



**Intelligent Transport Systems (ITS);
Security;
Feature specific Threat, Vulnerability and
Risk Analysis (TVRA);
Part 1: Infield Test mode, Quantum safety;
Release 2**

Reference

DTR/ITS-00546

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced in any form or by any means except for the purpose of implementation of standards.

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.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	6
3.3 Abbreviations	6
4 The TVRA Method	7
Annex A: Application Note - Quantum Computing attack on cryptographic protections of ITS.....	8
A.1 Overview of threat and form of attack	8
A.2 Scope of a quantum computing attack in ITS	8
A.3 Impact of the quantum computing attack in ITS.....	9
A.4 Risk assessment of quantum computing attack in ITS.....	9
A.5 Countermeasure considerations for quantum computing attack on ITS.....	9
A.6 Specific considerations for QSC in C-ITS	10
A.7 QSC support by modification of the C-ITS security model	12
Annex B: Application Note - Impact of in-field testing mode on ITS operation.....	14
B.1 Overview of threat and form of attack	14
B.2 Identification of delta Target Of Evaluation (TOE).....	15
B.3 Identification of security objectives	16
B.3.1 Purpose.....	16
B.3.2 Confidentiality.....	16
B.3.3 Integrity.....	16
B.3.4 Authenticity.....	17
B.3.5 Availability.....	17
B.4 Quantitative risk analysis for ITM	17
B.5 Security countermeasure identification	17
History	19

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

The present document is part 1 of a multi-part deliverable, each part containing one of more specific application notes documenting the TVRA results for a specific application.

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.

1 Scope

The present document summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of a number of aspects of an Intelligent Transport System (ITS) by means of application notes. Each application note is addressed in a distinct sub-part and considers the threat to existing and planned vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.2] operating in a fully deployed ITS.

The present document extends but does not replace previous publications addressing TVRA in ITS, e.g. in ETSI TR 102 893 [i.16].

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".
- [i.2] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Release 2".
- [i.3] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".
- [i.4] ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".
- [i.5] ETSI TR 103 949: "Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study".
- [i.6] ETSI TS 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".
- [i.7] ETSI TS 103 300-2: "Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2".
- [i.8] CCMB-2022-11-001: "Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model", November 2022, Revision 1.
- [i.9] CCMB-2022-11-002: "Common Criteria for Information Technology Security Evaluation; Part 2: Security functional components", November 2022, Revision 1.