ETSI TR 102 893 V1.1.1 (2010-03)

Technical Report

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

Reference
DTR/ITS-0050005

Keywords
ITS, 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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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 http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

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 (http://webapp.etsi.org/IPR/home.asp).

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 System (ITS).

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.8] operating in a fully deployed ITS.

The analysis in the present document considers issues of privacy implicitly with confidentiality. It does not consider regulatory requirements for privacy

The present document was prepared using the TVRA method described in 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

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[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 102 637-1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements.

[i.3] ETSI TS 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Co-operative Awareness Basic Service".

[i.4] ETSI TS 102 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Application; Part 3: Specification of Decentralized Environmental Notification Basic Service".

[i.5] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.6] ETSI TS 102 731: "Intelligent Transportation Systems (ITS); Security; Security Services and Architecture".

[i.7] Brown, C. (Aalborg. 2007): "Vehicles as Sensors for Cooperative Systems". Presentation on ITS in Europe..

[i.8] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

[i.9] IEEE 802.11 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.10] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.11] ETSI TS 102 637-4: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of applications; Part 4: Operational Requirements.".

[i.12] IETF RFC 4120: "The Kerberos Network Authentication Service (V5)".

NOTE: Available at http://tools.ietf.org/html/rfc4120.

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 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

ITS application: entity that defines and implements an ITS use case or a set of ITS use cases

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
CAM	Cooperative Awareness Message
CCH	Control CHannel
CDMA	Code Division Multiple Access
DNM	Decentralized environmental Notification Message
FA	Functional Asset
GNSS	Global Navigation Satellite System
I2V	Infrastructure to Vehicle
ITS	Intelligent Transport System
ITS-G5A	ITS radio signalling in the 5,875 GHz to 5,905 GHz frequency range
ITS-S	ITS Station
LDM	Local Dynamic Map
OS	Operating System
OSI	Open Systems Interconnection
PKC	Public Key Cryptography
PKI	Public Keying Infrastructure
PMI	Privilege Management Infrastructure
PMI	Privilege Management Infrastructure
RSU	Road Side Unit
SAML	Security Assertion Markup Language
SCH	Service CHannel
ToE	Target of Evaluation
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 involves the following seven steps:

1) Identify security objectives.

2) Identify security requirements.

3) Produce an inventory of system assets.

4) Classify system vulnerabilities and threats.

5) Quantify the likelihood and impact of attack.

6) Determine the risks involved.

7) Specify detailed security requirements (countermeasures).

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

Intelligent Transport Systems comprise the following communicating entities (as shown in Figure 1):

- Vehicles
- Roadside units
- A network infrastructure

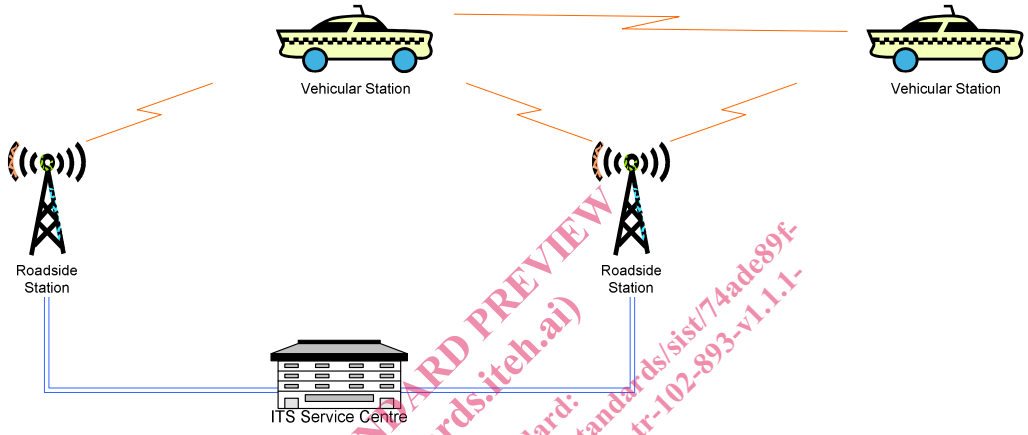

Figure 1: Communicating ITS entities

This simplified architecture can be represented in functional terms by the overlay shown in Figure 2.

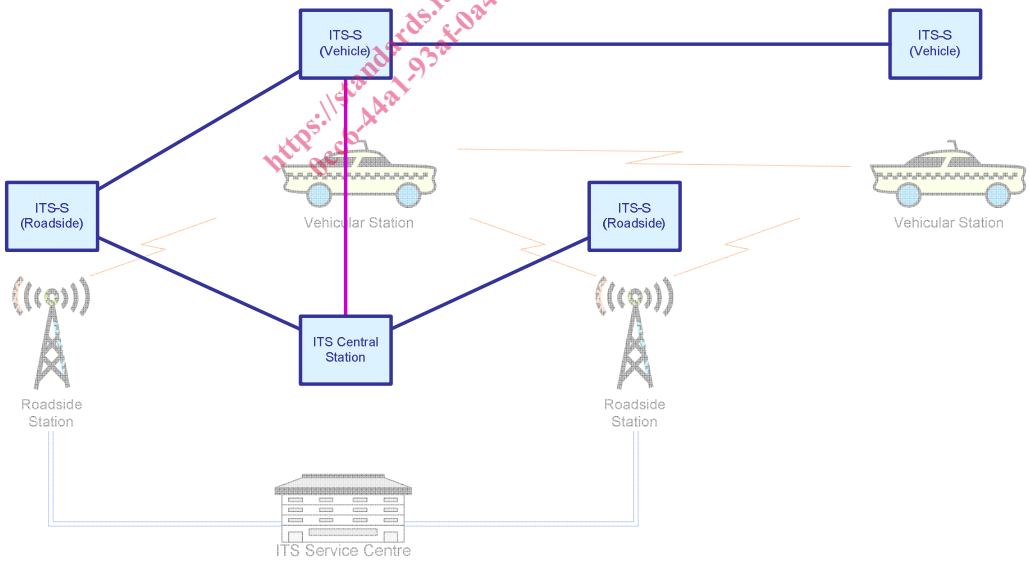

Figure 2: ITS functional entities

For the purpose of the TVRA, reference points are named and mapped to the ITS functional model as shown in Figure 3. The physical interface at reference point K may be implemented in a number of ways but, within the ITS functional model, the reference point itself represents the direct management relationship that an in-vehicle ITS station may have with the ITS infrastructure for the purpose of maintaining security parameters such as cryptographic keys.

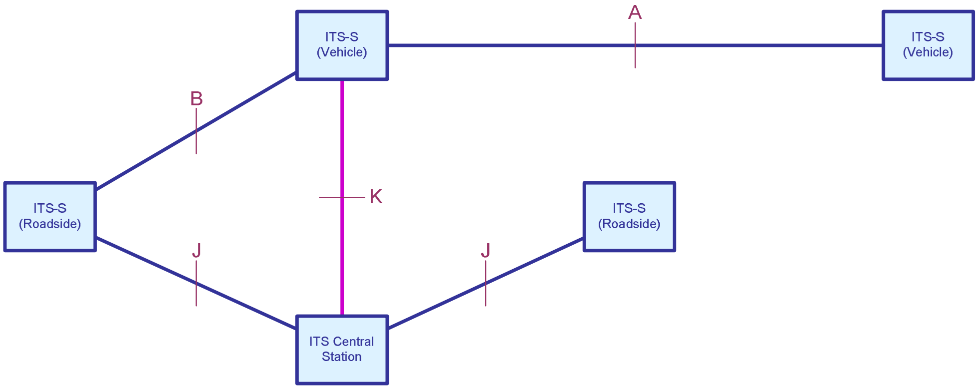

Figure 3: ITS functional model with reference points

The reference points indicated in Figure 3 are defined as follows:

- A describes the temporary relationship between two vehicles.
- B describes the temporary relationship between a vehicle and a roadside station.
- J describes the relationship between an ITS roadside station and the ITS network infrastructure.
- K describes the relationship between an ITS vehicle station and the ITS network infrastructure.

For the purpose of this TVRA, the interfaces at A and B are assumed to use communications in the 5,9 GHz band. It is also assumed that the interface at K could be routed to the ITS infrastructure indirectly through a roadside station, also in the 5,9 GHz band.

5.2 The Basic Set of Applications (BSA)

The Basic Set of Applications (BSA) [i.1] represents the mandatory set of services to be deployed in an ITS station. The BSA is described as a collection of traffic and transport use cases. For the purposes of the TVRA, these have been re-specified in clause 5.3 as a much smaller set of communications services.

The use cases in the BSA and, thus, included in the TVRA are as follows:

1) Stationary vehicle warning - accident/vehicle problem.
2) Traffic condition warning (includes traffic jam ahead warning).
3) Signal violation warning (includes stop sign violation).
4) Road work warning.
5) Collision Risk Warning from RSU.
6) Decentralized Floating Car Data - Precipitations/Road Adhesion/Visibility/Wind.
7) Regulatory/Contextual speed limits.
8) Traffic information & Recommended itinerary.
9) Limited access, detour notification.
10) In-vehicle signage.

5.2.1 BSA use case descriptions

The following clauses provide a brief description of the use cases within the BSA. Communication patterns and message repetition rates are specified in TS 102 637-1 [i.2] and TS 102 637-4 [i.11].

5.2.1.1 Stationary vehicle warning

A stationary vehicle at a potentially dangerous location periodically sends out a warning to other vehicles. The information may also be forwarded by available Road-Side Units (RSU) to a traffic management centre.

5.2.1.2 Traffic condition warning

Warning other vehicles about a detected potentially dangerous traffic condition.

5.2.1.3 Signal violation warning

When a signal violation is detected, all potentially affected vehicles are warned. The detection is done in the road side unit.

NOTE: Use cases 5.2.1.3 and 5.2.1.5 are similar

5.2.1.4 Road work warning

A mobile road infrastructure component distributes messages to warn affected vehicles about road works.

5.2.1.5 Collision risk warning from RSU

Detect potential collisions of vehicles that cannot directly communicate and warn the drivers.

NOTE: Use cases 5.2.1.3 and 5.2.1.5 are similar

5.2.1.6 Decentralized floating car data

Detect potential local dangers and send out warning message to potentially affected vehicles. Different warning reasons can be precipitation, road adhesion, visibility, or wind.

5.2.1.7 Regulatory/contextual speed limits

Road side infrastructure broadcasts speed limits that can be

- regulatory, i.e. set by an authority; or
- contextual, e.g. reduced limit due to rain.

NOTE: Use cases 5.2.1.7 and 5.2.1.10 are the same.

5.2.1.8 Traffic information & recommended itinerary

Broadcast traffic conditions. May also cause vehicles to download the recommended itinerary over a different channel.

5.2.1.9 Limited access warning, detour notification

Broadcast access restrictions, e.g. due to road works. May also provide detour advice in the same messages.

5.2.1.10 In-vehicle signage

Traffic sign information is broadcasted to be displayed in the vehicle.

NOTE: Use cases 5.2.1.7 and 5.2.1.10 are the same.

5.2.1.11 Emergency vehicle warning

An emergency vehicle periodically broadcasts its position, speed and heading as well as whether it has its siren on and/or its blue light (or equivalent) in use.

5.2.1.12 Slow vehicle warning

A slow vehicle periodically broadcasts its presence and thus encourages other vehicles to overtake. The broadcast information contains an indication that this is a special type of vehicle, called "slow vehicle".

5.2.1.13 Motorcycle warning

A motorcycle periodically broadcasts its presence. If other vehicles detect the imminent danger of collision, a warning is issued. The information broadcast contains an indication that this is a special type of vehicle, called "motorcycle".

5.2.1.14 Emergency electronic brake lights

Warn vehicles behind of a sudden slowdown. Broadcast respective message.

5.2.1.15 Wrong way driving warning

Warn vehicles in front of a detected violation of a one-way road. Broadcast respective message.

5.2.1.16 Traffic light optimal speed advisory

A traffic light to broadcasts timing data associated with its current state (e.g. time remaining before switching between green, amber and red).

5.2.1.17 Point of Interest notification

Road side unit periodically sends information about local services. The vehicle may establish a unicast connection to request more information.

NOTE: Use cases 5.2.1.17 through 5.2.1.19 are similar and mainly distinguished by the protocols used over the transparent communication channel.

5.2.1.18 Automatic access control and parking management

A road side unit periodically broadcasts the presence of an access controlled area. Vehicles requiring access provide credentials authorizing the access in unicast communications.

5.2.1.19 Local electronic commerce

A road side unit periodically broadcasts the presence of local electronic commerce. Vehicles requiring access provide credentials authorizing the access in unicast communications.

5.2.1.20 Enhanced route guidance and navigation

Road side unit periodically sends service announcements containing links to "known navigation support servers".

NOTE: Use cases 5.2.1.20 through 5.2.1.26 are similar and mainly distinguished by the type of service advertised and the respective service protocols.

5.2.1.21 Media downloading

A road side unit periodically broadcasts the presence of the possibility to download media files. Vehicles establish a unicast connection and download required media data.

5.2.1.22 Insurance and financial services

A road side unit periodically broadcasts the presence of the insurance and financial services. Vehicles establish a unicast connection and uses the services.