWER SUPPLY FAULT

Depending on the power supply mode, when the battery charge is very low (configurable) or a power supply outage is detected:

- backups are launched in order to prepare a secure shut-down of the R-ITS-S,
- the R-ITS-S is shut down in a secure manner.

On an autonomous power supply, when a low battery charge (configurable) is detected:

- DENMs are no longer passed on,
- the messages flowing through the SCH1 are no longer processed

#### 5.5.9.2.4 COMPUTING UNIT FAULT

When the computing unit indicates an operation in fail-soft mode (e.g., due to a software error), it records the cause in the log, if known.

Some tasks can then be suspended.

### 5.5.9.3 External problems

#### 5.5.9.3.1 LINK WITH THE PLATFORM INTERRUPTED

If the link between the R-ITS-S and the platform is interrupted:

- the R-ITS-S continues to send all of the DENMs to V-ITS-S, over a configurable period for each use-case. If the DENM does not end before, the default value is 10 minutes;
- all DENM and CAMs and the post-processing calculations are stored. The storage must remain functional at least 72 hours after the beginning of the fault.

If the link between the R-ITS-S and the platform is interrupted while the software is downloading an update, or updated or configured, the R-ITS-S makes a new request to restart the interrupted operation at a configurable frequency, if possible.

When the connexion is operational again, R-ITS-S and platform will only use snapshot in a "pull" mode to refresh their databases. It means:

- the platform can ask a snapshot of all data, the R-ITS-S must answer with one (or more, if necessary) Datex message including all the information of the LDM;
- the R-ITS-S can ask a snapshot to the platform, the platform must answer with a Datex message including all the valid events for this R-ITS-S.

### 5.5.10 Validation of the system

Tests will be implemented to technically and functionally validate the R-ITS-S: the software part must allow these tests to be defined. (see deliverables 2.3.1 and 2.6). An upper tester must be delivered with the product.

And an access to any command useful for those verification must be given to the authorised operator.