



TECHNICAL REPORT

## Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

*iTeh STANDARDS PREVIEW  
(standards.itih.ai)  
Full standard details: <https://standards.itih.ai/catalog/standards/sist/05b33f77-54d9-4536-80ff-59a028ba1d41/etsi-tr-102-893-v1.2.1-2017-03>*

---

**Reference**RTR/ITS-0050018

---

**Keywords**authentication, authorization, confidentiality,  
security**ETSI**650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

---

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**Copyright Notification**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

Intellectual Property Rights .....	6
Foreword.....	6
Modal verbs terminology.....	6
1 Scope .....	7
2 References .....	7
2.1 Normative references .....	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations .....	8
4 The TVRA Method .....	9
5 The ETSI Intelligent Transport System.....	10
5.1 ITS architecture .....	10
5.1.1 General.....	10
5.1.2 Summary of ITS applications .....	11
6 ITS Security Objectives.....	14
6.1 Confidentiality.....	14
6.2 Integrity .....	14
6.3 Availability.....	15
6.4 Accountability .....	15
6.5 Authenticity.....	15
7 ITS Functional Security classes.....	15
7.1 Confidentiality.....	15
7.2 Integrity .....	16
7.3 Availability.....	17
7.4 Accountability .....	17
7.5 Authenticity.....	17
8 ITS Target of Evaluation (ToE).....	18
8.1 General .....	18
8.2 Assumptions on the ToE .....	19
8.3 Assumptions on the ToE environment .....	19
9 ITS system assets .....	20
9.1 ITS station functional models.....	20
9.2 Functional assets .....	21
9.2.1 ITS-S (Vehicle).....	21
9.2.1.0 General .....	21
9.2.1.1 Protocol Control.....	22
9.2.1.1.1 General description.....	22
9.2.1.1.2 Vehicle to ITS infrastructure .....	22
9.2.1.1.3 Vehicle to vehicle .....	22
9.2.1.2 Service Control .....	22
9.2.1.3 ITS Applications .....	22
9.2.1.4 Sensor Monitor.....	23
9.2.1.5 Vehicle System Control .....	23
9.2.2 ITS-S (Roadside) .....	24
9.2.2.0 General .....	24
9.2.2.1 Protocol Control.....	24
9.2.2.1.1 General description.....	24
9.2.2.1.2 RSU to vehicle.....	24
9.2.2.1.3 RSU to ITS network .....	24
9.2.2.2 Service Control .....	24
9.2.2.3 ITS Applications .....	25

9.2.2.4	Sensor Monitor.....	25
9.2.2.5	Display Control.....	26
9.3	Data assets.....	26
9.3.1	ITS-S (Vehicle).....	26
9.3.1.1	Local Dynamic Map.....	26
9.3.1.2	Local Vehicle Information.....	27
9.3.1.3	Service Profile.....	27
9.3.2	ITS-S (Roadside).....	27
9.3.2.1	Local Dynamic Map (LDM).....	27
9.3.2.2	Local Station Information.....	28
9.3.2.3	Service Profile.....	28
10	ITS threat analysis.....	28
10.1	Attack interfaces and threat agents.....	28
10.1.1	Attack interfaces and threat agents for ITS-S (Vehicle) ToE.....	28
10.1.2	Attack interfaces and threat agents for ITS-S (Roadside) ToE.....	29
10.2	Vulnerabilities and threats.....	30
10.2.1	Threats to all ITS stations.....	30
10.2.2	Availability.....	30
10.2.2.1	General threats to availability.....	30
10.2.3	Integrity.....	31
10.2.3.1	General threats to integrity.....	31
10.2.4	Authenticity.....	31
10.2.4.1	General threats to authenticity.....	31
10.2.5	Confidentiality.....	32
10.2.5.1	General threats to confidentiality.....	32
10.2.6	General threats to accountability.....	32
10.2.7	Vulnerabilities and threats.....	33
10.2.7.1	Determining system vulnerabilities.....	33
10.2.7.2	Threats and vulnerabilities within an ITS-S (Vehicle).....	34
10.2.7.3	Threats and vulnerabilities within an ITS-S (Roadside).....	41
10.3	Security risks in an ITS system.....	46
10.3.0	Introduction.....	46
10.3.1	Risks in an ITS-S (Vehicle).....	47
10.3.2	Risks in an ITS-S (Roadside).....	48
11	Countermeasures.....	49
11.1	List of Countermeasures.....	49
11.2	Evaluation of Countermeasures.....	50
11.3	Countermeasure Analysis.....	51
11.3.1	Reduce frequency of beaconing and other repeated messages.....	51
11.3.2	Add source identification (IP address equivalent) in V2V messages.....	51
11.3.3	Limit message traffic to V2I/I2V when infrastructure is available and implement message flow control and station registration.....	52
11.3.4	Implement frequency agility within the 5,9 GHz band.....	53
11.3.5	Implement ITS G5A as a CDMA/spread-spectrum system.....	53
11.3.6	Integrate 3 <sup>rd</sup> Generation mobile technology into ITS G5A communications.....	54
11.3.7	Digitally sign each message using a Kerberos/PKI-like token system.....	55
11.3.7.0	General.....	55
11.3.7.1	Kerberos-like solution.....	55
11.3.7.1.1	General requirements.....	55
11.3.7.1.2	Countermeasure analysis.....	56
11.3.7.2	PKI-like solution.....	56
11.3.7.2.1	General requirements.....	56
11.3.7.2.2	Countermeasure analysis.....	57
11.3.8	Include a non-cryptographic checksum of the message in each message sent.....	57
11.3.9	Remove requirements for message relay in the ITS BSA.....	58
11.3.10	Include an authoritative identity in each message and authenticate it.....	58
11.3.11	Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages.....	59
11.3.12	Include a sequence number in each new message.....	60
11.3.13	Use INS or existing dead-reckoning methods (with regular - but possibly infrequent - GNSS corrections) to provide positional data.....	61
11.3.14	Implement differential monitoring on the GNSS system to identify unusual changes in position.....	61

11.3.15	Encrypt the transmission of personal and private data.....	62
11.3.16	Implement a Privilege Management Infrastructure (PMI).....	63
11.3.17	Software authenticity and integrity are certified before it is installed .....	64
11.3.18	Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle .....	64
11.3.19	Maintain an audit log of the type and content of each message sent to and from an ITS-S.....	65
11.3.20	Perform plausibility tests on incoming messages .....	66
11.3.21	Provide remote deactivation of misbehaving ITS-S (Vehicle) .....	67
11.3.22	Use hardware-based identity and protection of software on an ITS-S.....	67
11.4	Countermeasure Set.....	68
11.4.0	Introduction.....	68
11.4.1	ITS Countermeasure Set .....	69
11.4.1.1	Countermeasures to Denial of Service (DoS) and availability threats .....	69
11.4.1.2	Countermeasures to integrity threats.....	71
11.4.1.3	Countermeasures to confidentiality and privacy threats.....	71
11.4.1.4	Countermeasures to non-repudiation and accountability threats.....	72
11.4.2	Residual risk .....	72
<b>Annex A:</b>	<b>Cost - Benefit analysis of the selected countermeasures.....</b>	<b>73</b>
<b>Annex B:</b>	<b>GeoNetworking Risk Assessment .....</b>	<b>77</b>
B.1	Introduction .....	77
B.2	GeoNetworking Model.....	77
B.3	Packet Structure.....	78
B.4	Target of Evaluation.....	78
B.4.1	General .....	78
B.4.2	Assumptions .....	78
B.4.3	Assets .....	79
B.4.3.1	Data Assets .....	79
B.4.4	GeoNetworking Threat Analysis.....	79
B.4.4.1	General Assumptions .....	79
B.4.4.2	Attacks .....	79
B.4.4.2.1	General .....	79
B.4.4.2.2	Availability.....	79
B.4.4.2.3	Integrity .....	79
B.4.4.2.4	Confidentiality .....	80
B.4.4.2.5	Privacy .....	80
B.4.4.3	Security Risks of GeoNetworking .....	80
B.4.5	Countermeasures .....	81
B.4.5.1	General.....	81
B.4.5.2	Security Design Premise .....	81
B.4.5.3	List of Countermeasures .....	81
B.4.5.3.1	Overview .....	81
B.4.5.3.2	C1: Consistency check, incoming plausibility check and global misbehavior detection .....	82
B.4.5.3.3	C2: Restrict maximum range and maximum number of hops a packet is routed .....	83
B.4.5.3.4	C3: Restrict frequency to send messages .....	84
B.4.5.3.5	C4: Verify (forwarding ITS-S) packet payload on demand .....	84
B.4.5.3.6	C5: Optionally encrypt packet payload in an end-to-end manner .....	85
B.4.5.3.7	C6: Always sign (original sender and forwarding ITS-S) common header and verify (forwarding and final receiver ITS-S) common header on demand .....	85
B.4.5.4	Further Countermeasures .....	86
B.4.6	Incentive Schemes .....	86
B.4.7	Security Performance .....	87
B.4.7.1	General.....	87
B.4.7.2	Confidentiality (Countermeasure C5).....	87
B.4.7.3	Integrity (Countermeasures C4 and C6) .....	87
B.4.7.4	Confidentiality + Integrity (Countermeasures C4, C5 and C6) .....	87
History	.....	88

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

---

## Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

**ITeH STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/61b2f77-54d9-4536-80ff-59a028ba1d4f/etsi-tr-102-893-v1.2.1>  
2017-03

---

# 1 Scope

The present document summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.3] operating in a fully deployed ITS.

The present document was prepared using the TVRA method described in ETSI TS 102 165-1 [i.1].

NOTE: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the ETSI ITS Work Programme.

---

## 2 References

### 2.1 Normative references

Normative references are not applicable in the present document.

### 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".
  - [i.2] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".
  - [i.3] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".
  - [i.4] IEEE 802.11TM: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
  - [i.5] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
  - [i.6] IETF RFC 4120: "The Kerberos Network Authentication Service (V5)".
- NOTE: Available at <http://tools.ietf.org/html/rfc4120>.
- [i.7] ETSI TS 102 636-4-1: "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".
  - [i.8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

- [i.9] ETSI TR 102 863: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".
- [i.10] ETSI EN 302 636-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".
- [i.11] Risk analysis study of ITS communication architecture, R Moalla, H Labiod, B Lonc, N Simoni, IEEE Network of the Future conference, 2012.

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

- beaconing:** network layer service which retransmits requested information
- end user:** functional agent directly representing the human user of the ITS or the ITS service provider
- geo-addressing:** network layer service that enables the addressing a specific geographic region
- ITS application:** entity that defines and implements an ITS use case or a set of ITS use cases
- ITS use case:** specific scenario in which ITS messages are exchanged
- ITS user:** any ITS application or functional agent sending, receiving or accessing ITS-related information
- local dynamic map:** dynamically maintained information on driving and environmental conditions in the vicinity of the ITS-S
- restricted local ITS station data:** data to be shared only with authorized parties
- unrestricted local ITS station data:** data that may be shared without requiring authorization from the recipient

### 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Attribute Authority
AC	Attribute Certificate
BSA	Basic Set of Applications
CA	Co-operative Awareness
CAM	Cooperative Awareness Message
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CN	Co-operative Navigation
CS	Communities Services
CSM	Co-operative Speed Management
DENM	Decentralized Environmental Notification Message
DNM	Decentralized environmental Notification Message
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
FA	Functional Asset
FM	Frequency Modulation
GAC	GeoAnycast
GBC	GeoBroadcast
GNSS	Global Navigation Satellite System
GUC	GeoUnicast
HMAC	Hashed Message Authentication Code



HMI	Human-Machine Interface
I2V	Infrastructure to Vehicle
IAAA	Identification, Authentication, Authorization, Accountability
INS	Inertial Navigation System
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	ITS Station
LBS	Location Based Services
LCM	Life Cycle Management
LDM	Local Dynamic Map
OS	Operating System
PKI	Public Keying Infrastructure
PMI	Privilege Management Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SAML	Security Assertion Markup Language
SFR	Security Functional Requirement
SHB	Single-Hop Broadcast
SoA	Source of Authority
SSP	Service Specific Permissions
ToE	Target of Evaluation
TSB	Topologically-Scoped Broadcast
TTP	Trusted Third Party
TVRA	Threat, Vulnerability and Risk Analysis
UTC	Universal Coordinated Time
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VIN	Vehicle Identification Number

## 4 The TVRA Method

Without an understanding of the threats posed to a system it is impossible to select or devise appropriate measures to counter these threats. The ETSI Threat, Vulnerability and Risk Analysis (TVRA) [i.1] is used to identify risks to a system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system.

The TVRA method process consists of the following steps:

- 1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.
- 2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.
- 3) Identification of the functional security requirements, derived from the objectives from step 2.
- 4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.
- 5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.
- 6) Quantifying the occurrence likelihood and impact of the threats.
- 7) Establishment of the risks.
- 8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.
- 9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

- 10) Specification of detailed requirements for the security services and capabilities from step 9.

The present document summarizes the results from each of these steps in the analysis of the ETSI Intelligent Transport System (ITS) standards.

## 5 The ETSI Intelligent Transport System

### 5.1 ITS architecture

#### 5.1.1 General

The ITS security architecture is defined in ETSI TS 102 940 [i.8] and covers both the Communication Architecture and the architecture of the ITS-S itself. ETSI TR 102 638 [i.3] defines the basic set of ITS applications which it divides into groups according to the functionality provided which is further analysed in ETSI TR 102 863 [i.9] and transformed into a detail classification of ITS applications in ETSI TS 102 940 [i.8]. For ease of reading and for further risk analysis the relevant tables from ETSI TS 102 940 [i.8] are copied here.

**Table 1: ITS application classes**

Applications Class	Application	Use case	
Active road safety	Driving assistance - Co-operative Awareness (CA)	Emergency vehicle warning	
		Slow vehicle indication	
		Across traffic turn collision risk warning	
		Merging Traffic Turn Collision Risk Warning	
		Co-operative merging assistance	
		Intersection collision warning	
		Co-operative forward collision warning	
		Lane Change Manoeuvre	
		Driving assistance - Road Hazard Warning (RHW)	Emergency electronic brake lights
			Wrong way driving warning (infrastructure based)
	Stationary vehicle - accident		
	Stationary vehicle - vehicle problem		
	Traffic condition warning		
	Signal violation warning		
	Roadwork warning		
	Decentralized floating car data - Hazardous location		
	Decentralized floating car data - Precipitations		
	Decentralized floating car data - Road adhesion		
	Cooperative traffic efficiency	Co-operative Speed Management (CSM)	Regulatory/contextual speed limits notification
			Curve Warning
Traffic light optimal speed advisory			
Co-operative Navigation (CN)		Traffic information and recommended itinerary	
		Public transport information	
		In-vehicle signage	

Applications Class	Application	Use case
Co-operative local services	Location Based Services (LBS)	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities Services (CS)	Insurance and financial services
		Fleet management
		Loading zone management
		Theft related services/After theft vehicle recovery
	ITS station Life Cycle Management (LCM)	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration
	Transport related electronic financial transactions (road tolls)	

### 5.1.2 Summary of ITS applications

In order to define security classes the communication patterns of the different applications also need to be considered. Table 2 summarizes the communication behavior of each application.

**ITeH STANDARD PREVIEW**  
 (standards.iteh.ai)  
 Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/05b33f77-54d9-4536-80ff-59a028ba1d4f/etsi-tr-102-893-v1.2.1-2017-03>

Table 2: ITS applications communication behavior

Use case	Addressing	Hops	Frequency	Direction	Session	
Emergency vehicle warning	Broadcast	Single	High	V2V/V2I	No	
Slow vehicle indication	Broadcast	Single	High	V2V	No	
Across traffic turn collision risk warning	Broadcast	Single	High	V2V	No	
Merging Traffic Turn Collision Risk Warning	Broadcast	Single	High	V2V/I2V	No	
Co-operative merging assistance	Broadcast	Single	High	V2V/I2V	No	
Intersection collision warning	Broadcast	Single	High	V2V/I2V	No	
Co-operative forward collision warning	Broadcast	Single	High	V2V	No	
Lane Change Manoeuvre	Broadcast	Single	High	V2V	No	
Emergency electronic brake lights	Broadcast	Multi	Low	V2V	No	
Wrong way driving warning (infrastructure based)	Broadcast	Single	Low	I2V	No	
Stationary vehicle - accident	Broadcast	Multi	Low	V2V/V2I	No	
Stationary vehicle - vehicle problem	Broadcast	Multi	Low	V2V/V2I	No	
Traffic condition warning	Broadcast	Multi	Low	V2V/I2V	No	
Signal violation warning	Broadcast	Single	High	I2V	No	
Roadwork warning	Broadcast	Multi	Low	I2V	No	
Decentralized floating car data - Hazardous location	Broadcast	Multi	Low	V2V/I2V	No	
Decentralized floating car data - Precipitations	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Road adhesion	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Visibility	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Wind	Broadcast	Multi	Low	V2V	No	
Vulnerable road user Warning	Broadcast	Single	Low	V2V/I2V	No	
Pre-crash sensing warning	Indication	Broadcast	Single	High	V2V	No
	Data exchange	Unicast	Single	High	V2V	Yes
Co-operative glare reduction	Broadcast	Single	Low	V2V/I2V	No	
Regulatory/contextual speed limits notification	Broadcast	Single	Low	I2V	No	
Curve Warning	Broadcast	Single	Medium	I2V	No	
Traffic light optimal speed advisory	Broadcast	Multi	Medium	I2V	No	
Traffic information and recommended itinerary	Advertisement	Broadcast	Single	I2V	No	
	Service	Unicast/Multicast	Multi	Medium	I2V	Yes
Public transport information	Advertisement	Broadcast	Single	I2V	No	
	Service	Multicast	Multi	Medium	I2V	Yes
In-vehicle signage	Broadcast	Single	Medium	I2V	No	
Point of Interest notification	Advertisement	Broadcast	Single	I2V	No	
	Service	Multicast	Single	I2V	Yes	

Use case	Addressing	Hops	Frequency	Direction	Session
Automatic access control and parking management	Advertisement	Broadcast	Single	I2V	No
	Service	Unicast	Single	I2V/V2I	Yes
ITS local electronic commerce	Unicast	Single	Low	I2V/V2I	Yes
Media downloading	Unicast	Single	Low	I2V/V2I	Yes
Insurance and financial services	Unicast	Single	Low	I2V/V2I	Yes
Fleet management	Unicast	Single	Low	I2V/V2I	Yes
Loading zone management	Unicast/Multicast	Single	Low	I2V/V2I	Yes
Theft related services/After theft vehicle recovery	Unicast	Multi	Low	I2V/V2I	Yes
Vehicle software/data provisioning and update	Unicast	Single	Low	I2V/V2I	Yes
Vehicle and RSU data calibration	Unicast	Single	Low	I2V/V2I	Yes

**iTeh STANDARD PREVIEW**  
 (standards.iteh.ai)  
 Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/05f33f77-54d9-4536-80f-59a028ba1d4f/etsi-tr-102-893-v1.2.1-2017-03>