



Analysis of safety objectives

Deliverable 2.4.4.1

Activity 2: Studies

Sub-activity 2.4 > Specifications

Version 1.00

Publication date: 16/10/2015



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

Information on the document

Document: Analysis of safety objectives

Publication date: 16/10/2015

Responsible, Entity: Houda LABIOD, Telecom ParisTech

Status: Version 1.00 – Approved

Input deliverables: Deliverable 2.2 v4, deliverable 2.4.1 v0.2, deliverable 2.4.1bis v0, deliverable 2.4.4-2 v2

Publication history

Date	Version	Authors	Main changes	Distribution
16/10/2015	1.00	Houda Labiod		Release 1

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.	Deliverable objective	6
2.	Methodology.....	6
3.	SCOOP@F system architecture, part1	6
4.	Reminders about use cases.....	7
5.	List of use cases retained.....	9
6.	Comprehensive system architecture with PKI	10
7.	Safety objectives	11
8.	Classification of attacks.....	13
9.	Analysis of safety objectives	15
9.1	Detailed analysis by use case.....	16
9.2	Analysis by group of use cases.....	23
10.	Conclusion	24
11.	Bibliographic references.....	24

List of illustrations

Illustration1: SCOOP@F system architecture	6
Illustration2: Comprehensive architecture of the SCOOP" F part 1 system with PKI	10

List of tables

Table1: The use cases described in the deliverable 2.2-v4	8
Table2: The use cases that will be specified and developed in SCOOP"F part 1.	9
Table3: Possible attacks on the SCOOP@F system part 1	14
Table4: Attacks on ITSS-V, ITSS-R and ITSS-C	14
Table5: Analysis of safety objectives by use case	22
Table6: Analysis of safety objectives by groups of use cases	23

1. Deliverable objective

The objective of this deliverable is to deliver an analysis of the safety objectives of the use cases retained in part 1 of the SCOOP@F project.

2. Methodology

The methodology used is described in the plan of action 2.4.4.

3. SCOOP@F system architecture, part1

The SCOOP@F architecture is comprised of 3 main entities: the ITSS-V (vehicles), the ITSS-Rs and the ITS network (operator network), which includes the SCOOP@F platform (ITSS-C). Data is communicated from and to vehicles via a G5 communication with the ITSS-Rs and could also use the 3G cellular technology.

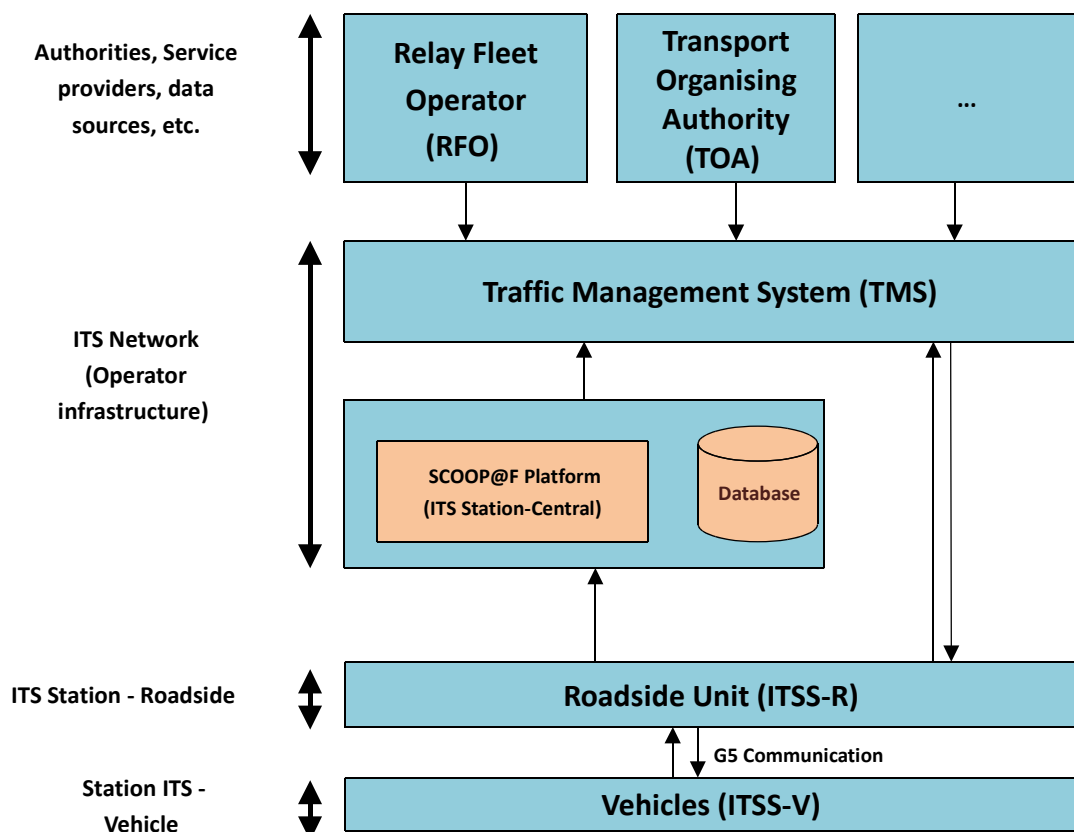


Illustration1: SCOOP@F system architecture

In the group of A services concerning the reporting of individual traffic-related data and data concerning events inside vehicles and road events, the communication with the TMS should go through the SCOOP@F platform so the information can be stored in a database. For some groups of services, considered as comfort services, the information should be retrieved from different entities like the transport organising authorities and the operators of relay fleets, so it can be communicated to drivers.

4. Reminders about use cases

The use cases are described in the deliverable 2.2-v4. They form 6 different groups (A to F). The table below presents a concise description of the different groups of use cases.

Services group		Use case		General description
A	Data collection	A1	Traffic data (position, speed, direction)	This involves the collection of data that interests in particular the network operators. It concerns two types of data: traffic data and event data. The data are used to produce the services described in the groups B to F.
		A2	Data on detected events (crashes, etc.)	
		A3	Data on reported events	
		A4	Vehicles' consumption and emission data	
B	Warning roadwork	B1	Warning – planned roadwork	These are warnings that inform users of roadwork and its characteristics (location, duration of work, etc.). The messages provided by this service can be considered as taking priority over comfort messages.
		B2	Warning – road operator intervention (accidents and unscheduled incidents, intervention of patrol officers)	
		B3	Warning - winter maintenance	
C	In-vehicle signage - driving information	C1	Fixed signage	This group of services provides users with driving information The driving information can cover both comfort information (e.g., directional signage) and network related information (dangers or speed limits). They can provide permanent or real-time information.
		C2	Real-time speed signage	
		C3	Panels with variable messages embedded (embedded VMS)	
D	In-vehicle signage - unexpected and dangerous events	D1	Warning – temporary slippery road	These are warnings sent to users when accidents or incidents that had a major impact on safety occur.
		D2	Warning - animal, people on the road	
		D3	Warning - obstacle on the road	Therefore, this is the group of services that has the highest priority.
		D4	Warning - stationary vehicles, breakdown	
		D5	Warning - unprotected accident area	In-vehicle signage - unexpected and dangerous events corresponding to I2V and V2V services
		D6	Warning - reduced visibility	

Services group		Use case		General description
D	In-vehicle signage - unexpected and dangerous events	D7	Warning - wrong way drivers	
		D8	Warning - unmanaged blockage of a road	
		D9	Warning - exceptional weather conditions	
		D10	Warning - emergency brake	
		D11	Warning - end of queue	
		E1	Traffic color	This group concerns supplying the user with information and comfort services that he can use to adapt his itinerary based on the state of traffic and the operator's recommendations.
		E2	Transit time	
		E3	Recommended itinerary, rerouting related to traffic conditions	
		E4	Information on access to amenities	
		E5	Information on access to services	
F	Relay fleets and multimodality	F1	Location and availability of relay parking lots - static information	This group offers users an information service on the multimodal transfer possibilities.
		F2	Location and availability of relay parking lots - real-time information	
		F3	Timetable of next TC departures (fixed)	
		F4	Timetable of next TC departures (real-time)	

Table1: The use cases described in the deliverable 2.2-v4

5. List of use cases retained

Based on the deliverable 2.4.1bisv0 and the document 'priority Scoop use case Copil development, 13 November 2014,' a list of priority use cases has been identified to be specified and developed in SCOOP" F part 1. This list is presented in table 2.

Services group		Use-case	
A	Data collection	A1	Traffic data (position, speed, direction)
		A2	Data on detected events (crashes, etc.)
		A3	Data on reported events
B	Warning roadwork	B1	Warning - planned roadwork (land line and cell)
		B2	Warning - road operator intervention
		B3	Warning - winter maintenance
D	In-vehicle signage - unexpected and dangerous events	D1	Warning - temporary slippery road
		D2	Warning - animal, people on the road
		D3	Warning - obstacle on the road
		D4	Warning - stationary vehicles, breakdown
		D5	Warning - unprotected accident area
		D6	Warning - reduced visibility
		D8	Warning - unmanaged blockage of a road
		D10	Warning - emergency brake
		D11	Warning - end of queue
E	Information on road traffic	E6	Weather info

Table2: The use cases that will be specified and developed in SCOOP" F part 1.

6. Comprehensive system architecture with PKI

The illustration below shows the different entities of the SCOOP[®]F system part 1, public key infrastructure (PKI), plus the messages exchanged.

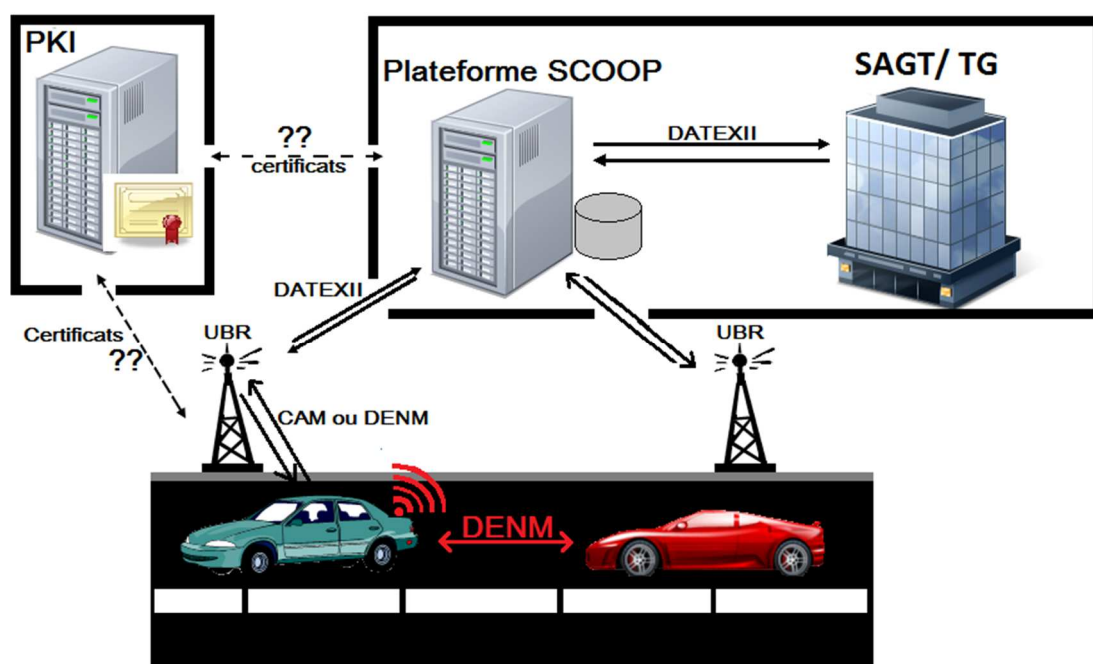


Illustration2: Comprehensive architecture of the SCOOP[®]F part 1 system with PKI

7. Safety objectives

The safety objectives that we consider in the project are listed below:

- Availability

This is the property of authorised users' accessibility at the desired time to information and functions.

- For a function: guarantee that the processing services are continuous; lack of problems related to the response time in the broad sense.
- For information: guarantee that the data can be accessed according to the planned availability (lead-times and timetable)
 - There is no total loss of information
 - As long as there is an archived version of the information, the information is considered as available (the availability of information is related to its archiving function).

The unavailability of information or a function can be due to its destruction or erasing, or even to a malfunction of the hardware, services or processes supporting it. The applications supported by the cooperative ITS systems, especially those that concern driving safety, require very high system availability.

- Integrity

This is the property of exactness and completeness of information and functions.

- For a function: assurance that the automated processing algorithm complies or not with the specifications; lack of incorrect or incomplete function results.
- For information: guarantee that the data are exact and complete vis-a-vis unauthorised handling or use errors; no alteration of the information.

This is a very important requirement for road safety applications. It makes it possible to ensure that the information exchanged has not been altered.

Confidentiality

This is the property that only authorised users can access information and functions.

- For a function: users are aware of the function and have the ability to access it.
- For information: data, whose access or use by unauthorised third parties could cause damage, are protected; lack of disclosure of confidential data.

Some applications require restricting access to the contents of messages exchanged with the transmitter and the receiver.

Non-repudiation/Traceability

Non-repudiation involves ensuring that no entity can repudiate having participated in an exchange (partially or wholly). Non-repudiation involves the notion of proof in the legal sense of the term.

Traceability is the guarantee that the transmission or reception of information cannot be refuted, with the ability to be able to audit the results provided. Only the functions can be categorised by a level of proof (which constitutes information proving the function was applied). For information, the level of integrity and proof are the one and the same because they are equivalent.

It is very important to be able to trace the origin of the message in certain ITS use cases (e.g., in the case of false information that could lead to accidents).

Authentication and authorisation

Authentication involves ensuring that the identity of the origin of data is indeed the claimed identity. Authorisation is the function specifying the access rights to the resources related to the security of the information (and the security of information systems in general) and access control in particular. More formally, "authorise" involves defining an access policy. Authentication makes it possible to guarantee that the entities involved in a communication are identified correctly. The entity has to be authorised for the applications that need to define the entity's rights.

Personal privacy protection

The objective of personal privacy protection is to control third parties' access to personal information. It concerns the respect of personal freedoms and the protection of personal privacy. Personal privacy protection is based on implementing legal means (according to the French data Protection Law No. 78-17 of 6 January 1978 completed by the law of 6 August 2014), technical means (cryptographic, etc.) or organisational means (internal rules). Protecting anonymity is a safety requirement that is closely tied to protecting personal privacy.

Since use cases handle personal data on users, users should comply with European and national directives related to the protection of personal data (Directive 95/46/EC, etc.).

In the context of the SCOOP@F project we believe this requirement is very important.

Plausibility

Plausibility checks are used to validate the plausibility of data with the aim of accepting or rejecting them. They are typically performed upon receiving the message.

The risk analysis presented by Solucom (deliverable 2.4.4-2v2: SCOOP@F risk analysis - Summary version 2) is based on four A.I.C.T criteria (A for Availability, I for Integrity, C for Confidentiality and T for Traceability), which are evaluated on a scale of four levels (level 1: weak, level 2: average, level

3: strong, level 4: very strong) available in the appendix of the Deliverable 2.4.4-2v2 (Slide 51). The A.I.C.T. criteria levels taken into account reflect the maximum-security needs identified on the data considered as the most critical. These are the:

- Group data in A use cases: Information collection
- Group data in B use cases: Roadwork warnings
- Group data in D use cases: In-vehicle signage - Unexpected and dangerous events

In our study, we considered in addition to these AICT criteria, 3 security criteria that we deem very important in the implementation of SCOOP@F use cases, which are:

- protection of personal privacy
- authentication / authorisation
- plausibility

For reasons of coherence, we adopt the same scale for the security levels.

8. Classification of attacks

In this section, we provide a quick preview of possible attacks on the SCOOP@F system. These attacks are listed in the literature [1,2]. They can be classified into two main categories:

- common attacks on wireless communication systems, and
- specific attacks on cooperative ITS systems.

Attacks			Description	Layer affected
Common attacks on wireless communication systems.	Denial of service (DoS)	Saturation of messages (Flooding)	Send a high volume of false messages and useless data in order to block the operation of the network and the hardware.	Facilities, Network, Access
		Junk email (Spamming)	Send excessive messages to increase the network latency and consume bandwidth	Facilities, Network, Access
		Black hole	Implement a node with bad behaviour that drops, poorly delivers and redirects messages	Network
		Malicious software (Malware)	Introduce malware with the aim of damaging the network / taking control of an ITSS-R remotely / modifying the software behaviour of ITSS-Rs / etc.	Applications, Facilities
		Greedy behaviour	Saturate the network by modifying the access controls or congestion control mechanisms in order to obtain more bandwidth than the other users	Access
		Jamming	Create an interference on the transmission channels in order to disrupt access / jam the G5 connection	Access

Attacks		Description	Layer affected
Common attacks on wireless communication	Message handling	Modify or delete messages, which results in the loss of information	Facilities, Network, Transport, Access
	Injection of false messages	Generate and send false information in messages	Facilities, Network, Access
	Recover the radio fingerprint (RF Fingerprinting)	Identify and distinguish someone else's radio transmitter using the transmission profiles.	Access
	Masquerade	Usurp the identity of an entity (pose as an ITSS-V or ITSS-R station) in order to transmit as a legitimate entity	Facilities, Network, Access
	Replay	Resend old messages (expired messages)	Facilities, Network
	Eavesdropping + data analysis	Listen to communications in order to collect information and analyse it	Network
Specific attacks on cooperative ITS systems.	GPS Spoofing	Use a GPS simulator to generate radio signals in order to convince the GPS receiver that it is at a given location at a given time	Access
	Location tracking	Collect location information	Facilities
	Sybil attack	Multiply false nodes (send multiple messages from a node using different identities)	Applications, Facilities, Network
	Illusion attack	Create a false traffic situation and send false traffic warning messages in order to deceive drivers by informing them that an event has occurred	Applications, Facilities
	Vehicle Sensor spoofing	Manipulate sensors in order to generate false data while respecting the protocols in place	Access

Table3: Possible attacks on the SCOOP@F system part 1

In table 4 we list the attacks that can target the different entities involved.

Target entity	Attacks
ITSS-V	Masquerade Vehicle Sensor spoofing Track the vehicle (link between messages) Eliminate/Isolate/Disrupt the station Affect communications
ITSS-R	Masquerade Track the terminal (link between messages) Eliminate/Isolate/Disrupt the station Affect communications
ITSS-C	Unauthorised access Information leak Disrupt the servers and security infrastructure

Table4: Attacks on ITSS-V, ITSS-R and ITSS-C

9. Analysis of safety objectives

This section includes two parts: one part that delivers a detailed analysis of the safety objectives for each use case and a second part that provides an overview of the safety objectives for all use cases.

9.1 Detailed analysis by use case

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
A1: Traffic data	Automatic reporting of: <ul style="list-style-type: none"> Station type Reference Position Heading Speed Drive Direction Vehicle Length Vehicle Width Longitudinal Acceleration Curvature Curvature Calculation Mode Yaw Rate Vehicle Role Exterior Lights Path History (23 points) Special Transport Type (if special vehicle?) Dangerous Goods Basic - Protected Communication ITSS-R areas (information on electronic tolling points) <ul style="list-style-type: none"> Generation Delta Time (instant when the CAM is generated) 	CAM (V2I)	Confidentiality	Unsupported	SCOOP platform: temporary storage TMS (*): archiving / permanent storage	<ul style="list-style-type: none"> ITSS-V ITSS-R ITSS-C TMS 	Broadcast (V2I)	ITSS-V	TMS	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack
			Integrity	Strong						
			Personal privacy protection	Very strong						
			Non-repudiation	Strong						
			Authentication 1st case: Authentication (at the ITSS-R) 2nd case: Authentication at the platform	Very strong						
			Plausibility (verification of the exactness of reported data) 1st case: at the ITSS-R 2nd case: at the platform or at the TMS	Strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
A2: Data on detected events A3: Data on reported events	Automatic or manual reporting of: <ul style="list-style-type: none"> Action ID Detection Time Reference Time (generation time) Termination (cancellation) Event position Relevance Distance Relevance Traffic Direction Validity Duration Transmission Interval Station Type Information Quality Event Type Linked Cause Event History... Example: Automatic reporting of: <ul style="list-style-type: none"> Emergency brake Triggering ABS/ESP <ul style="list-style-type: none"> Activation of hazard warning lights Triggering of windscreen wipers Manual reporting of: <ul style="list-style-type: none"> Instantaneous position, speed and direction parameters Accident report Presence of animals or people on the lanes Fog, strong rain, black ice Wrong way driver Congestion 	DENM	Confidentiality	Unsupported	SCOOP platform: temporary storage	<ul style="list-style-type: none"> ITSS-V ITSS-R ITSS-C TMS 	Broadcast (V2I)	ITSS-V	TMS	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Integrity	Strong	TMS (*): archiving / permanent storage					
			Personal privacy protection	Weak						
			Non-repudiation	Strong						
			Authentication	Strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
B1: Warning - planned roadwork (land line and cell)	- DENM + Information related to work zone	DENM	Availability	Strong	System embedded in ITSS-V and ITSS-R	<ul style="list-style-type: none"> Fixed roadwork: TMS, ITSS-C, ITSS-R, ITSS-V Mobile roadwork ITSS-V (operator), ITSS-V (client) 	Broadcast (I2V, V2V)	ITSS-C (stationary case), ITSS-V (operator, mobile case)	ITSS-V (client, relay)	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Plausibility	Weak						
			Non-repudiation	Very strong						
			Authentication	Strong						
B2: Warning - road operator intervention	• DENM + Information related to work zone	DENM	Availability	Strong	In-vehicle system	<ul style="list-style-type: none"> ITSS-V (operator) ITSS-V (client) ITSS-R ITSS-C TMS 	Broadcast	• ITSS-V (operator)	ITSS-V (client), ITSS-C TMS	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages Masquerade Replay GPS Spoofing Sybil attack Illusion attack
			Authentication	Strong						
			Non-repudiation	Strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
B3: Warning - winter maintenance	DENM + Information related to work zone	DENM	Availability	Strong	<ul style="list-style-type: none"> In-vehicle system ITSS-R 	<ul style="list-style-type: none"> TMS ITSS-C ITSS-R ITSS-V (operator) ITSS-V (client) 	Broadcast - (V2I, V2V)	<ul style="list-style-type: none"> TMS ITSS-C ITSS-R ITSS-V (operator) ITSS-V (client) 	ITSS-V (client)	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Authentication	Strong						
			Non-repudiation	Strong						
D1: Warning - temporary slippery road	DENM + information related to the road conditions	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (Client)	Broadcast (V2V, I2V)	ITSS-V ITSS-C	ITSS-V	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Plausibility	Very strong						
			Authentication	Strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
D2: Warning - animal on the road	DENM + information related to the event (animal on the road)	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (Client)	Broadcast (V2V, V2I, I2V)	ITSS-V ITSS-C	ITSS-V	<ul style="list-style-type: none"> • Denial of service • Message handling • Injection of false messages • RF Fingerprinting • Masquerade • Replay the messages • Eavesdropping + data/traffic analysis • GPS Spoofing • Location tracking • Sybil attack • Illusion attack • Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
D3: Warning - obstacle on the road (**)			Availability	Strong						
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
D4: Warning - vehicle, stationary or breakdown (**)			Availability	Strong						
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
D5: Warning - unprotected accident area (**)			Availability	Strong						
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
D6: Warning - reduced visibility	DENM + information related to the road and weather (visibility, etc.)	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (Client)	Broadcast (V2V, V2I, I2V)	ITSS-V ITSS-C	ITSS-V	<ul style="list-style-type: none"> • Denial of service • Message handling • Injection of false messages • RF Fingerprinting • Masquerade • Replay the messages • Eavesdropping + data analysis • GPS Spoofing • Location tracking • Sybil attack • Illusion attack • Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
D8: Warning - unmanaged blockage of a road	DENM+ information related to the road blocked event (accident, etc.)	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (client)	Broadcast (V2V, V2I, I2V)	ITSS-V ITSS-C	ITSS-V	<ul style="list-style-type: none"> • Denial of service • Message handling • Injection of false messages • RF Fingerprinting • Masquerade • Replay the messages • Eavesdropping + data analysis • GPS Spoofing • Location tracking • Sybil attack • Illusion attack • Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						

Services	Data communicated	Type of message	Safety function	Level	Storage location	Participating entities	Transmission	Source	Destination	Possible attacks
D10: Warning emergency brake	DENM + information related to the event (automatic detection)	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (client)	Broadcast (V2V, V2I)	ITSS-V	ITSS-V	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
D11: Warning end of queue	DENM + information related to the event	DENM	Availability	Strong	In-vehicle system	TMS ITSS-C ITSS-R ITSS-V (client)	Broadcast (V2V, V2I, I2V)	ITSS-V ITSS-C	ITSS-V	<ul style="list-style-type: none"> Denial of service Message handling Injection of false messages RF Fingerprinting Masquerade Replay the messages Eavesdropping + data analysis GPS Spoofing Location tracking Sybil attack Illusion attack Vehicle Sensor spoofing
			Integrity	Strong						
			Non-repudiation	Strong						
			Authentication	Strong						
			Plausibility	Very strong						
E6: Weather info	DENM (see box D9)	DENM	Availability	Weak	TMS ITSS-C	TMS ITSS-C ITSS-R ITSS-V (client)	Broadcast (I2V)	TMS	ITSS-V	
			Integrity	Strong						
			Non-repudiation	Weak						
			Plausibility	Weak						

Table5: Analysis of safety objectives by use case

(*) TMS: Traffic Management System (**) The services identified in D3, D4 and D5 clearly have the same characteristics as D2, consequently the safety services are probably similar.

9.2 Analysis by group of use cases

Service groups	Safety functions						
	Availability	Integrity	Confidentiality	Personal privacy protection	Non-repudiation/Traceability	Authentication	Plausibility
A - Data collection		x	x	x	x	x	x
B - Warning roadwork	x				x	x	x
D - In-vehicle signage - unexpected and dangerous events	x	x			x	x	x
E - Information on road traffic	x	x			x		x

Table6: Analysis of safety objectives by groups of use cases

10. Conclusion

This deliverable delivers a detailed analysis of the safety objectives of the use cases retained in part 1 of the SCOOP@F project. We see a return to some objectives that were considered in the risk analysis carried out by Solucom such as availability, integrity, confidentiality and traceability plus new objectives that we believe should be taken into account and treated in great detail such as personal privacy protection, authentication, authorisation and plausibility.

11. Bibliographic references

R. Moalla, Securing future cooperative ITS applications, Cifre Thesis, Renault-Telecom ParisTech, defended on 29 September 2014.

M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Networks*, vol. 15, no. 1, pp. 39-68, 2007.

Deliverable 2.4.4v2, SCOOP@F risk analysis – Summary version 2, November 2014.

Supporting note, Analysis of SCOOP@F information security risk, Solucom document, version 1.0, November 2014.

Deliverable 2.2 v4, July 2014.

Deliverable 2.4.1 v0.2, November 2014.

Deliverable 2.4.1bis v0, November 2014.