

French C-ITS Deployment Coordination committee

R-ITS-S specifications

Deliverable 2.4.2.1_H

Activity 2 : Studies

Sub Activity 2.4.2

Version 4.00

Publication date: 14/11/2019



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

The contents of this publication are the sole responsibility of the SCOOP@F project consortium, C-ROADS France project consortium and InterCor project consortium (French beneficiaries only) and do not necessarily reflect the opinion of the European Union.

Information on the document

Document: R-ITS-S specifications

Date of publication: 14/11/2019

Responsible, Entity: Jean François RIZZO, Cerema

Status: Version 4.00

Publication history

Date	Version	Author(s)	Updates & changes	Diffusion
14/11/2019	4.00	Atika MENHAJ Emilie PETIT Eric PILLET Fouzia BOUKOUR Jean François RIZZO Ludovic HOARAU Valérie LABICHE Valérie LERAY	Consolidated version for release 4 Release 4	Release 4

Quality rules

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

Requirements identification& traceability

In this document, the following verbal forms are used to indicate requirements: **Shall / Shall not**

Recommendations shall be indicated by the verbal forms: **Should / Should not**

Permissions shall be indicated by the verbal forms: **May / May not**

Possibility and capability shall be indicated by the verbal forms: **Can / Cannot**

Inevitability used to describe behavior of systems beyond of the scope of this del. shall be indicated by: **Will / Will not**

Facts shall be indicated by the verbal forms: **Is / Is not**

In the table here below:

2.4.X.XX> is the number given to the deliverable (e.g. 2.4.4.8)

YYYY > for digit are given to identifying which component/entity the requirement is addressing (e.g. LTCA for long terme certificate authority)

ZZZ > is the numeration of the requirement

ID	2.4.X.XX-YYYY-ZZZ
Component(s)	(e.g) ITSS-VU, ITSS-VRO, ITSS-R, PKI
Requirement	(e.g) An ITS station SHALL be able to request and get a Long term Certificate (LTC) from the SCOOP Public Key Infrastructure (PKI).
Acceptance	(e.g) CA1 : ITSS-VU sends a LTC request to the LTCA CA2 : ITSS-R relays the LTC request CA3 : The LTCA verifies the request and sends a response CA4 : The ITSS-R relays the response CA5 : The response is received by the ITSS-VU and is valid
Additional information	

Acronyms & abbreviations

BTP	Basic Transport Protocol
C2C-CC	Car2Car communications Consortium
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
C-ITSS	Cooperative Intelligent Transport Systems Station
DCC	Decentralised Congestion Control
DENM	Decentralized Environmental Notification Message
DP	DCC profile
DPID	DCC profile identifier
DSMIP	Dual Stack Mobile IP
DSRC	Dedicated Short Range Communications
GBC	Geo Broadcast
GN	Geo Networking
GPS	Global Positioning System
HST	Header Sub-Type
HT	Header Type
Hybrid Vru-ITS-S	Intelligent Transport Systems Station Vehicle User with ITS-G5 and cellular (3G/4G) connection
ITS	Intelligent Transport Systems
ITSS	Intelligent Transport Systems Station
ITS-G5	ITS-G5 is a European standard for ad-hoc short-range communication of vehicles among each other (V2V) and with Road ITS Stations (V2I). ITS-G5 refers to the approved amendment of the IEEE 802.11 (standard IEEE 802.11p). This technology (possibly others) uses the 5.9 GHz frequency band to support safety- and non-safety ITS applications. In this document ITS-G5 stands for IEEE802.11p/ETSI ITS-G5.
IVI	Infrastructure to Vehicle Information
IVIM	Infrastructure to Vehicle Information Message
LDM	Local Dynamic Map
LT	Lifetime
LTE	Long Term Evolution
MAP	Geometric information for the intersection
MAPEM	MAP (topology) Extended Message
MHP	Maximum Hop limit
National Central	French National Central Intelligent Transport Systems

ITSS	
NH	Next Hop
R-ITS-S	Intelligent Transport Systems Station Roadside
RSP	Wifi ITS-G5 Roadside System Profile (short also Roadside System Profile)
RWW	Roadworks Warning
s	Seconds
SCF	Store Carry Forward
SHB	Single-Hop Broadcast
SPAT	Signal Phase and Timing
SPATEM	Signal Phase and Timing Extended Message
TC	Traffic class
TCC	Traffic Control Centre
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-National
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Vehicle and/or Vehicle-to-Infrastructure
V-ITS-S	Intelligent Transport Systems Station Vehicle
Vro-ITS-S	Intelligent Transport Systems Station Vehicle Road Operator
Vru-ITS-S	Intelligent Transport Systems Station Vehicle User

Table of Contents

Quality rules	3
Acronyms& abbreviations	4
Table of Contents	6
List of figures	8
1 Introduction	9
1.1 Document contents	9
1.2 Standards and related references	9
2 General Points	11
2.1 Definitions	11
2.2 Environment	11
2.3 Main R-ITS-S Functionalities	12
3 Equipment	16
3.1 Main unit	16
3.1.1 Power supply module (optinal)	16
3.1.2 Hardware Security Module (HSM) (mandatory)	17
3.1.3 Memory (mandatory)	18
3.1.4 Computing unit (mandatory)	18
3.2 Telecommunication components	19
3.2.1 ITS-G5	19
3.2.2 Cellular network	21
3.2.3 Satellite network	21
3.3 Connections and sensors	23
3.3.1 External connection	23
3.3.2 Monitoring sensors	23
3.4 R-ITS-S Case	23
3.5 Antenna and module Bluetooth	24
4 Installation specifications	25
5 Software	26
5.1 Process received messages from V-ITS-S	27
5.1.1 Process received CAM	27
5.1.2 Process DENM received from the ITS stations	34
5.1.3 Forward received DENM messages	38
5.1.4 Verify the authenticity of a message	39

5.2	Distribute messages to users of the road network.....	40
5.2.1	DENM from the platform.....	40
5.2.2	CAM-I	43
5.2.3	Secure sent messages	43
5.2.4	IVI from the local platform.....	44
5.2.5	[optional] DENM and IVI from the HMI (local or remote)	46
5.3	Security of the R-ITS-S.....	46
5.4	Facilities for the Vru-ITS-S	46
5.4.1	Relay security messages between Vru-ITS-S and PKI.....	47
5.4.2	Upload T-log/U-log from Vru-ITS-S	47
5.4.3	Send road tolling positions to Vru-ITS-S and Vro-ITS-S.....	47
5.4.4	Relay messages from V-ITS-S to National Central ITSS, through Home Agent.....	48
5.5	Internal R-ITS-S management:.....	48
5.5.1	R-ITS-S Start-up.....	48
5.5.2	R-ITS-S Shut-down	49
5.5.3	Data management	49
5.5.4	Data protection	49
5.5.5	Connection	49
5.5.6	Supervision (local and remote access).....	50
5.5.7	Configuration, (remote and local access.)	51
5.5.8	T-log	53
5.5.9	Fail-soft modes	54
5.5.10	Validation of the system	56
5.6	Management of Bluetooth beacon.....	56

List of figures

Illustration 1: Architecture of the SCOOP project, from the point of view of R-ITS-S	12
Illustration 2: Different functionalities between fixed and mobile ITSS's	15
Illustration 3: ITS Station architecture	26
Illustration 4: R-ITS-S functions about CAM	28
Illustration 5: Description of a zone	30
Illustration 6: CAM reception orchestration	34
Illustration 7: CAM aggregation orchestration	34
Illustration 8: R-ITS-S functions about DENM	35
Illustration 9: DENM reception orchestration	38
Illustration 10: DENM orchestration	38
Illustration 11: DENM form the platform	41

1 Introduction

1.1 Document contents

This document compiles the technical specifications for the road-side unit communication equipment designated hereafter by R-ITS-S, which has to be installed as part of the French C-ITS projects (SCOOPv2, C-ROADS France and INTERCOR). These projects introduce the possibility to use cellular communications, in addition to the communication based on ITS-G5 in SCOOP wave1. Thus, resulting in a “hybrid” architecture combining cellular and ITS-G5 accesses.

These specifications 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 of the deployment sites may require adding additional 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. Furthermore, their reasons shall be detailed to the other partners and approved by the Steering Committee.

The extracts of deliverables present in this document may not be up to date (evolutions, retroactions) and consequently only the reference documents from which they come are authentic.

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].

The functions of the hybrid present in this document refer to the following deliverables:

- [2.4.1_H : Functional and technical hybrid architecture – Common specifications]
- [2.4.1.4_H : Specification of DATEX II v2.3 messages in conjunction with C-ITS messages]
- [2.4.1.2_H : Use Case]
- [2.4.1.5 : Network architecture for road operators]
- [2.4.2.4_H : National central ITS Station specifications]
- [2.4.3.2_H : Detailed functional specifications of SCOOP local SCOOP platform]
- [2.4.4.x series : Security, Certificate, Pki, ...]

The list of standards is described in the deliverable [2.4.1_H.bis: List of standards], the elements below are presented for information by family and in a non exhaustive way:

CEM/EMF tests (CE marking)

- EN 61000-6-2 : 2005 (industrial part)
- Draft ETSI EN 301 489-1 V2.2.0 : 2017 (general part)
- Final Draft ETSI EN 301 489-3 V2.1.1 : 2017 (GPS part)
- Final draft ETSI EN 301 489-52 V1.1.0 : 2016 (2G/3G part)
- EN 62479 : 2010 (EMF part)

Radio tests (CE marking)

- Draft ETSI EN 303 413 V1.1.1 : 2017 (GPS part)
- ETSI EN 301 511 V.12.5.1 : 2017 (2G part)
- ETSI EN 301 908-2 V11.1.1 : 2016 (3G)
- Collocation test for EU type examination
- ETSI EN 302 571 V2.1.1 (G5 part)

EU type examination according to Directive 2014/53 / EU (RED Directiv)

- EU type examination certificate

Electrical safety engineering

- EN/CEI 61010-1

2 General Points

2.1 Definitions

In this document, the following terms are used:

- R-ITS-S: also called RSU (Road Side Unit), it is an ITS station deployed on the side of the road network, called "UBR".
- V-ITS-S: also called OBU (On Board Unit) it is an ITSS station in a vehicle. Vru-ITS-S is in any vehicle, and Vro-ITS-S is in a Road Operator Vehicle.
- ITSS-C: French National Central ITS Station.
- HA: Home Agent it is an interface server between the National Platform and V-ITS-S

R-ITS-S have different functional types:

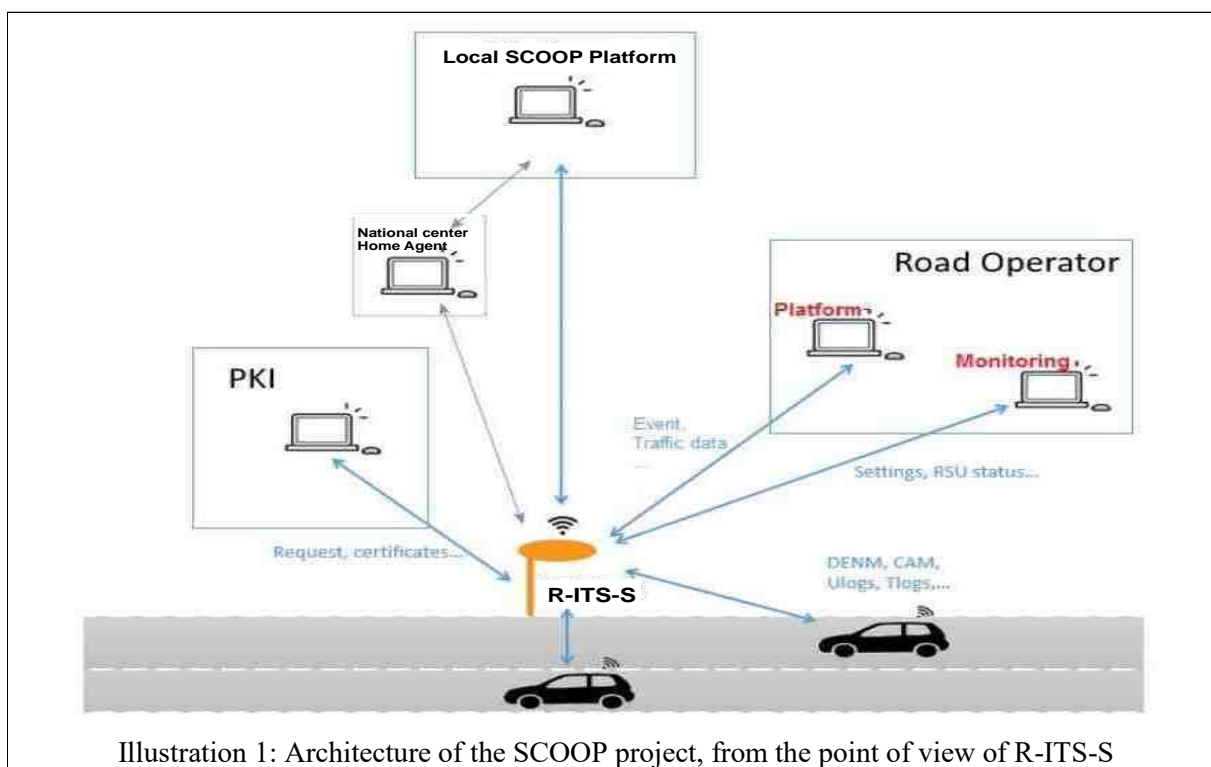
- Fixed R-ITS-S: ITS-S station on the side of the road. All the functions described in this document are implemented inside.
- Mobile R-ITS-S: Function of a Vro-ITS-S vehicle, that have only some of the functions described in this document (see chapter: [Main R-ITS-S Functionalities](#)).

2.2 Environment

This document calls on the description of the hybrid architecture described in the SCOOP deliverables [2.4.1_H : Deliverable Functional and technical hybrid architecture – Common specifications] and [2.4.1.5 : Network architecture of the SCOOP project for road operators]. The communication protocols used between the different elements are described in the same deliverable.

The architecture of the SCOOP project, from the point of view of R-ITS-S is presented in the figure below.

A R-ITS-S communicates with 5 different main entities: the Local SCOOP platform, the PKI, the Home Agent, the monitoring server and C-ITS vehicles.



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 (V-ITS-S and Vro-ITS-S)
 - make the translation of the CAM or DENM messages to DATEXII v2.3 messages
 - make the translation of DATEXII v2.3 messages received from the Local SCOOP Platform to IVI messages and DENM messages
 - forward messages to the ITS stations on the road network
- **distribute messages to users of the road network:**
 - from the Local SCOOP 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 the Vru-ITS-S and Vro-ITS-S
- send CAM-I to others R-ITS-S
- relay messages to National Central ITSS, through Home Agent

The supervision server must be able to update all the functions currently present in the R-ITS-Ss. These functions are specified in the chapter: [Supervision](#).
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, diary, 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
process received messages:		
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	X ^{Note}
make the translation of DATEXII v2.3 messages received from the Local SCOOP Platform to IVI messages	X	X ^{Note}
forward messages to the ITS stations on the road network	X	X ^{Note}
distribute messages to users of the road network:		
from the local SCOOP platform	X	X
from the HMI (local or central)	X	X ^{Note}
offer services to the V-ITS-S:		
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 Vru-ITS-S and Vro-ITS-S	X	
the CAM and DENM messages from the V-ITS-S are relayed by the home agent to the French National Central ITSS.	X	X ^{Note}
send CAM-I to others R-ITS-S	X	X ^{Note}
security management:		
download and management of the R-ITS-S certificates	X	X ^{Note}
update	X	X ^{Note}
internal management:		
protection of data (HSM, ...)	X	X ^{Note}
supervision and log file (local / remote)	X	X ^{Note}
configuration (local / remote)	X	X ^{Note}
update (local / remote)	X	X ^{Note}
T-log (local / remote)	X	X ^{Note}
management of degraded modes	X	X ^{Note}

functions or software to enable the validation of the R-ITS-S software (HMI, specific commands, diary, upper tester, etc.)	X	X ^{Note}
--	---	-------------------

Illustration 2: Different functionalities between fixed and mobile ITSS'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 Local SCOOP platform)
- the antennas (GNSS, ITS-G5, cellular, Bluetooth, ...), 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.

The maintenance and replacement procedures for the equipment must be described in the technical and usage documents of R-ITS-S.

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 communication unit (ITS-G5, cellular, ...) can be either partially remote (only the antenna - see chapter: [Antenna cable](#)) or totally remote (antenna and communication module).

The R-ITS-S, and all the components using the radiofrequency, shall respect the European directive about electronic device, RED. (see http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en for guides).

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 (optinal)

The power supply module must comply with the NF C15-100 standard including, in particular, the following components:

- TT networks (earthing)

The power supply can operate self feeding (example via Ethernet: Power over Ethernet (PoE)) or operate directly on the operator's electrical network. An independent power supply shall operate one quarter 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,
- autonomous operation: it shall be able to operate via an autonomous power supply the entire day without any power supply (e.g. battery, electric generator), connection on a solar panel (calibrated on the most unfavourable periods of the year) or with wind turbine.

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 12V 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 private keys like the critical security components
- perform cryptographic operations with the stored keys,
- support Cryptography algorithms (cited in ETSI TS 103 097: "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 this process, the R-ITS-S must perform them.

3.1.2.4 Functions not covered by 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)
- ...

Data self-erasureThe HSM can self-destruct 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 destruction 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 authenticated him-self, the self destruction is done after an alterable time, by default 0sec. It is therefore up to the operator to set it.

Note: The destruction 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 partitions used 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 shall be larger if necessary, because it must absolutely have 30% unused capacity when all the services 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: [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 900 Mhz 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;
- the 176 channel centred on 5880 MHz, called SCH1 (service channel 1);

Note: the multichannel is used on one antenna for the G5 and another antenna is used for the cellular.

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

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 RSU 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.

In case of interference the communication ITS-G5 is not guaranteed, the passage in cellular use must be used.

3.2.1.3 Range

The range of the transmitters depends largely on the installation site because the radio waves in this range of frequencies are quickly attenuated, even stopped, depending on the propagation environment specially 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 RSU, must be received at a rate of at least 90% by the SCOOP V-ITS-S, positioned in free space 500m from the R-ITS-S, and driving at a normal speed (under 100 km/h), adapted to the road.

3.2.1.4 Receiver sensitivity

Depending on the type of radio modulation used, 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 2 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 must have a minimum gain of 5 dBi to offset the losses in the coaxial cable.

If necessary, the antenna may be multiple uses since under their protective dome some models can house two antennas (dual-band): one for the ITS-G5 and the other for the cellular.

Multichannel is therefore possible on a single ITS-G5 antenna and two separate antennas are required, one for the cellular and the other for the G5.

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;
 - 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 better 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: [Time consideration](#)) for software time synchronisation;
- a differential position calculation.

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

Consequently, the GNSS module shall be remote if needed.

The elements to choose the type of GNSS are described in the [2.4.2.1_H.bis] deliverable.

3.3 Connections and sensors

The external connections, located in the R-ITS-S case (see chapter: [R-ITS-S Case](#)), 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: [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 or many 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 the same monitoring items that the R-ITS-S's local monitoring could display on a connected terminal:

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

In order to do so, all the components 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%,
- 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, they can also be installed on the same type of support.

3.5 Antenna and module Bluetooth

The elements relating to the Bluetooth technology will be added later.

4 Installation specifications

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

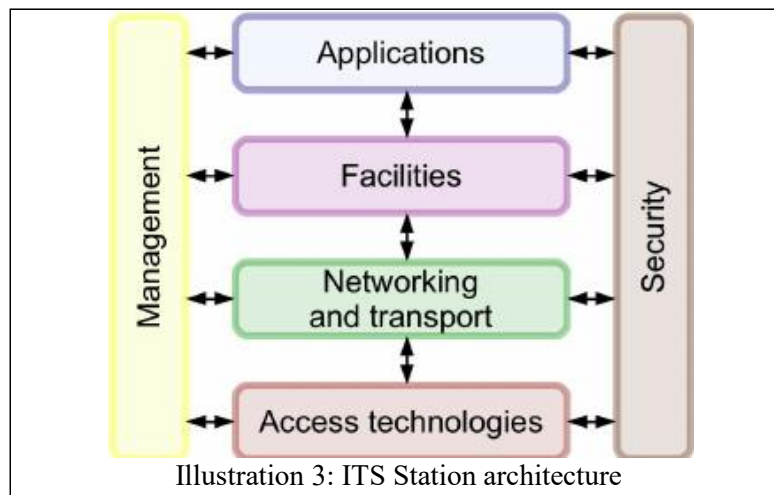
- Fixed R-ITS-S (term by default): This station can't be simply removed once it is installed.
- Autonomous R-ITS-S ("UBR autonome"): A station fully autonomous in terms of networks and light enough to be moved by a human operator (for example: the R-ITS-S + a battery + a solar panel + a cellular connection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

All these specifications are set in the [2.4.2.1_H_bis] deliverable.

5 Software

The software part of the R-ITS-S includes the application layer and the different upper layers (which are non hardware). The internal software architecture of a ITS station is described in the standards:



- Applications layer:
 - details the R-ITS-S configuration,
 - details the application software for use-cases,
 - contains part of the Local Dynamic Map (LDM),
 - does the translation between DATEX and IVI,
 - does the translation between DENM and DATEX.
- Facilities layer
 - contains 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.
 - the R-ITS-S must pass on the requests and responses related to the V-ITS-S PKI traffic to the "Public Key Infrastructure" that delivers them and then backup and resend them to the vehicles concerned. If relevant, this flow can pass through a home agent (see [2.4.1_H: Deliverable Functional and technical hybrid architecture – Common specifications] for more details).
- 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 Local SCOOP platform and the National Central ITS is reliable, it supports the PKI requests and the logs upload (see [2.4.2.4_H: French National Central ITS Station specifications] for more details).

- Communications are transported between the Vru-ITS-S, Home Agent and R-ITS-S by the Geo-Networking Basic Transport Protocol (GNBTP).
- the PKI traffic flows through HTTP.
- the Datex messages flows through HTTP.
- the log files from the Vru-ITS-S flow through sftp.
- Access layer
 - R-ITS-S – Local SCOOP platform: the R-ITS-S accesses the platform via a wire-based Ethernet link or via a cellular link, in full-duplex.
 - R-ITS-S –National Central ITS: ethernet or cellular link.
 - R-ITS-S - Vru-ITS-S: WIFI, ITS-G5.
 - R-ITS-S – PKI: 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 certificate
 - the wire-based communication links between the R-ITS-S and the supervision of the Local SCOOP platform must also be quantified by the Secure Shell (SSH) Ethernet protocol.
 - 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.
- Exchanges
 - the exchanges are carried out in Geonet or IPv4 or IPv6 towards National Node, PKI, Home Agent, Platform Relay and Road Operator Network.
 - These exchanges can concern CAM, DENM, IVI, PKI or DATEX.

5.1 Process received messages from V-ITS-S

The processes for receiving CAM messages, DENMs and their transfers as well as checking messages are described in the following paragraphs.

5.1.1 Process received CAM

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

5.1.1.1 Situation

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

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

The R-ITS-S sent calculated information to the 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, applying the rules accordingly to the received CAMs and resending the messages.

5.1.1.2 Functions

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

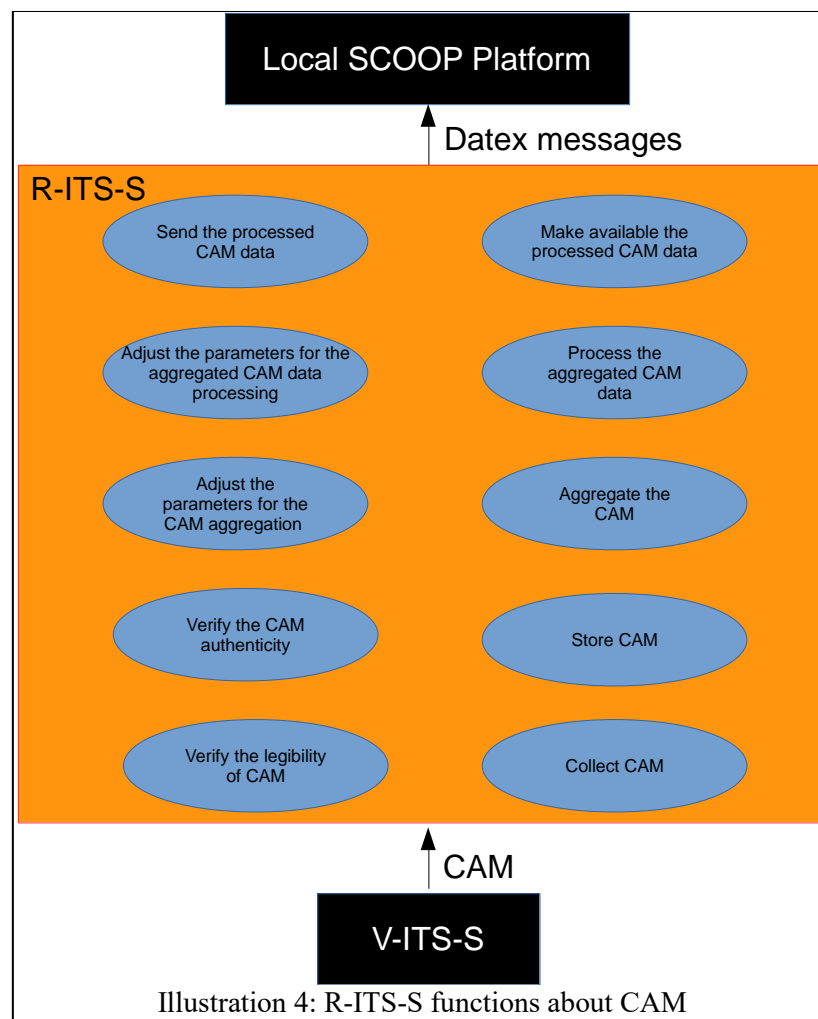


Illustration 4: R-ITS-S functions about CAM

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 at least one second 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/FILTER CAMs

It is necessary to control the legality of the received message, which corresponds to the transmission of a message CAM. The function consolidates the ability to identify an incomplete CAM that can't be processed and to know how to process it.

For example, the R-ITS-S can filter the messages:

- based on their completeness,
- based on the authorisation set in the certificate
- based on the type of station (in order to eliminate the R-ITS-S (15) and potentially the unknowns (0)).

5.1.1.2.4 AGGREGATE THE CAM DATA

This function is used 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.

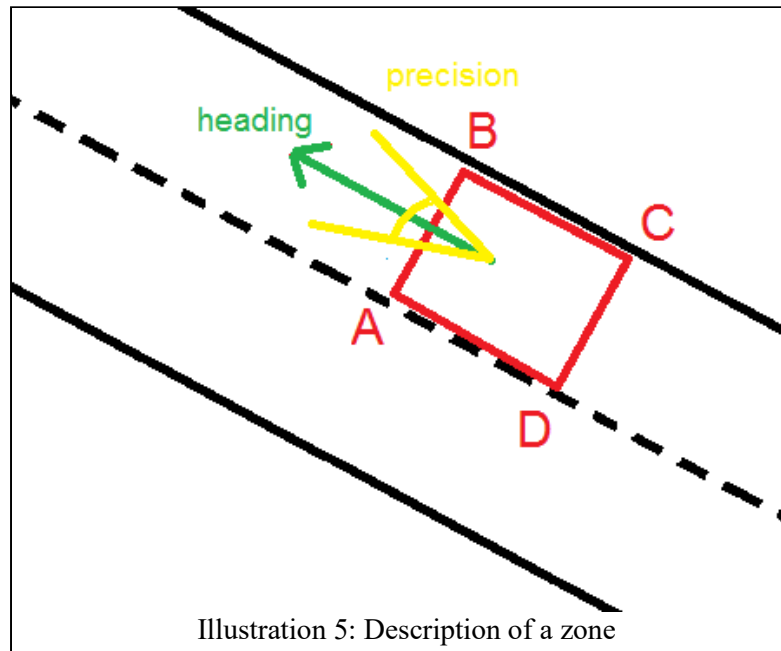
The CAM is relevant for the aggregation considered:

- if the message was issued 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 should be set by a server, in the Datex Format (see deliverable [2.4.1.4 : Specification of DATEX II v2.3 messages in conjunction with CAMs

and DENMs in SCOOP].

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 take into account.



Over the aggregation period, and in the virtual sensor zones, the data collected from the CAM can be aggregated for the same vehicle identifier, for example in a harmonic mean for the speed. By default, they are then averaged for values variable over time like harmonic speed mean over a default period of 1s. This average per vehicle is calculated on the entire virtual sensor the CAM is detected in.

For the constants over time related to a vehicle, like the vehicle length, a value can be taken without processing.

This pre-processing can be modified or disabled by the operator, from the platform, if it seems necessary (e.g., one can choose to only process one CAM per vehicle and per second).

For the CAM relevant in the aggregation considered, the software will calculate for each virtual sensor:

- number of vehicles presents,
- a harmonic speed mean of each 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 define 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, by direct request from the supervisor system.

Note: there may be several types of aggregation in parallel. For example: aggregation of vehicles 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 send 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 parametrization 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 CAM received is verified.

Note: The security systems in SCOOP, is described in the deliverables [2.4.4.1 to 2.4.4.8]. The deliverables [2.4.4.6.bis] 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 CAM 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 CAM 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.

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.

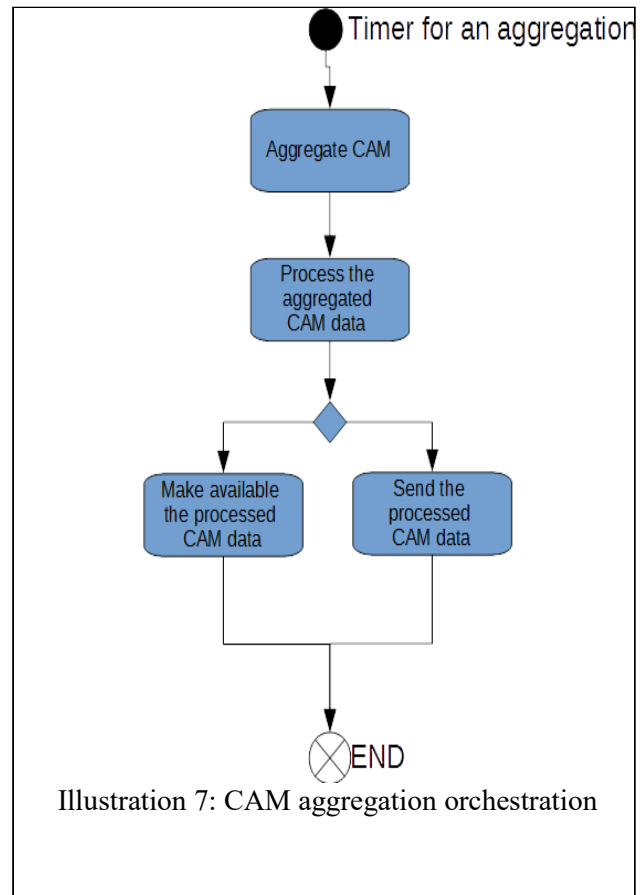
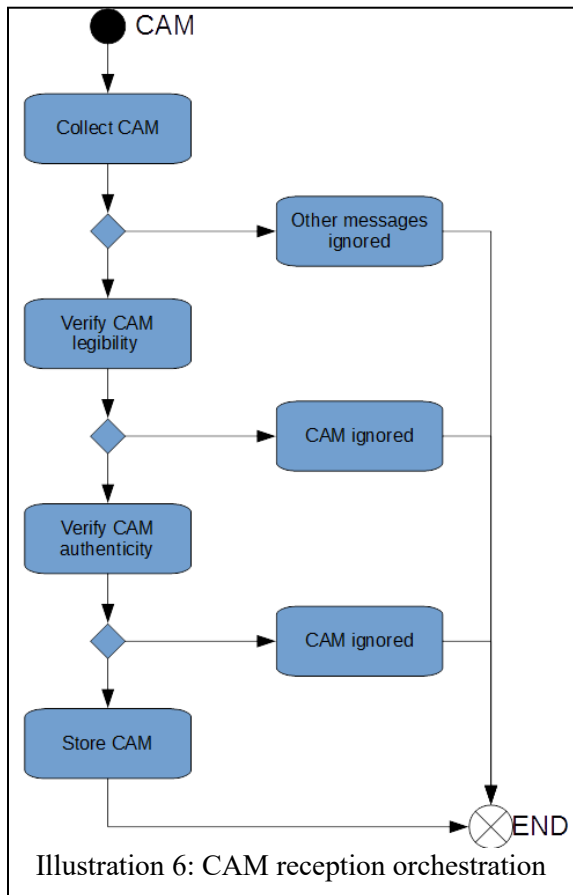
The parameters should be at least:

- number of aggregations
- for each aggregation,

- 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 R-ITS-S in the CAM aggregation (stationtype = 15)
- Boolean : filter the unknowns in the CAM aggregation (stationtype = 0)
- frequency 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

5.1.1.3 **Orchestration**

To illustrate this, the R-ITS-S can orchestrate the different functions as mentioned below:



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.

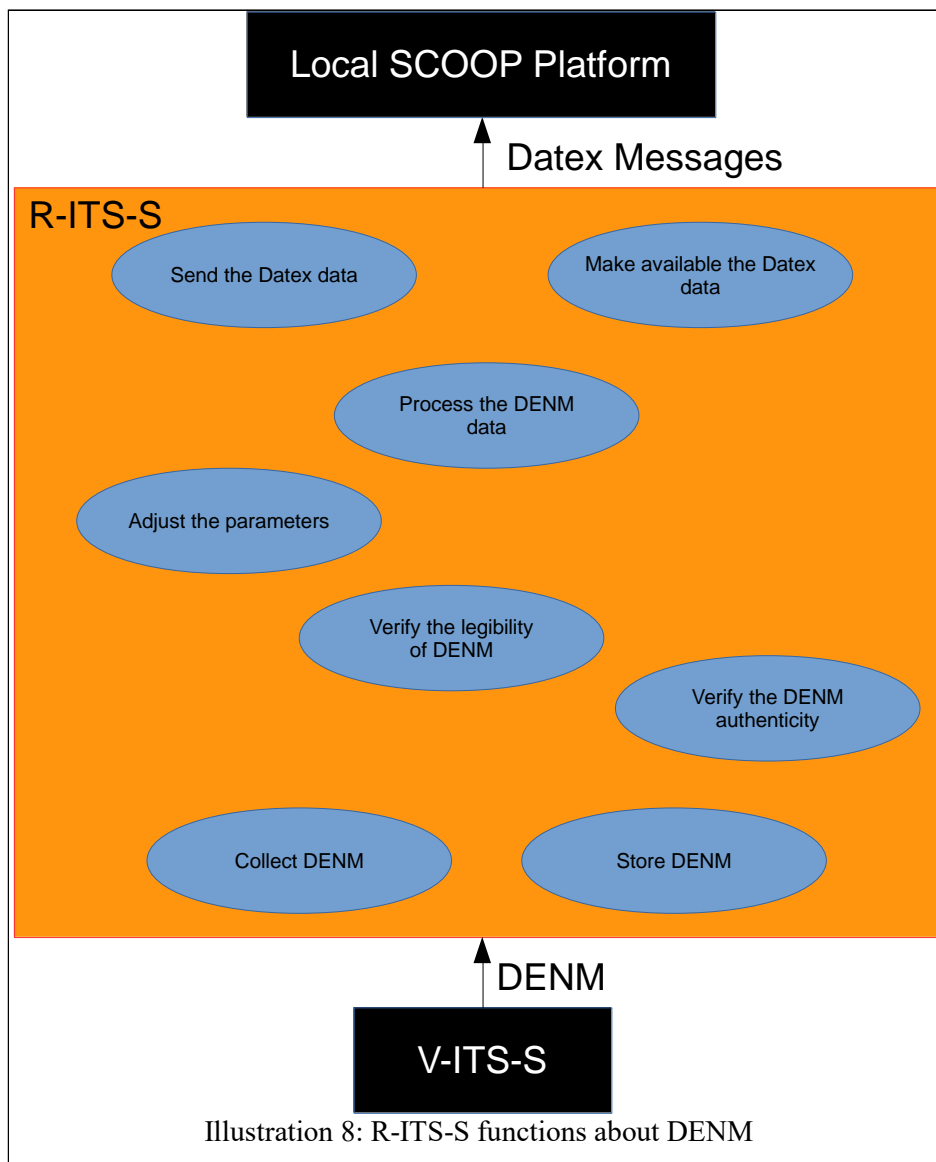
The R-ITS-S received DENM.

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 DENM use cases.



5.1.2.2.1 COLLECT DENMs

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.

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

5.1.2.2.2 STORE DENMs

This function stores the relevant DENM information, according to a configurable storage

time, with a 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 point, same referenceTime...)
- If the same DENM is already present in the LDM, but some data are updated, the message is updated in the LDM (same actionID, 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.

A road-operator could use the "informationQuality" to define the importance of DENMs, or the causeCode/subCauseCode of message (for example "Accident" is more important than "slippery road").

The storage space reserved for post-processing will also store all the processed received DENM, from the last transmission of 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 AND FILTER THEM

This function concerns verifying the veracity 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't be processed and to know how to process it. If the DENM message has already expired, ("detectionTime + validityDuration < 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 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 [2.4.4.6.bis] and [2.4.4.8] describe the process of the message's signature verification by using TSL and CRL.

5.1.2.2.5 MAKE AVAILABLE THE PROCESSED DENM DATA

The processed information used to produce the SCOOP - A2 and A3 service 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. It can be the same for CAM or others messages).

5.1.2.2.6 SEND THE PROCESSED DENM DATA

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

Data can also be sent regularly to the platform without waiting for a request from the platform. 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.

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).

5.1.2.2.7 ADJUST THE PARAMETERS

This function makes it possible to modify the rules and algorithms used to consolidate and 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.

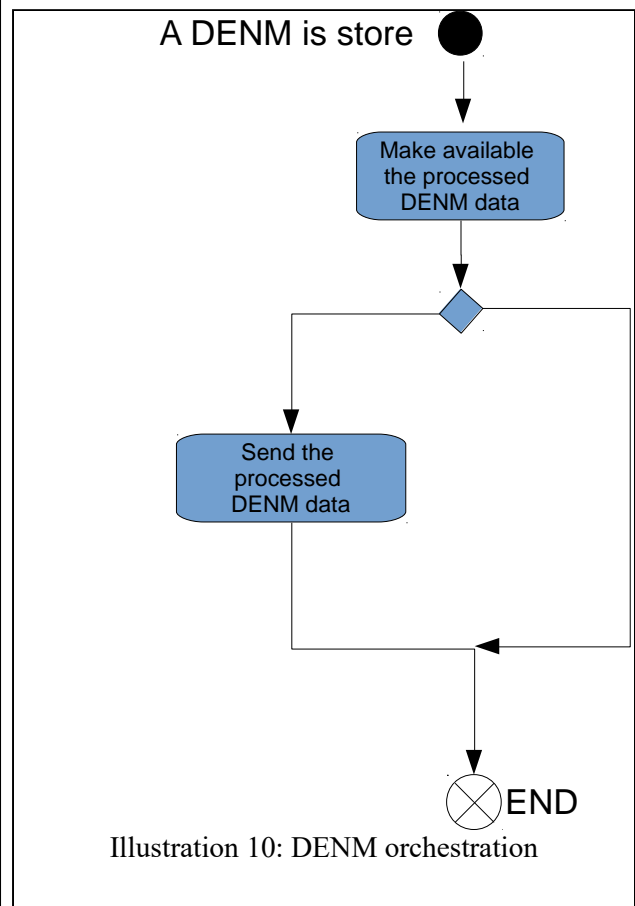
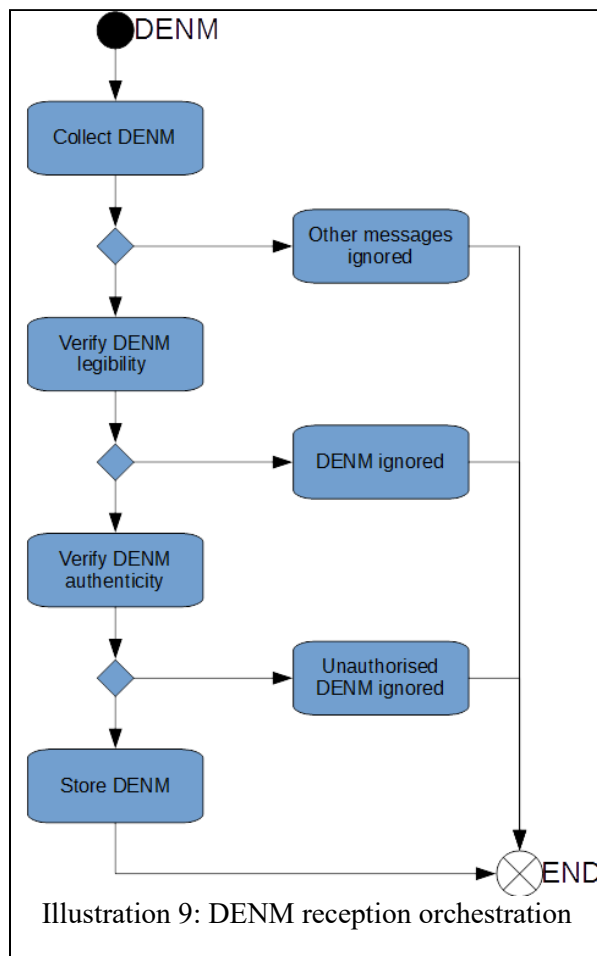
The parameters should be at least:

- 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)

- frequency of data retrieval (default value = 6 minutes)
- period of data disposal (default value = 24h)
- Datex II settings

5.1.2.3 Orchestration

To illustrate this, the R-ITS-S can orchestrate the different functions as mentioned below:



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 others 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

5.1.4 Verify the authenticity of a message

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. A part of the document is set below for simplification, but the reader must refer to the deliverables for exact information.

PROCEDURE

1- Receives the secured message

2- Checks the header field, and particularly the signer info,

a. Case 1: the signer_info is a certificate_digest_with_sha256 of the PC1 belonging to the V-ITS-S. The R-ITS-S has already received the entire certificate PC1.

The R-ITS-S verifies the digest, it calculates the hash of the certificate PC1 using sha256, compares the result with the value contained in the secured message, if the hashes are similar, the R-ITS-S can trust the sender and processes the secured message.

b. Case 2: the signer_info is a certificate_digest_with_sha256 of the PC1 belonging to the V-ITS-S. The R-ITS-S does not have the corresponding entire certificate (PC1).

In such case, the R-ITS-S sends a CAM message with header field of type request_unrecognized_certificate, requesting the V-ITS-S its entire PC1.

c. Case 3: The signer_info is a certificate or certificate_chain. The R-ITS-S verifies the certificate's validity and legitimacy, and saves it in its database. Verifying the certificate consists of verifying the validity date and the signer_info of the certificate. The signer_information should be the certificate or the certificate digest of the CA that issued the V-ITS-S's certificate.

3- The R-ITS-S verifies the authorization of the V-ITS-S to send CAMs messages or this causeCode/subCauseCode DENM, by verifying the its_aid included in the Secured Message and whether it matches with the SSP list included in the certificate.

a. Case 1: The its_aid that exists in the Secured Message do not match with the SSP list existing V-ITS-S's certificate. The V-ITS-S is not allowed to access this type of service, and the message is rejected.

b. Case 2: The its_aid matches with the SSP list and the message is accepted.

4- Once the eligibility and authorization of the V-ITS-S are verified, the R-ITS-S verifies the signature of the message deciphers the signature value with the public key associated with the PC1, obtains the hash result, calculates the hash of the message, and finally compares the two hashes.

- a. Case 1: The two hashes are not similar. The signature is not valid, the message is rejected.
 - b. Case 2: The two hashes are similar. The signature is valid and the message is accepted.
- At every step of this procedure, if one verification fails, then the signed message must be considered as invalid and must be rejected by the R-ITS-S.

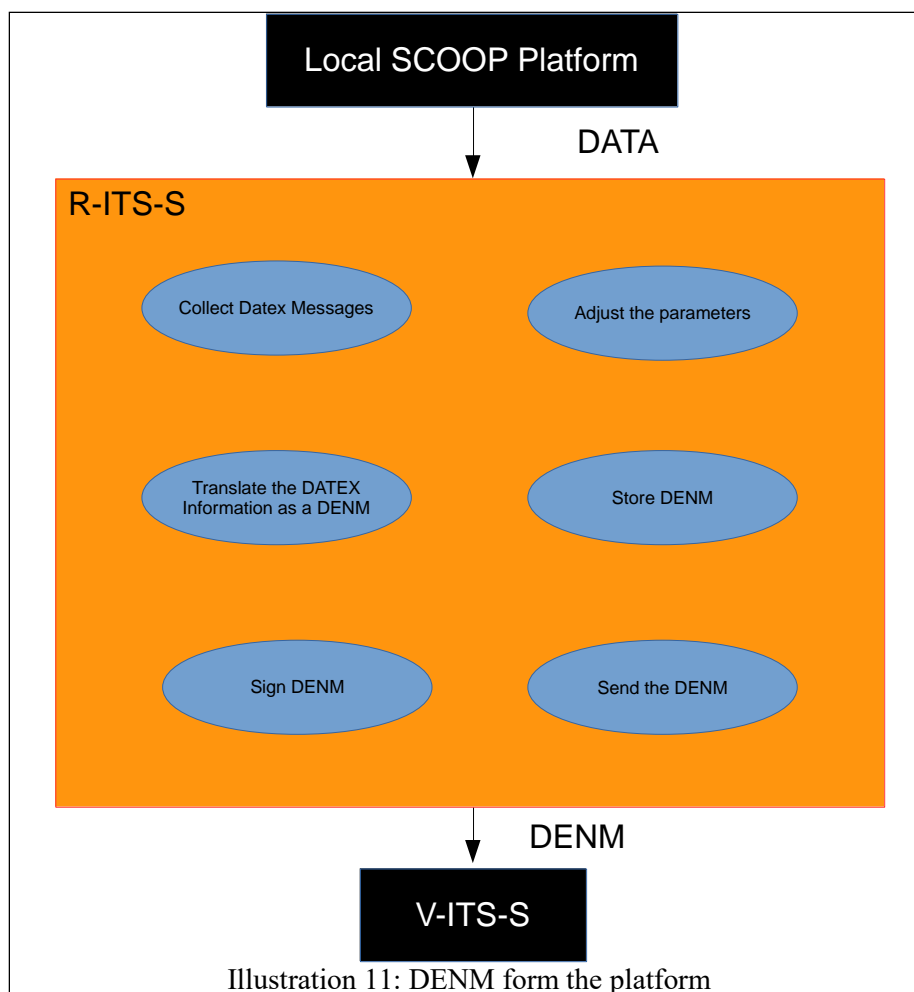
5.2 Distribute messages to users of the road network

5.2.1 DENM from the platform

5.2.1.1 Situation

This function produce the necessary information to operate the I2V 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 ITS Station on the road.



The UML type diagram hereafter explains the functions implemented through the D* use-cases (which are identical for the B* and the E6).

See Deliverable [2.4.1.4_H : Specification of DATEX II v2.3 messages in conjunction with CAMs and DENMs in SCOOP] for more information about Datex syntax and translation.

See Deliverable [2.4.3.2 : Spécifications fonctionnelles détaillées de la plate-forme SCOOP and 2.4.3.2_H : Detailed functional specifications of SCOOP platform] for more information about the platform.

5.2.1.2 Functions

5.2.1.2.1 COLLECT A DATEX II MESSAGES

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 could check the value "SOURCE" or <nationalIdentifier> in its database, to be shall of the source of the message. Consistency between the different databases shall be done by the road operator, especially on the value of <nationalIdentifier>.

5.2.1.2.2 TRANSLATE THE DATEX INFORMATION AS A 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_H : Specification of DATEX II v2.3 messages in conjunction with CAMs and DENMs in SCOOP]. Some extracts are mentioned below:

- *The “Linear” elements inside the “GroupofLocation” in the DATEX message send 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 chapter: [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 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

In order to process all the treatments, the R-ITS-S and the platform exchange other information than the messages to sent.

For the R-ITS-S and platform send 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 specific information snapshot to the other. It means request a Dutex 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 specific information snapshot at a regular period, or at a start-up.

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

5.2.1.2.7 ADJUST THE PARAMETERS

This functions lets 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", ...)
- for each causeCode/subCauseCode, frequency of the sendings
- frequency and time of the the snapshot to the platform (default value = 24h at 01:00 am)
- frequency of request after failure

5.2.2 CAM-I

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

These messages containing additional information are transmitted to the V-ITS-S in areas with a DSRC system (to avoid disturbances).

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

- SCOOP Deliverable 2.4.1_appendix 1 : Renewal of pseudonym certificates and upload of Logs (T-Logs and U-Logs)
- SCOOP Deliverable 2.4.1_appendix 2 : CAM-I Specification

The CAM-I must be sent to an alterable frequency (default value = 2 message in a second).

Optionally, the R-ITS-S can have a function to send CAM.

In this case, the messages are sent in the form of CAM and must comply with the standards defining the operating rules of CAM (especially for toll areas, the works, the rescues, safety vehicles, ...).

5.2.3 Secure sent messages

5.2.3.1 Sign a message to send

See DENM standards and SCOOP deliverables [2.4.4.6.bis] 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].

5.2.3.2 Add the R-ITS-S certificate to some messages

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

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

The R-ITS-S must add its certificate to the IVI.

5.2.4 IVI from the local platform

The description of the different fields of the type IVI message is indicated in the deliverable 2.4.1.2_H.

5.2.4.1 Send message DATEX II from platform to R-ITS-S and translate DATEX/IVI:

5.2.4.1.1 COLLECT A DATEX MESSAGES

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 could check the value "SOURCE" or < nationalIdentifier> in its database, to be sure of the source of the message. Consistency between the different databases shall be done by the road operator, especially on the value of "SOURCE".

5.2.4.1.2 ADJUST THE PARAMETERS

This functions lets the operator adjust the translation modalities for event-based information entering the road-side equipment as IVI to be broadcast to users.

Parameters:

- URL of the platform
- Datex II settings ("nationalIdentifier", ...)
- for each causeCode/subCauseCode, frequency of the sendings
- frequency and time of the snapshot to the platform (default value = 24h at 01:00 am)

5.2.4.1.3 TRANSLATE THE DATEX INFORMATION AS A IVI

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, etc.) in order to develop the corresponding IVI message that should be sent to users.

This shall be done according to the SCOOP Deliverable 2.4.1.4_H. Some extracts are mentioned below:

- The "Linear" elements inside the "GroupofLocation" in the DATEX message send

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. The conversion rules (operated by R-ITS-S) are defined below.

5.2.4.1.4 STORE THE IVI

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

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

The storage of a IVI consist in adding a new entry in the database for the IVI. In some cases it can consists in modifying an already present entry:

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

The expired IVI 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 IVIs will be deleted and replaced by the more recent IVIs. A message shall also be sent to the operator in order to inform him of the problem (the means used to trace this information must be defined by the manager). Moreover, the log files will be completed with the information.

A road-operator could use the “informationQuality” to define the importance of IVIs, or the causeCode/subCauseCode of message (for example “Accident” is more important than “slippery road”).

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

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

5.2.4.1.5 SIGN A IVI

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

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.

5.2.4.1.6 SEND IVI

This involves, for each road-side equipment, transmitting the signed IVI when it's necessary, to the others users via ITS-G5 wifi. For each causeCode/subCauseCode, frequency and duration are set in the parameters.

5.2.5 [optional] DENM and IVI from the HMI (local or remote)

For sending messages, 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, IVI...) provided in the French C-ITS Projects specifications.

- Any value of any data element of the DENM could be changeable, except header, actionID, and sequenceNumber. The HMI can provide more causeCodes than specified in the French C-ITS Projects.
- IVI messages can be editable, except header, serviceProviderId, ivIdentification Number, timestamp, validFrom. More data element than those specified in the French C-ITS Projects, can be changeable (fields from the local Scoop Platform, a parameter or the system).

5.3 Security of the R-ITS-S

As define in deliverable 2.4.4.x_H, 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: [Hardware Security Module](#) for more information about the process in the HSM

See deliverable [2.4.4.6 bis] for details.

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 offer 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] from 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.

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] from more information on direct exchange, and deliverable [2.4.4.11_H] from more information on exchange through the home agent.

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

For SCOOP:

If the facility is available for the R-ITS-S, the T-log and U-log will flow through 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 stored informations.

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

The R-ITS-S do 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)].

For C-Roads and InterCor:

The T-Log and U-Log will be defined later.

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-ITSSs is left up to the discretion of each road operator.

The V-ITSSs 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 in SCOOP Deliverables 2.4.1 and 2.4.1.1).

5.4.4 Relay messages from V-ITS-S to National Central ITSS, through Home Agent

The CAM and DENM messages from the V-ITS-S are relayed by the home agent to the French National Central ITSS, in accordance to the Interface 2 in the deliverable [2.4.1_H: Deliverable Functional and technical hybrid architecture – Common specifications].

This point concerns only V-ITS-S SCOOP wave 2, with hybrid connexion.

The sending of the V-ITS-S positions is transmitted as well as the CAM-I of the other R-ITS-S. In the CAM-I messages, the services indicate that the position of the tolls, the work areas, the rescues, the safety vehicles, ...

Some extracts from the 2.4.1_H below:

FIGURE 22: INTERFACE 2 END-TO-END IPV6 COMMUNICATION FLOW

Interface 2:

o uplink: CAM and DENM (ASN1 upper)/BTP/geonet/TCP/IPV6/802.11p (security at geonet level)

The RSU shall comply the requirements set in the 241H for the RSU. Some extracts :

The R-ITS-S shall support two services on the 802.11p SCH1 channel:

IPv6 router

And the Recursive DNS

The R-ITS-S shall configure two IPv6 addresses on the 802.11p-SCH1 link:

Link-local address in the fe80::/64 range

Global address, following the IPv6 router global prefix range

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 process (BIOS, OS, check memory, supervision ...)
- launch the security process (check/update certificates...)

- launch all the C-ITS process (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-destructs its data if it is handled physically (see chapter: [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. The R-ITS-S has the same operation with 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 describe in chapter: [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 state 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 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 : Specification of DATEX II v2.3 messages in conjunction with CAMs and DENMs in SCOOP].

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 second interleaves 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 include 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 deliverable 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 describe above could be accessible for the configuration process and should be set to their default value during the first installation:

- CAM parameters
- DENM parameters
- Forwarding DENM parameters
- Platform parameters
- 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:
 - [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.

For Scoop:

T-log are described in the SCOOP deliverables: [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 Tlog file size, the file is closed.
- The Tlog file is sent to a server.

Some T-logs contains personal data. The others T-logscan be used for statistics, or supervision by the road operator. It implies two different process for the two types of T-logs. For example, the first must be removed as soon as they have been send 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 Tlogs accessible by the road operator owner, is set in the SCOOP deliverable [2.3.8.1 : Privacy and personal data protection (only French version)].

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.

For C-Roads and InterCor:

The T-Log and U-Log will be defined later.

5.5.9 Fail-soft modes

5.5.9.1 General points

The Local 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 eventually in a T-log files.

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 and the post-processed traffic information 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 PRIORITISATION OF THE R-ITS-S'S FUNCTIONALITIES

By default, a R-ITS-S normally operates based on the following continuous application layer cycle. It:

1. Processes the monitoring information;
2. Forward the DENM
3. Receives the information from the PF;
4. Processes the information received from the PF;
5. Broadcast relevant information in the LDM module;
6. Receives the information from the V-ITS-S;
7. Processes the information from the V-ITS-S;
8. Sends the information received from the V-ITS-S to the PF:
 - i. Datex II events still valid (via DENM):
 - A3 service (events provided by a driver),
 - A2 service (automatic events),
 - ii. real-time Datex II traffic information (via CAM) [A1 service],
 - iii. expired Datex II events (via DENM),
 - iv. logs,

- v. batch-mode Datex II traffic information (via CAM),
- vi. the message history (CAM and DENM).

5.5.9.1.3 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 effective by sending a Datex II snapshot request that can restore the entire memory (and thereby update all the information to send).

Upon return from the fail-soft mode, the supervision server pushes to the R-ITS-S all of the configuration parameters that it must take into account for its operation as well as the complete updated map of events in its broadcast zone.

Upon return from a fail-soft mode that cut the R-ITS-S – PF link, a new PKI request can be envisaged.

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 or 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 while respecting the R-ITS-S priority of functionalities.

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 being 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 ask a snapshot of all data, the R-ITS-S must answer with one (or more, if necessary) Datex message included all the information of the LDM;
- the R-ITS-S ask a snapshot to the platform, the platform must answer with a Datex message.

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] A manual with all tests results must be deliver with the product.

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

For the tests, more functions can be offered to the operators. For exemple, accès to the log in local, sending CAM (and not CAM-I), ...

5.6 Management of Bluetooth beacon

The functions will be implemented later.