Draft ETSI TS 103 300-2 V0.4.1 (2020-01)

DRAFT

Intelligent Transport System (ITS);
Vulnerable Road Users (VRU) awareness;
Part 2: Functional Architecture and Requirements definition
Release 2

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ITS only. ETSI and its Members accept no liability for any further use/implementation of this Specification.

Approved and published Specifications and reports shall be obtained exclusively via the ETSI Standards Search at http://www.etsi.org/standards-search

Reference
DTS/ITS-00186

Keywords
ITS, Vulnerable Road Users, Automotive

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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.

© ETSI 2019.
All rights reserved.

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

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Executive summary 5
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 9
3.1 Terms 9
3.2 Symbols 10
3.3 Abbreviations 10
4 General overview 11
4.1 Introduction 11
4.2 Abstracted flow from use cases 12
4.3 Analysis of possible messages for each use case described in [i.1] 13
4.4 VRU system physical architecture 14
4.5 Security analysis of VRU use cases 16
4.5.0 Introduction 16
4.5.1 UC-A1: Sharing pavement between pedestrian and cyclists 18
4.5.2 UC-A2: Pedestrian crossing a road with an e-scooter approaching 18
4.5.3 UC-B1: Active roadwork 19
4.5.4 UC-B2: VRU crossing road 20
4.5.5 UC-B3: Rider is ejected from his motorbike 20
4.5.6 UC-B4: Emergency electronic brake light 21
4.5.7 UC-B5: Motorcycle approach indication / motorcycle approach warning 22
4.5.8 UC-C1: Signalling VRU hidden by an obstacle 22
4.5.9 UC-D1: Signalled few VRUs in a protected area 23
4.5.10 UC-D2: Non equipped VRUs crossing a road 24
4.5.11 UC-D3: VRUs crossing at a zebra protected by a traffic light 24
4.5.12 UC-D4: Scooter / bicyclist safety with turning vehicle 25
4.5.13 UC-E1: Network assisted vulnerable pedestrian protection 26
4.5.14 UC-E2: Detection of an animal or pedestrian on a highway 27
4.5.15 UC-F1: Signalled many VRUs in a protected area 28
4.5.16 UC-F2: Intelligent traffic lights for all 29
5 VRU related requirements 30
5.1 Introduction 30
5.2 Functional requirements 31
5.2.1 System requirements 31
5.2.2 Communication requirements 34
5.2.3 Security requirements 36
5.3 Operational requirements 37
5.3.1 System requirements 37
5.3.2 Communication requirements 39
5.3.3 Security requirements 41
5.4 Additional recommendations 41
6 Functional architecture of the VRU system 43
6.1 VRU profile specification 43
6.2 VRU cluster specification 47
6.2.1 VRU cluster concept 47
6.2.2 VRU cluster requirements 47

DRAFT

6.2.3 VRU cluster reference position ... 48
6.2.4 VRU cluster approach ... 48
6.3 VRU system functional architecture ... 49
6.4 VRU-related functions in the ITS station architecture ... 50
6.5 Function descriptions (informative) ... 51
6.5.1 General overview ... 51
6.5.2 VRU sensor system - IoT platform ... 52
6.5.3 Local Sensor data fusion and actuator (including AI) ... 52
6.5.4 Local perception ... 52
6.5.5 Motion dynamic prediction ... 52
6.5.6 Vehicle motion control ... 53
6.5.7 Human – Machine Interface (HMI) ... 53
6.5.8 Connected System / Information System ... 53
6.5.9 Traffic Management System ... 54
6.5.10 ITS Station Application Layer ... 54
6.5.10.1 Global overview ... 54
6.5.10.2 Device role setting ... 54
6.5.10.3 Remote Sensor data fusion and actuator (including AI) ... 54
6.5.10.4 Cooperative Perception ... 55
6.5.10.5 Collision risk analysis ... 56
6.5.10.6 Collision risk avoidance ... 57
6.5.10.7 Event detection ... 57
6.5.10.8 Infrastructure services ... 58
6.5.10.9 Manoeuvre coordination ... 58
6.5.11 ITS Station Facilities Layer ... 58
6.5.11.1 VRU basic service ... 58
6.5.11.2 LDM ... 60
6.5.11.3 PoTI ... 61
6.5.11.4 Other Application Support Facilities: CA, DEN, CPS, MCS, SPaT, etc. ... 61
6.5.11.5 Decentralized Congestion Control (DCC-FAC) ... 61
6.5.12 ITS Station Management Entity ... 61
6.5.12.1 VRU profile management ... 61
6.6 Security considerations ... 62
6.6.2.1 Overall roles ... 62
6.6.2.2 Entitlement to roles ... 63
6.7 Impact of the deployment and automation level roadmap ... 64
6.8 Interfaces between entities ... 67
6.8.1 Introduction ... 67
6.8.2 External interfaces ... 67
6.8.3 Internal interfaces ... 68
6.8.4 VRU Basic Service interfaces ... 70
6.9 Vulnerable Road User Awareness Message, VAM ... 70

7 Impact on existing standards and protocols ... 71
7.1 Introduction ... 71
7.2 Facilities Layer ... 71
7.3 Networking & Transport Layer ... 72
7.4 Access Layer ... 72
7.5 Management Entity ... 72
7.6 Security Entity ... 72

8 Conclusion ... 72

Annex A (informative): New potentialities for decision ... Error! Bookmark not defined.
A.1 More accurate profile types and clusters ... **Error! Bookmark not defined.**
A.1.1 Objectives ... **Error! Bookmark not defined.**
A.1.2 Profile specification ... **Error! Bookmark not defined.**
A.1.3 VRU cluster management ... **Error! Bookmark not defined.**
A.2 VRU motion dynamic prediction ... **Error! Bookmark not defined.**

Annex (informative): Bibliography ... **74**

Annex (informative): Change History ... **75**

DRAFT

History 76

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (TC ITS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Executive summary

The present document is Part 2 of a set of VRU-related specification set.

Part 1 provides a definition of the Vulnerable Road Users (VRU) system and its components. It describes and categorises typical use cases relevant to traffic safety that involve road users such as pedestrians, bicyclists, e-scooters, motorcycles and road workers and are enabled by Cooperative Intelligent Transport Systems. The Technical Report concludes with a preliminary analysis of the challenges to be solved by the VRU awareness basic service.

Part 2 defines the VRU related requirements, as well as the functional architecture of the VRU system. In addition, it will analyse the impact of use cases, requirements and functional architecture on existing standards (for instance the Cooperative Awareness Message (CAM) European Standard [i.2]).

Part 3 will specify the VRU awareness basic service. It will define the communication protocols, message format, semantics and syntax as well as key interfaces and protocol operation for the VRU awareness service.

The present document builds on the analysis presented in the Part 1 Technical Report.

The first major section, section 4, provides an overview of the system architecture, recommends information flows for VRU use cases for which a specific Vulnerable Road User Awareness Message (VAM) should be defined, and presents a security analysis of the use cases from the Part 1 Technical Report. The security analysis is to be used in section 5 to derive security requirements.

DRAFT

The next section presents formal functional and operational requirements for system, communications, and security.

The next section outlines the functional architecture of the VRU system. Within this section:

- VRU device profiles are defined. VRU profiles distinguish between different types of VRU based on their likely behaviour. The profiles defined in this document cover pedestrians, cyclists, motorcyclists, and animals. The goal of this section is to allow implementers to target specific VRU profiles with their devices, so that they can produce specialized devices at lower cost.
- There is an extensive discussion of VRU clustering. VRU clustering is a technique used to reduce traffic on the airlink by allowing VRU devices, under particular conditions, to delegate responsibility for sending VAMs to a device known as the "cluster leader", which is associated with a different VRU within the cluster.
- There is an extensive discussion of the services that are used by a VRU application running on a VRU ITS-S and how they are to be situated within the ITS-S architecture.
- The section also describes the uses of the different interfaces with a VRU system.

Finally, the document discusses any necessary changes to the ITS-S application and facilities layers, and to the Station Management and Security Management entities within the ITS-S.

Introduction

VRU applications extend the awareness of and/or about Vulnerable Road Users such as motorcycles, bicycles, pedestrians and more impaired traffic participants in the neighbourhood of other traffic participants. They enable further improvement of traffic safety and management based on both direct ITS station-to-ITS station communications and via a third party ITS station (e.g. vehicle or road-side equipment).

The present document specifies the VRU system requirements and architecture building form the analysis of the use cases described in TR 103 300-1 [i.1]. These specifications lead to recommendations for updates of existing C-ITS standards.

DRAFT

1 Scope

The present document defines the VRU related requirements, as well as the functional architecture of the VRU system that will prevent collisions with other road users. In addition, it analyses the impact of use cases, requirements and functional architecture on existing standards, identifying which messages are needed to support the use cases described in [i.1].

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

The following referenced documents are necessary for the application of the present document.

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

[2] ETSI TS 102 894-1: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications"

[3] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[4] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[5] ETSI EN 302 890-2: " Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Facility Position and Time management (PoTi). [Release 2]".

[6] ETSI TS 103 097: “Intelligent Transport Systems (ITS); Security; Security header and certificate formats”

[7] ETSI TS 101 539-1 “Intelligent Transport System (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification “.

[8] ETSI TS 102 731: “Intelligent Transport Systems (ITS); Security; Security Services and Architecture”

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.

DRAFT

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 TR 103 300-1: "Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 1: Use Cases definition; Release 2".

[i.2] Deliverable D4.2: " Architecture for integration of VRUs and draft recommended practices for usability & user acceptance", Project H2020 VRUITS, December 2014

[i.3] SAE Surface Vehicle Standard J2945/5, Service Specific Permissions and Security Guidelines for Connected Vehicle Applications.

[i.4] ETSI TR 103 562: "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS)".

[i.5] C-ITS Platform, Final report Phase II, September 2017

[i.6] SAE J2945/9 (March 2017): "Vulnerable Road User Safety Message Minimum Performance Requirements".

[i.7] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)"

[i.8] Internet Engineering Task Force (IETF) Request for Comments (RFC) 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", available from https://tools.ietf.org/html/rfc8446

[i.9] Internet Engineering Task Force (IETF) Request for Comments (RFC) 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", available from https://tools.ietf.org/html/rfc5246

[i.10] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management"

[i.11] ETSI TS 103 300-3: "Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2".

[i.12] ETSI EN 302 890-1V1.2.1: " Intelligent Transport Systems (ITS); Facilities Layer function; Part 1: Services Announcement (SA) specification"

[i.13] ETSI TS 103 301 V1.2.1: " Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services"

[i.14] ETSI TS 102 894-2 V1.3.1: " Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary"

[i.15] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles.

NOTE: Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0168&from=EN.

[i.16] ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements

[i.17] FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) PUBLICATION 199 (FIPS 199): Standards for Security Categorization of Federal Information and Information Systems

[i.18] ETSI TS 103 175: "Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium"

[i.19] SAE J3016™ "Levels of Driving Automation"

[i.20] Yingying Zhang, Danya Yao, Tony Qiu, Lihui Peng: "Scene-based pedestrian safety performance model in mixed traffic situation", IET Intelligent Transportation Systems 2014, Vol. 8 Issue 3, pp 209-218

DRAFT

[i.21] Ahmed Tageldin, Mohamed Zaki, Tarek Sayed: "Examining pedestrian evasive actions as a potential indicator for traffic conflicts", IET Intelligent Transportation Systems 2017, Vol. 11 Issue 5, pp 282-289.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in [i.1] [8], and the following apply:

actor: participant in a use case

attestation: process by which a device proves to another party that it is in a known valid state

authorization authority: security management entity responsible for issuing, monitoring the use of, and withdrawing authorization tickets(from [8])

authorization ticket: data object that demonstrates that the valid holder is entitled to take specific actions (from [8])

availability: security service providing assurance that intended recipients of certain data will in fact receive that data

blacklisting: process by which an authorization authority is instructed not to issue authorization tickets to an end entity in future

certificate: type of authorization ticket; a digital document issued by a trusted third-party binding properties (identity or permissions) to a cryptographic public key, so that use of the corresponding private key (typically to sign a message) gives assurance that the private key holder has the indicated properties

combined VRU: combination of a VRU and a VRU vehicle (e.g. bicycle, wheel chair)

confidentiality: security service providing assurance that unauthorized parties cannot read certain data

dynamic state: collection of properties of a moving object including position, velocity, acceleration, mass, and forces acting on the object, that allow path prediction

end-entity: user of an authorization ticket

homogeneous VRU cluster: VRU cluster composed of VRU belonging to the same VRU profile.

heterogeneous VRU cluster: VRU cluster composed of VRU belonging to different VRU profiles

integrity: security service providing, in the context of this document, assurance that certain data and associated metadata are correct. (This term has a narrower meaning in other contexts, but the definition given is the definition used in this document)

misbehaviour: sending messages within an application that cause undesirable actions to be taken by the receivers

misbehaviour detection: process whereby a receiver of messages determines that those messages constitute misbehaviour

misbehaviour reporting: process whereby an actor that has carried out misbehaviour detection, reports the misbehaving messages to a central authority to determine whether the originating device should be blacklisted

pseudonymity: a security service providing protection against an unauthorized party being able to determine that multiple different messages have come from the same source. Only needed when confidentiality services are not applied

role: a property of an actor in a system indicating what activities they are entitled to carry out or request within that system

security control: a feature of a system included in order to achieve a security goal of the system

security goal: a system requirement to ensure that the system has the appropriate security properties

DRAFT

security property: one of confidentiality, integrity, availability, and pseudonymity

sensitivity level: an estimate of the impact of a failure of one of the security properties of a system low, medium or high.

service specific permissions: field in an ETSI TS 103 097 certificate (or, equivalently, an IEEE 1609.2 certificate), bound to a specific ITS Application Identifier (ITS-AID), indicating the permissions of the certificate holder to carry out specific activities within the set of activities defined by that ITS-AID

Time To Collision (TTC): important calculated data element enabling the selection of the nature and urgency of the collision avoidance action to be undertaken

NOTE: This variable is related to other variables such as the road state, the weather conditions, the vehicle / VRU action capabilities. In the present document, TTC is used as a trigger for certain activities, such as starting to transmit VAMs or taking some avoidance/mitigation action. Research has been carried out on alternative metrics such as Post-Encroachment Time (PET) and Permutation Entropy (PE) (see [i.20] [i.21]). The use of TTC in the present document is not meant to preclude the use of other metrics that may be used to fulfil the safety goals of the applications, and in particular the present document does not prescribe a specific means for calculating TTC, specifically in order to support improvements in this algorithm in the future.

velocity: vector indicating speed in a particular direction (from EN 302 890-2 [5])

Vulnerable Road Users (VRU): non-motorized road users as well as users of VRU vehicles

NOTE: A VRU can only be living being. This living being is only considered as a VRU when it is in the context of a safety related traffic environment.

VRU application: application extending the awareness of and/or about Vulnerable Road Users such as motorcycles, bicycles, pedestrians and impaired traffic participants in the neighbourhood of other traffic participants

VRU cluster: set of VRUs moving in a coherent manner, i.e. with coherent velocity or direction

NOTE: A cluster of VRUs can be homogeneous (set of pedestrians, of bicycles) or heterogeneous (pedestrians with e-scooters, bicycles). A combined VRU is not a heterogeneous cluster.

VRU device: portable device used by a VRU integrating a standard ITS station

NOTE: The definition of an ITS station is given in ETSI EN 302 665 [1]. A VRU device can also integrate applications interfacing the ITS-S. For example, an application can improve the VRU trajectory prediction by learning continuously from its behaviour when sharing the space with other road users.

VRU ITS-S: P-ITS-S / V-ITS-S capable of handling VRU related ITS applications

VRU system: ensemble of ITS stations interacting with each other to support VRU use cases, e.g. personal ITS-S, vehicle ITS-S, roadside ITS-S or Central ITS-S

VRU vehicle: L class of vehicles (for example mopeds or motorcycles, etc.), as defined in Annex I of EU regulation 168/2013 [i.15] and light unpowered vehicles (bicycles, skates, wheelchairs, prams)

3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

VOID

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in [i.1] and the following apply:

AA	Authorization Authority
AT	Authorization Ticket
CAM	Cooperative Awareness Message

DRAFT

CDD	Common Data Dictionary
C-ITS	Cooperative ITS
CIA	Confidentiality, Integrity, Assurance
CPM	Cooperative Perception Message
CPS	Cooperative Perception Service
DCC	Decentralized Congestion Control
DENM	Decentralized Environmental Notification Message
EMI	Electromagnetic Interferences
FIPS	Federal Information Processing Standard
GN	GeoNetworking
IETF	Internet Engineering Task Force
IoT	Internet of Things
ITS	Intelligent Transport System
ITS-AID	ITS Application Identifier
ITS-S	ITS Station
IVI	In Vehicle Information
MaaS	Mobility as a Service
MCM	Manoeuvre Coordination Message
MCS	Manoeuvre Coordination Service
NIST	National Institute of Standards and Technology
P-ITS-S	Personal ITS station
POI	Point Of Interest
PoTi	Position and Time
PSM	Personal Safety Message
PTW	Powered Two-Wheelers
RFC	Request For Comments
RHS	Road Hazard Signalling
R-ITS-S	Roadside ITS Station
RSE	Road Side Equipment
RX	Receive
SAE	Society of Automotive Engineers
SPaT	Signal Phase and Timing
SSP	Service Specific Permissions
TDTC	Time Difference To Collision
TLS	Transport Layer Security
TMS	Traffic Management System
TR	Technical Report
TS	Technical Specification
TTC	Time-To-Collision
TVRA	Threat, Vulnerability and Risk Analysis
TX	Transmit
UC	Use Case
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle-to-everything
V-ITS-S	Vehicle ITS Station (VRU or non-VRU)
VAM	VRU Awareness Message
VRU	Vulnerable Road User

4 General overview

4.1 Introduction

The present document specifies the requirements and the architecture of the VRU system and ITS Station (ITS-S), based on the results and analysis performed in TR 103 300-1 [i.1]. It describes the different functions involved in this architecture as well as their interfaces. Finally, it provides the impact of the VRU basic service introduction on other C-ITS standards and protocols.

DRAFT

A vulnerable road user (VRU) is considered to be a living being which participates in the road traffic. Such a living being is only in a role of a VRU when it acts in a safety related traffic context. As such, a VRU can also be assumed in other than road context, e.g. rail context.

Based on this definition, a bicycle or scooter itself is not considered as a VRU as long as no person is using this equipment. As long as the rider is on the bicycle, the combination (cluster) is a VRU, but as soon as the person is separated from the bicycle, the object "bicycle" is no longer a VRU. A standalone bicycle should not to be protected as a VRU but signalled by a CPM or DENM as an object on the road. Transport devices which can become a VRU when used by a person in a safety related traffic context are called VRU vehicles.

Based on the analysis in TR 103 300-1 [i.1] the transmission of a VRU standard message is needed in a large majority of use cases. The present document introduces this VRU standard message, named VAM for VRU Awareness Message, designed as a separate message, as described in Clause 6.9. The main advantages are to differentiate it from the CAM, making it a more flexible and potentially smaller message, as well as the harmonisation with the Personal Safety Message (PSM) standardised in SAE J2945/9 [i.6].

As described in TR 103 300-1 [i.1], a VRU device can be of one of the three types defined in Table 1 below.

Table 1: VRU device types

VRU device type	Description of VRU device
VRU-Tx	The device contains an ITS-S, having only a transmitter (no receiver) that broadcasts awareness messages or beacons about the VRU. The VRU device is however able to comply with Decentralized Congestion Control (DCC) rules.
VRU-Rx	The device contains an ITS-S, having only a receiver and an HMI to receive messages from other ITS-S and can act upon the information received, e.g. inform or warn the VRU.
VRU-St	The device contains an ITS-S that includes the VRU-Tx and VRU-Rx functionalities.

The number of VRUs operating in a given area can get very high (see for example Use Case UC-B2 in [i.1], pedestrian crossing, where numbers can reach 500 or more) or the VRU can be combined with a VRU vehicle (e.g. rider on a bicycle). In order to reduce the amount of communication and thus the resource usage, VRU should be grouped together leading to VRU clusters which are indicated to other road users using a single VAM, rather than a VAM for each participant. These clusters can be homogeneous VRU clusters (for example group of pedestrians) or heterogeneous VRU clusters (rider on a bicycle). Each cluster is considered as a single entity and only the cluster head will transmit the VAM. The parameters of the VRU cluster will be disseminated using the VAM.

4.2 Abstracted flow from use cases

The use cases in [i.1] have shown the following steps (compiled as an abstraction of the use cases), with different alternatives. These steps were also highlighted by the VRUITS project.

1. Detection of the VRU presence. The alternatives are:
    - VRU self-positioning. The VRU has sensors and potentially other sources allowing it to determine its own properties, including its location and velocity.
    - Another road user (e.g. a V-ITS-S) detects and tracks the VRU.
    - Roadside equipment connected to an R-ITS-S detects and tracks the VRU.
2. Evaluation whether the VRU is at potential risk from other road users and VRU position and dynamic state should be transmitted. Any party may transmit information about VRUs that it is aware of. Information on VRUs should be filtered and only be transmitted according to the message triggering conditions. The potential risk from other road users depends on the following conditions, among others:
    - Presence of other road users.
    - Road layout.
    - Dynamic state of the VRU and the other road users.
    - Traffic signal status for both VRU and vehicles, if relevant, and compliance to traffic lights.
3. Evaluation of safety message environment, specifically whether the VRU is part of a cluster, to determine whether the VRU's own ITS-S should transmit.
4. Transmission of information about at-risk VRU. Alternatives:
    - VRU sends ego-status information.
    - VRU cluster leader sends cluster information.

- R-ITS-S or another road user sends information about a VRU in a potential risk situation.

5. Risk assessment. Phases (receiver side):
    - Fusion of sensor data, and observed information transmitted by other road users to build a local dynamic map, with information about road users' location, velocity and potentially other data, e.g. intention.
    - Assessment of risk based on estimated trajectory and velocity of different road users.
6. Warning or action to protect the VRU.
    - warning of the device carrier (VRU or any other road user).
    - transmission of collision warning to other road users.
    - action in the case of an automated vehicle.

4.3 Messages for the use cases described in [i.1]

This clause summarizes the C-ITS standardized messages that are involved in each of the use cases in the description in [i.1]. Its objective is to highlight the use cases defined in [i.1] that require new or revised message standards.

DRAFT

Table 2: C-ITS messages for [i.1] use cases

UC-	Description	Existing standard messages						VAM	Comments
		CAM	DENM	SPAT	MAP	CPM	MCM		
A1	Sharing pavement between pedestrian and cyclists		X					X	VAM is used for awareness between VRUs, DENM is used for warning of a potential risk of collision (applies to all use cases below)
A2	Pedestrian crossing a road with an e-scooter approaching		X					X	
B1	Active Roadwork	X	X					X	
UC-B2	VRU crossing a road	X	X				X	X	
UC-B3	Rider is ejected from his motorbike	X	X				X	X	
UC-B4	Emergency Electronic Brake Light	X	X						This UC is already covered by existing C-ITS messages
UC-B5	Motorcycle Approach Indication / Motorcycle Approach Warning	X						X	
UC-C1	Signalling VRU hidden by an obstacle	X	X			X		X	
UC-D1	Signalled few VRUs in a protected area	X	X			X	X	X	
UC-D2	Non equipped VRUs crossing a road	X	X			X	X		
UC-D3	VRUs crossing at a zebra protected by a traffic light	X	X	X		X	X	X	
UC-D4	Scooter/Bicyclist Safety with Turning Vehicle		X			X	X	X	
UC-E1	Network assisted vulnerable pedestrian protection	X	X			X	X	X	
UC-E2	Detection of an animal or pedestrian on a highway		X			X	X	X	
UC-F1	Signalled Many VRUs in a protected area	X	X		X	X	X	X	
UC-F2	Intelligent traffic lights for all (P2I2V)	X		X			X	X	

NOTE: For UC-E2, the CAM is not used as it is not involved in the use case described. It could be present in an alternative use case when the central station disseminates a warning only in the case when it has detected an actual risk of collision, using the CAMs transmitted by the vehicles for this evaluation.

4.4 VRU system physical architecture

The physical architecture is shown in Figure 1. This figure is derived from the physical architecture defined by the VRUITS project in [i.2]. It consists of three main components:

- VRU's (noted VRU), including combined VRUs and VRU clusters. The VRU ITS-S may be a personal ITS-S (P-ITS-S) or a vehicular ITS-S (V-ITS-S) depending on the type of road user.
- Non-VRU Vehicles (noted V), using V-ITS-S
- Infrastructure (noted I), made of R-ITS-S or C-ITS-S.

DRAFT

NOTE: A motorcycle is considered as a VRU from VRU Profile 3 (see clause 6.1) when it moves below a certain speed. It then sends VAM. Above that speed it is considered as a non-VRU vehicle and transmits CAM messages. Both are exclusive. This behaviour applies only to VRUs from VRU Profile 3. TS 103 300-3 [i.11] will specify this behaviour with more details, including how this is operated with the use of security certificates.

The overall environment comprises ITS stations (ITS-S), illustrated in Figure 2, that may communicate directly as follows:

- from VRU to Vehicle and vice versa (VRU2V / V2VRU)
- from VRU to VRU (VRU2VRU)
- from VRU to Infrastructure and vice versa (VRU2I / I2VRU)
- from Vehicle to Vehicle (V2V)
- from Vehicle to Infrastructure and vice versa (V2I / I2V).

Figure 1: VRU system physical architecture (adapted from VRUITS project)

DRAFT

Figure 2: ITS-Stations (ITS-S) in the VRU system

Figure 2 illustrates the notion of VRU ITS-S (left pane) and non-VRU-ITS-S (right pane).

The arrows in the diagram indicate sub-classes. VRU vehicle ITS-S is a sub-class of V-ITS-S, as shown by the arrows in Figure 2.

NOTES:

1) A P-ITS-S can take the role of a V-ITS-S, e.g. when connected to a VRU vehicle such as a motorbike. In this case it can deploy VRU protocols sending VAMs, e.g. in the case of a combined VRU composed of a VRU and a VRU vehicle. This happens when there is no VRU device in the VRU vehicle.

2) It is necessary to distinguish between the physical implementation (P-ITS-S, V-ITS-S, R-ITS-S and C-ITS-S) and the role of the communication mechanisms deployed. Role and communication mechanisms can be deployed synchronously, e.g. a V-ITS-S can send out vehicular related messages or VRU related messages depending on its role.

3) A physical implementation of a VRU-only ITS-S is possible. This is not a full P-ITS-S but rather a subclass of P-ITS-S. This station can only deploy VRU related protocols, it might be a TX-only device (but still complying with DCC) or a device with limited capabilities. This might be needed to reduce power consumption and costs. These devices might not be capable of taking the role of a VRU cluster head.

4.5 Security analysis of VRU use cases

4.5.0 Introduction

This clause presents the security analysis of the VRU use cases considered in [i.1] and in the present document.

This security analysis considers each “entity activity” (i.e. each information flow with a particular goal) in the use cases. Each entity activity is rated as low, medium or high sensitivity with respect to the three security properties confidentiality (C), integrity (I) and availability (A) as identified in ISO 27001 [i.16] and Federal Information Processing Standard (FIPS) 199 [i.17].

- The confidentiality sensitivity measures how severe the effect is if information is read by a party that should not read it.
- The integrity sensitivity measures how severe the effect is if information is trusted by a party when the information is incorrect. This concept captures both intentionally false data, introduced by an attacker, and data that is honestly inaccurate without the receiver knowing it. (This meaning of “integrity” is different from its meaning in a purely cryptographic context – in that context the term simply means assurance that data has not been modified since it was created by a legitimate party and does not include considerations of data quality at the time of creation). The

DRAFT

integrity sensitivity level takes into account how the receiver is expected to behave on receipt of information, as this affects the impact of an integrity failure.
- The availability sensitivity measures how severe the effect is if information is not received by the party that relies on receiving it.

Sensitivity levels are categorized as low, medium or high: low indicates a limited adverse effect, medium indicates a serious adverse effect, and high indicates a critical or catastrophic effect. Confidentiality can also have sensitivity level of "none", indicating that the data is public.

As a guide to how to think about sensitivity levels, examples of possible adverse outcomes and the corresponding sensitivity levels are:

- Events that can cause false collision warnings are categorized as having integrity sensitivity "Low". These events are undesirable and should be mitigated but are extremely unlikely to lead to physical harm or to significant financial losses.
- Events that could cause a single collision are categorized as having integrity sensitivity "Medium". (Note that no such events are identified in the analysis below). This indicates that the outcome is extremely undesirable and should be prevented but that in the big picture it is possible to accept a non-zero number of these events.
- Events that could cause widespread collisions from a single event are categorized as having integrity sensitivity "High". (Note that no such events are identified in the analysis below). This indicates that the outcome is so severe that the system should not be deployed unless it can be guaranteed that no such false events will occur.

Note that as automated vehicles become more widespread, there will be an increased potential that "low" or "medium" sensitivity events can be scalable to create widespread incidents. The analysis on this document does not reflect this potential scalability and focuses on messages used to raise warnings to human drivers. The assumption here is that autonomous drivers will go through a process of fusion and decision similar to human drivers and will ultimately behave similarly to human drivers from the point of view of security. Cyber-vulnerabilities due to bad implementations of autonomous systems are not considered in this document as they are unpredictable and may have an impact that is unconnected with the initial use case, making analysis purely speculative.

The C/I/A analysis enables the derivation of security requirements.

One set of security requirements is derived directly from the sensitivity analysis: for any information flow, communications security mechanisms should be specified to meet the sensitivity requirements for confidentiality (provided by encryption) and integrity (provided by authentication) and communications assurance mechanisms should be specified to meet the sensitivity requirements for availability.

Additionally, the sensitivity requirements of the information flows involving a particular actor within the use case indicate security controls that the actor must implement. Those security controls can be physical, such as the inclusion of hardware security modules, and/or process or organizational, such as following a data management plan for secure storage and deletion of generated data or specifying particular methods to be used to determine that an actor is entitled to certificates with a particular set of permissions. These process controls can also include risk reduction measures taken on receipt of a message.

Within the set of integrity controls, one control that can be used to manage risk is separation of roles within the application. In this context, "separation of roles" means "identifying different groups of activities within the application such that an actor in one role can carry out activities from only some of those groups". If separate roles are needed, they will typically be addressed by defining a Service Specific Permissions (SSP) structure for the application. This matches the methodology recommended in SAE J2945/5 [i.3].

Separately, the security analysis should consider requirements for pseudonymity. Pseudonymity is in general required when devices operated by or associated with private citizens send messages with no confidentiality mechanisms applied. The standard pseudonymity mechanism is to provide those devices with multiple digital certificates, allowing the device to use different certificates to sign different messages and so inhibiting the ability of an eavesdropper to determine whether two messages sent at different times and in different places have come from the same device. Pseudonymity requirements are captured in the notes for the security analysis for each use case.

The present document does not present a full Threat, Vulnerability and Risk Analysis (TVRA) carried out per ETSI TS 102 165-1[i.7] as there are elements of the full TVRA process, such as estimating the attack likelihood, that are impossible for a system that has not yet been deployed and may depend on specifics of implementation.

DRAFT

4.5.1 UC-A1: Sharing pavement between pedestrian and cyclists

Table 3: Risk analysis: UC-A1: Sharing pavement between pedestrian and cyclists

Use case: Sharing pavement between pedestrian and cyclists			
Actors: Pedestrian VRU, Cyclist VRU			
Information flow	Entity activities	Description	Impact
IA1-1 Exchange messages	EA1-1.1 VRU → VRU	Broadcast of dynamic and other information about sending VRU	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.2 UC-A2: Pedestrian crossing a road with an e-scooter approaching

Table 4: Risk analysis: UC-A2: Pedestrian crossing a road with an e-scooter approaching

Use case: Pedestrian crossing a road with an e-scooter approaching			
Actors: Pedestrian VRU, Cyclist VRU			
Information flow	Entity activities	Description	Impact
IA2-1 Exchange messages	EA2-1.1 E-Scooter → Pedestrian	Broadcast of dynamic and other information about E-Scooter	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EA2-1.2 Pedestrian → E-Scooter	Broadcast of dynamic and other information about pedestrian	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective

DRAFT

IA2-2 Warn other vehicles	EA2-2.1 Pedestrian notifies passing-by vehicles	Warning of potential risk that E-Scooter will create hazard	C: None – broadcast model I: Low – False warning makes drivers drive more carefully, but they should be driving carefully in this environment anyway. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.3 UC-B1: Active roadwork

Table 5: Risk analysis: UC-B1: Active roadwork

Use case: Active roadwork			
Actors: Active worker (pedestrian) VRU, Local Vehicle, Remote Vehicle			
Information flow	Entity activities	Description	Impact
IB1-1 Exchange messages	EB1-1.1 Local Vehicle → Active Worker	Broadcast of dynamic and other information about local vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB1-1.2 Active Worker → Local Vehicle	Broadcast of dynamic and other information about active worker	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB1-1.3 Local Vehicle → Remote Vehicle	Broadcast of notification about presence of active worker	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB1-1.4 Remote Vehicle → Local Vehicle	Broadcast of dynamic and other information about remote vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective

DRAFT

	EB1-1.5 Local Vehicle → Active Worker	Broadcast of notification about presence of hazardous vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.4 UC-B2: VRU crossing road

Table 6: Risk analysis: UC-B2: VRU crossing road

Use case: VRU crossing road			
Actors: VRU, Vehicle			
Information flow	Entity activities	Description	Impact
IB2-1 Exchange messages	EB2-1.1 VRU → Vehicle	Broadcast of dynamic and other information about VRU	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB2-1.2 Vehicle → VRU	Broadcast of dynamic and other information about vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB2-1.3 Vehicle → VRU	Warning of collision risk	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.5 UC-B3: Rider is ejected from his motorbike

DRAFT

Table 7: Risk analysis: UC-B3: Rider is ejected from his motorbike

Use case: Rider ejected from motorbike			
Actors: Rider VRU-St, Motorbike VRU-St, Approaching Vehicle			
Information flow	Entity activities	Description	Impact
IB3-1 Exchange messages	EB3-1.1 Rider VRU-St → Motorbike VRU-St: communications to establish whether VRU is on board bike (NOTE: the exact mechanism used is not specified in this document and, while it may be based on VAMs from the motorbike, it may also be sensor based or based on non-C-ITS communications)	Information used by VRU device to determine whether VRU is still on motorbike	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB3-1.2 Motorbike VRU-St → Vehicle	Message warning of ejected VRU	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB3-1.3 Rider VRU-St → Vehicle	Message warning of ejected VRU	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in information flow EB3-1.2 and EB3-1.3 require pseudonymity. In information flow EB3-1.1 the actors do not necessarily require pseudonymity from each other but the mechanism used to implement information flow EB3-1.1 should provide pseudonymity from other road users. Notes: the security mechanism to be used for EB3-1.1 depends on the specific design of that information flow.			

4.5.6 UC-B4: Emergency electronic brake light

Table 8: Risk analysis: UC-B4: Emergency electronic brake light

Use case: Emergency Electronic brake light			
Actors: Braking ITS-S, Receiving ITS-S			
Information flow	Entity activities	Description	Impact

DRAFT

IB4-1 Exchange messages	EB4-1.1 Braking ITS-S → Receiving ITS-S	Broadcast of information about brake event	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.7 UC-B5: Motorcycle approach indication / motorcycle approach warning

Table 9: Risk analysis: UC-B5: Motorcycle approach indication / motorcycle approach warning

Use case: Emergency Electronic brake light			
Actors: Motorbike ITS-S, Vehicle ITS-S, Receiving ITS-S (which may be motorbike or vehicle)			
Information flow	Entity activities	Description	Impact
IB5-1 Exchange messages	EB5-1.1 Motorbike ITS-S → Receiving ITS-S	Broadcast of dynamic information about the VRU	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EB5-1.2 Vehicle ITS-S → Motorbike ITS-S	Broadcast of dynamic and other information about vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity.			

4.5.8 UC-C1: Signalling VRU hidden by an obstacle

Table 10: Risk analysis: UC-C1: Signalling VRU hidden by an obstacle

Use case: Signalling VRU hidden by an obstacle			
Actors: VRU, Sensor-equipped vehicle, Receiving vehicle			
Information flow	Entity activities	Description	Impact
IC1-1 Detect	EC1-1.1 Sensor-equipped vehicle detecting VRU	Sensor activity to detect VRU	C: None – VRU is detectable by any sensor-equipped vehicle

DRAFT

			I: Low – Impact of false sensor data is false warnings. A: Low – Any level of availability allows this use case to be effective
IC1-2 Warn	EC1-2.1 Sensor-equipped vehicle → Receiving vehicle	Perception message	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case require pseudonymity. NOTES: 1. The integrity requirement on EC1-1.1 reflects the requirement for integrity as applied to sensor data fed to the V-ITS-S on the sensor-equipped vehicle. ETSI TS 103 300-3 [i.11] may in practice not specify this information flow, in which case integrity mechanisms for this information flow will be out of scope. 2. Although the impact of an integrity failure is the same in this case (sensed VRU) as in other cases (self-reporting VRU), it may be appropriate to define an SSP-protected role for the sensor-equipped vehicle to provide assurance that vehicles that send the perception message have in fact been certified as being equipped with the appropriate sensors.			

4.5.9 UC-D1: Signalled few VRUs in a protected area

Table 11: Risk analysis: UC-D1: Signalled few VRUs in a protected area

Use case: Signalled few VRUs in a protected area			
Actors: VRU, RSE, Approaching vehicle			
Information flow	Entity activities	Description	Impact
ID1-1 Detect	ED1-1.1 Approaching vehicle → RSE	Broadcast of dynamic and other information about vehicle used to predict hazard situation	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
ID1-2 Warn	ED1-2.1 RSE → Approaching vehicle	Broadcast of warning about protected area	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	ED1-2.2 RSE → VRUs	Warning Siren	C: None – broadcast model

DRAFT

			I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: All actors in the use case except for the RSE require pseudonymity. Notes: 1. A false CAM in information flow ED1-1.1 may cause a false alarm. The result of a false alarm is an evacuation of the protected area. If the protected area is a work zone, this may result in damage to equipment being used in the protected area and prolonged disruption to work done in the protected area. Similarly, even if the protected area is not a work zone, it is possible (though not high probability) that VRUs will be injured during the evacuation. However, this still does not meet the threshold for Medium integrity sensitivity as it does not cause disruption, or a threat of physical damage, on a sufficiently large scale or with sufficiently high probability.			

4.5.10 UC-D2: Non equipped VRUs crossing a road

Table 12: Risk analysis: UC-D2: Non equipped VRUs crossing a road

Use case: Non equipped VRUs crossing a road			
Actors: Notifying ITS-S, Receiving vehicle			
Information flow	Entity activities	Description	Impact
ID2-1 Warn	ED2-1.1 RSE → Approaching vehicle	Broadcast of warning information of VRUs in road	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: The RSE is the only transmitter in this case and does not require pseudonymity. Notes: 1. This description omits the CAM used by the RSE to detect vehicles as this activity will happen anyway, outside the context of the VRU use case. 2. The traffic signal RSE in this case is assumed to be equipped with more sensors than a traffic signal RSE that simply sends SPaTs. This therefore creates a potential requirement for a role identifier (an SSP) that distinguishes between sensor-equipped RSEs and non-sensor-equipped RSEs. However, since the impact of a false message is low, the recommendation of this analysis is that a separate role identifier is not necessary.			

4.5.11 UC-D3: VRUs crossing at a zebra protected by a traffic light

Table 13: Risk Analysis: UC-D3: VRUs crossing at a zebra protected by a traffic light

Use case: VRUs crossing at a zebra protected by a traffic light in the presence of a priority vehicle			
Actors: Priority vehicle, RSE, VRU			
Information flow	Entity activities	Description	Impact

DRAFT

ID3-1 Request priority	ED3-1.1 Priority vehicle → RSE	message implicitly or explicitly requesting signal prioritization	C: None – broadcast model I: Medium – False signal prioritization messages can cause significant traffic disruption A: Low – Any level of availability allows this use case to be effective
ID3-2 Detect VRUs	ED3-2.1 Sensor-equipped RSE detecting VRU	Sensor activity to detect VRU	C: None – VRU is detectable by any sensor-equipped vehicle I: Low – The worst outcome is false warnings but these will be delivered to a series of different drivers and so will not significantly affect the confidence of any driver in the system A: Low – Any level of availability allows this use case to be effective
ID3-3 Send Signal Prioritization Result	ED3-3.1 RSE → Priority vehicle	Signal priority request result: message indicating presence of VRUs, or indicating that priority will (not) be granted	C: None – VRU is detectable by any sensor-equipped vehicle I: Low –Priority vehicle should be moving with caution anyway since it is approaching a signalized intersection and so a false safety indication should not result in excessive speed. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: Neither the RSE nor the priority vehicle require pseudonymity. Notes: 1. The traffic signal RSE in this case is assumed to be equipped with more sensors than a traffic signal RSE that simply sends SPaTs. This therefore creates a potential requirement for a role identifier (an SSP) that distinguishes between sensor-equipped RSEs and non-sensor-equipped RSEs. However, since the impact of a false message is low, the recommendation of this analysis is that a separate role identifier is not necessary. 2. The design of the traffic signal prioritization mechanism in ED3-1.1 is not in scope for the present document and the security analysis is included only for completeness			

4.5.12 UC-D4: Scooter / bicyclist safety with turning vehicle

Table 14: Risk analysis: UC-D4: Scooter / bicyclist safety with turning vehicle

Use case: Scoots / bicyclist safety with turning vehicle			
Actors: VRU, RSE, vehicle			
Information flow	Entity activities	Description	Impact

DRAFT

ID4-1 Detect	ED4-1.1 Sensor-equipped RSE detecting VRU	Sensor activity to detect VRU	C: None – VRU is detectable by any sensor-equipped vehicle I: Low – False positives will affect a number of different drivers and will not have a significant impact on confidence in the system. A: Low – Any level of availability allows this use case to be effective
ID4-2 Warn	ED4-2.1 Sensor-equipped RSE → Vehicle	Perception message	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity requirements: The vehicle requires pseudonymity, the RSE does not. Notes: The traffic signal RSE in this case is assumed to be equipped with more sensors than a traffic signal RSE that simply sends SPaTs. This therefore creates a potential requirement for a role identifier (an SSP) that distinguishes between sensor-equipped RSEs and non-sensor-equipped RSEs. However, since the impact of a false message is low, the recommendation of this analysis is that a separate role identifier is not necessary.			

4.5.13 UC-E1: Network assisted vulnerable pedestrian protection

Table 15: Risk analysis: UC-E1: Network assisted vulnerable pedestrian protection

Use case: Network assisted vulnerable pedestrian protection			
Actors: VRU, vehicle, third party in cloud			
Information flow	Entity activities	Description	Impact
IE1-1 Detect	EE1-1.1 VRU → Third party in cloud	Position report	C: None – VRU is detectable by any sensor-equipped vehicle I: Medium – If location can be spoofed then attacks will be scalable. A: Low – Any level of availability allows this use case to be effective
IE1-2 Warn	EE1-2.1 Third party in cloud → Vehicle	Perception message	C: None – broadcast model I: Medium – If this communications session can be hacked then the system is vulnerable to widespread false alerts and disruption.

DRAFT

			A: Low – Any level of availability allows this use case to be effective
Pseudonymity: The VRU may be identified to the third party in the cloud if the VRU has given consent, if the third party follows good privacy and data management practices, and if the third party does not reveal the identity of the VRU to the third party. The third party in the cloud does not need pseudonymity. The Vehicle does not send messages in this use case. Notes: 1. The security mechanisms on the two information flows in this scenario need not be based on the current (role-based) ETSI ITS security specifications but may use existing (identity-based) web authentication technologies			

4.5.14 UC-E2: Detection of an animal or pedestrian on a highway

Table 16: Risk analysis: UC-E2: Detection of an animal or pedestrian on a highway

Use case: Network assisted vulnerable pedestrian protection			
Actors: Roadside Camera, vehicle, third party in cloud, VRU			
Information flow	Entity activities	Description	Impact
IE2-1 Detect	EE2-1.1 Roadside camera → Control center	VRU report	C: None – VRU is detectable by any sensor-equipped vehicle I: Medium – If location can be spoofed then attacks will be scalable. A: Low – Any level of availability allows this use case to be effective
IE2-2 Warn	EE2-2.1 Third party in cloud → Vehicle	Broadcast of notification about presence of hazardous VRU	C: None – broadcast model I: Medium – If this communications session can be hacked then the system is vulnerable to widespread false alerts and disruption. A: Low – Any level of availability allows this use case to be effective
	EE2-2.2 Third party in cloud → Equipped VRU	Broadcast of warning message	C: None – broadcast model I: Low – A false warning to a VRU will not cause significant widespread disruption to the system. A: Low – Any level of availability allows this use case to be effective
Pseudonymity: None of the sending parties in this use case need pseudonymity. Notes:			

DRAFT

1. The security mechanisms on the two information flows in this scenario need not be based on the current (role-based) ETSI ITS security specifications but may use existing (identity-based) web authentication technologies

4.5.15 UC-F1: Signalled many VRUs in a protected area

Table 17: Risk analysis: UC-F1: Signalled many VRUs in a protected area

Use case: Signalled many VRUs in a protected area			
Actors: Equipped VRUs, RSE, Approaching vehicle			
Information flow	Entity activities	Description	Impact
IF1-1 Detect	EF1-1.1 Approaching vehicle → RSE	Broadcast of dynamic and other information about vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EF1-1.2 Equipped VRU → RSE	Broadcast of dynamic and other information about VRUs	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
IF1-2 Warn	EF1-2.1 RSE → Approaching vehicle	Broadcast of warning of protected area	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
	EF1-2.2 RSE → VRUs	Warning Siren or broadcast of notification about presence of vehicle	C: None – broadcast model I: Low – Impact of false messages is false alarm for individuals. A: Low – Any level of availability allows this use case to be effective
Pseudonymity: The VRUs and the vehicles need pseudonymity, the RSE does not. Notes: 1. Even though a false alarm would cause disruption to a potentially large number of VRUs, this is still not sufficiently large disruption to count as Medium integrity sensitivity.			

DRAFT

4.5.16 UC-F2: Intelligent traffic lights for all

Table 18: Risk analysis: UC-F2: Intelligent traffic lights for all

Use case: Intelligent traffic lights for all			
Actors: Privileged VRU, RSE, Vehicle			
Information flow	Entity activities	Description	Impact
IF2-1 Detect	EF2-1.1 Equipped VRU → RSE	Awareness message of (a) presence of VRU (b) fact that VRU is privileged (c) fact that VRU is about to cross or is crossing the road	C: None – broadcast model I: Low – If there are bad actors who falsely claim to be privileged VRUs, the system can still manage the impact by asking them to wait before crossing the road, etc. A: Low – Any level of availability allows this use case to be effective
IF2-2 Extended signal notification	EF2-2.1 RSE → Approaching vehicle	Indication that red will be extended	C: None – broadcast model I: Low – Message should be in synch with signals and is for information only. A: Low – Any level of availability allows this use case to be effective
	EF2-2.2 RSE → VRUs	Indication that red signal will be extended	C: None – broadcast model I: Low – Message is unlikely to affect VRU behaviour in a way that has wider impact on the traffic system. A: Low – Any level of availability allows this use case to be effective
Pseudonymity: The VRU and the vehicle need pseudonymity; the RSE does not. Notes: 1. The impact of an integrity breach on EF2-1.1 is low, because excessive requests can be handled by adjusting the vehicle movement phase length or by choosing not to prolong the crossing phase immediately after a request instead interspersing prolonged phases between normal-length phases. As such, although these "social weak" VRUs have elevated privileges compared to ordinary VRUs, it is not clear that there is a security requirement for the "social weak" VRU role to be separated from the ordinary VRU role. This document nevertheless recommends that a "social weak" VRU role is identified to help manage the risk of potential fake social weak VRUs in this and other contexts.			

DRAFT

5 VRU related requirements

5.1 Introduction

The objective of clause 5 is to specify the requirements on the VRU-related components in the C-ITS. These requirements are derived from the use cases described in clause 6 and their analysis in clause 7 of ETSI TR 103 300-1 [i.1].

Each use case presented in [i.1] has been analysed to produce these requirements. Furthermore, additional requirements were identified from clause 7 "Summary and conclusion" of [i.1] which already discussed challenges and topics that need to be taken into account in the present document, such as VRU profiling, performance figures, security or deployment roadmap.

The requirements are classified into two categories: functional requirements, which will have an impact on the VRU system architecture and operational requirements to be validated when testing and deploying the VRU system. They are further considered at system, communication and security level. Some of these requirements may feed into further work, such as the communication architecture to be used by the VRU system (see [i.1] clause 4.3 for the definition of the VRU system).

The requirements have been numbered using the following naming convention: XYYYnn.i, where

- X= F for functional / O for operational
- YYY = SYS for system, COM for communication, SEC for security
- nn is a sequential number identifying the requirement
- i is a sequential number identifying sub-requirements when different options exist on a specific requirement. (optional).

NOTE: requirements at station level are included in the system level as ITS-S are part of the C-ITS.

DRAFT

5.2 Functional requirements

5.2.1 System requirements

System functional requirements identify the ITS functions necessary to support the VRU services.

Table 19: Functional system requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
FSYS01	An element of the VRU system shall use an ITS-S (either personal, vehicle, road side or central) for transmission and shall either be integrated with that ITS-S or have a secure connection to that ITS-S.	The VRU system is made of a composition of the 4 interacting ITS elements which are the VRU device, the non-VRU vehicle, the Roadside equipment and the central system. Each constituting element integrates one ITS Station.	Diversity of proposed use cases [i.1] clause 6.
FSYS02	The VRU system shall include functions aiming at detecting a risk of collision between VRUs and other road users and avoiding such collisions.	These functions and associated data can be distributed in an optimal way in different elements of the VRU system.	Diversity of proposed use cases [i.1] clause 6.
FSYS03	The VRU system architecture shall support several possible interaction scenarios between the four elements of ITS architecture it is made of.	These interaction scenarios depend on the distribution of functions and data in the four possible types of ITS stations (personal device, vehicle, RSE, central) of the VRU system.	Diversity of use cases, functional and operational requirements [i.1] clauses 6 and 7.
FSYS04	The VRU system shall be able to fuse incoming C-ITS messages with other data, if available, to form a dynamically updated map of the motion of relevant road users.	The collision risk analysis function is one key functional element which relies on the ITS elements being able to fully and constantly perceive the movements of mobiles which are possibly colliding.	Diversity of proposed use cases [i.1] clause 6. Clauses 7.2, 7.8, 7.9, 7.12
FSYS05	Calculations of risk to the VRU shall be based on all relevant physical properties, including but not necessarily limited to the dynamic state and the mass of the moving objects.	The collision risk analysis function considers the full dynamic state of the road users and predict their respective evolutions with a good level of confidence for the collision risk analysis, the time-to-collision (TTC) evaluation and then the most	Diversity of proposed use cases [i.1] clause 6. Clauses 7.2, 7.8, 7.9, 7.12

DRAFT

		appropriate collision avoidance strategy (acting on the trajectories or on the velocities or both).	
FSYS06	The VRU collision risk analysis function, and dynamic state prediction shall be able to reliably predict the relevant road users manoeuvres with an acceptable level of confidence for the purpose of triggering the appropriate collision avoidance action, assuming that the input data is of sufficient quality.	The collision risk analysis function analyses the level of collision risk based on a reliable prediction of the respective dynamic state evolution. Consequently, the reliability level aspect needs to be characterized in terms of confidence level.	[i.1] clauses 7.2, 7.8, 7.9, 7.12.
FSYS07	The collision avoidance actions shall be triggered at the level of the VRU or the vehicle or both, depending on the VRU capabilities to act (VRU profile and type), the vehicle type and capabilities and the TTC value.	VRU do not always have the capability to act to avoid a collision (ex: animal, children, aging person, disabled…etc.), especially if the TTC is short (a few seconds). Vehicles may have in the future the capability to trigger automatically an emergency brake or include pre-crash systems to mitigate a collision with a VRU.	[i.1] clauses 7.2, 7.9, 7.12.
FSYS08	Depending on the vehicle level of automation, the collision avoidance action or impact mitigation action shall be triggered as a warning / alert to the driver or as a direct action on the vehicle itself.	The following collision avoidance actions can be envisioned at this point (may be combined): • extend or change the phase of a traffic light • act on the trajectory and / or velocity of the vehicle (slow down, change lane) if the vehicle has a sufficient level of automation, • alert the ITS device user through the HMI, • disseminate a C-ITS message to other road users, including the VRU if relevant The following impact mitigation actions can be envisioned at this point (may be combined): • trigger a protective mean at the vehicle level (e.g. extended external airbag), • trigger a portable VRU protection airbag	[i.1] clause 7.8. B1
FSYS09	At the VRU level, the reliable prediction of the VRU movement shall take into account the VRU profile (including for example the type of VRU, see [i.1] and clause 6.1) with	The VRU dynamic state prediction algorithm may be improved over time by local learning about the usual behaviour of specific VRUs or by other means.	[i.1] clause 7.2, 7.4, 7.5

DRAFT

	the purpose to provide a reasonable level of confidence in this prediction		
FSYS10	The VRU basic service of a VRU ITS-S shall be deactivated as long as the VRU device owner is inside a non-VRU vehicle (e.g. a vehicle with a strong exterior) or protected area and cannot be considered any more as vulnerable. The VRU basic service shall be activated after the VRU device owner leaves the protected vehicle	A Road User may not be vulnerable any more when entering a protected area or using a non VRU transportation means. Consequently, the VRU state transition is managed with the objective to adapt the VRU service, even deactivate it when not necessary anymore, as soon as the VRU state disappears. NOTE: TS 103 300-3 [i.11] defines performance values for the activation / deactivation of the VRU ACTIVE state.	[i.1] clause 7.2,
FSYS11	The configuration of all elements of the VRU system, including changes and updates that may be necessary during their life cycles, shall be managed.	Configuration management is necessary for the update of the ITS station during its life cycle. It is necessary for preventive and corrective maintenance, but also for technological, protocol evolutions and more generally functional evolutions.	[i.1] clause 7.7
FSYS12	The V-ITS_S of a VRU vehicle shall not send the CAM as long as it is considered as a VRU and transmits the VAM.	An ITS station should avoid transmitting simultaneously CAM and VAMs to prevent channel congestion. This may apply to motorcycles which are considered as VRUs when moving at low speed and as regular vehicles when moving at speeds higher than the limit of their VRU profile. This requirement is relevant only for VRU devices using VRU Profile 3, not for devices using any of the other profiles.	
FSYS13	When participating to the VRU system, a R-ITS-S associated to a traffic light shall be able to adapt the phase duration according to the VRU profile or send warnings to provide additional safety for VRUs.	A Road Side Equipment that can send warnings is still useful, even if it can't affect signal phase and timing.	
FSYS14	VRU devices involved in C-ITS communications shall support at least one of the following configurations: VRU-Tx, VRU-Rx, VRU-St, as defined in [i.1] and in clause 4.1.	A VRU device configured as a VRU-Tx or a VRU-St complies with the Decentralized Congestion Control (DCC) rules as defined in ETSI TS 103 175 [i.18].	A1
FSYS15	VRU devices supporting VRU-Rx / VRU-St configuration shall include an appropriate HMI to notify their users in case of safety issue.	This HMI can be audio, text, graphics or any means relevant with the VRU profile.	A1

DRAFT

FSYS17	When relevant, a VRU device shall indicate special VRU conditions such as very vulnerable person, disable, pram, wheelchair, etc.	This indication is optional, but will help for example traffic lights adapt their phase accordingly.	E1

5.2.2 Communication requirements

Table 20: Functional communication requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
FCOM01	A VRU system shall operate effectively when up to [5000] number of users are within the same communications zone, i.e. within a circle of radius up to 300 m, as defined in the Road Hazard Signalling (RHS) standard [7]. This may be achieved by the clustering of active users.	The maximum number of users depends on the density of VRUs in a geographical area. Moreover, this also depends on standardized communication protocols such as DCC and on the clustering efficiency. Example: Considering a crowd of VRUs within a communication distance of 100 meters, in a quadratic area of 10000 m2, which can be divided in 1000 bounding boxes of 10 m2 each. This results in 1000 VRU clusters, i.e. 1000 users of the VRU system.	
FCOM02	A VRU system shall support an appropriate congestion control mechanism	DCC shall consider the maximum number of VRUs which may be communicating simultaneously. It shall also consider the available network bandwidth.	Clause 7.5
FCOM03	VRU devices shall operate to mitigate a channel congestion problem if there are many ITS-S in the VRU environment. -	Possible solutions for prevention and reduction of the number of transmitted messages are: • Consulting appropriate maps to verify if the VRU is on a drivable road or in protected areas such as buildings before sending VAMs. • Designating a geographical area as a pedestrian zone (using the MAPEM)	A1, A2, B1, B2, B5, F1

DRAFT

		• Considering itself as part of a VRU cluster when relevant and transmitting VAM • Considering the VRUs as part of a VRU cluster when transmitting CPM by V-ITS-S or R-ITS-S • Considering CPMs from other sources to detect if the VRU has already been reported by others and hence inhibit the sending of VAM by the VRU itself.	
FCOM04	A VRU system shall support the flexible and dynamic triggering of messages with generation intervals from 100ms at the most frequent.	The VAMs frequency is related to the calculated TTC, distances separating the mobiles and respective dynamic states of mobile objects being under a risk of collision.	
FCOM05	A VRU device supporting the VRU-Tx or VRU-St configuration shall be able to broadcast VAMs, with sufficient frequency to enable timely detection of a collision risk.		A1, A2, B1, B2, B3, B5, F1, F2
FCOM06	When the VRU ITS-S is able to transmit (VRU-Tx or VRU-St configuration), the VRU ITS-S shall adapt the periodicity of transmitted VAMs to its profile, velocity, context and potentially to the evaluation of increased risk.		A1, A2, B1, B2, B3, B5, F1, F2
FCOM07	The VAM shall include in its data elements the VRU position, its dynamic state, its dimensions, the current VRU profile (as defined in clause 6.1) and whether it is part of a cluster of VRUs. **Optional:** It may include the mass of the VRU for a combined VRU (e.g. a motorcycle) and the trajectory of the VRU including the history and estimated future trajectory	These data elements are necessary to the collision risk analysis.	B3
FCOM08	When relevant, V-ITS-S and R-ITS-S shall transmit VRU related warning and awareness messages selecting the most appropriate message.	DENM and CPM have been considered in the present document. Note: IVI and MCM, which are more general-purpose messages, have been introduced in TR 103 300-1 [i.1] for	C1

DRAFT

		similar conditions. SPaT is not considered as a VRU-related warning.	
FCOM09	A VRU-related warning or awareness message shall contain at least the following data elements: VRU position, dimensions, velocity and direction. If available, it shall also contain the VRU orientation and its estimated VRU profile.		D2
FCOM10	The VRU ITS-S receiving warning and awareness messages shall check their relevance and if suitable, notify the user appropriately.	The user of a VRU may receive event notifications for neighbouring VRUs.	B2

5.2.3 Security requirements

Table 21: Functional security requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
FSEC01	All RF transmissions to support VRU use cases shall come from an ITS-S and all ITS-S shall ensure that inputs used to form messages are from trustworthy sources.		
FSEC02	Messages within the VRU system shall use communications security mechanisms appropriate to address the risks that would otherwise be associated with unsecured messages.		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.
FSEC03.1	The security mechanisms used shall be extensible to allow for the deployment of additional use cases.		Diversity of use cases [i.1] clause 6; see also security discussion in 7.6.
FSEC03.2	The security mechanisms used shall support the case where vehicular reaction to the VRU is automated, as well as the case where vehicular reaction is caused by alerting the vehicle operator.		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.
FSEC04	The security mechanisms used shall preserve the privacy of all system users to the greatest extent consistent with the safety goals of the system.		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.

DRAFT

FSEC05	While preserving user privacy (SecFR04), the security mechanisms used shall support the ability to detect devices that are sending malicious messages.		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.
FSEC06	The security mechanisms used shall support the ability to withdraw the trusted status of devices that are considered to be causing a risk to the correct operation of the system.		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.
FSEC07	Special VRU conditions such social weakness, very vulnerable person, disable, pram, wheelchair, etc. shall be security protected against false usage.		

5.3 Operational requirements

5.3.1 System requirements

System operational requirements which characterize the system performances and other operational aspects related to the identified functions.

Table 22: Operational system requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
OSYS01	Positioning capabilities of the communication system shall be better than [50cm].	The VRUs' relative positioning accuracy will be used to analyse a risk of collision with a vehicle or other VRUs. As VRUs are smaller than vehicles and the trajectory is less predictable, the relative accuracy of VRUs' positions need to be better than for non-VRU vehicles.	[i.1] clause 7.5.
OSYS02	Each VRU and VRU cluster shall have a reference position.	A reference point is necessary to estimate and track the movement of the VRU, combined VRU or VRU cluster.	
OSYS03	The confidence of a VRU dynamic state prediction shall be computed for the purpose of risk analysis.	The prediction of the dynamic state of the VRU is complicated especially for some specific VRU profiles (ex: animal, child, disabled person, etc.). It is thus necessary to associate a confidence level to this prediction and include it as an element of the VAM.	

DRAFT

OSYS04	The collision risk analysis requires the information about vertical position. A collision avoidance action should be triggered only in the case where the VRU and vehicle are on the same vertical level (altitude) of the road network.	False positive alert could result of not considering this aspect. An example is when VRUs are on a footbridge crossing a road.	B2
OSYS05	The data exchanged shall be recent enough to be useful to the receiver for collision avoidance purposes, leading to a minimum end to end latency time (ex: less than 300 ms as in the RHS standard ETSI TS 101 639-1 [7] and to a sufficient data sampling rate (e.g., 10 Hz).	At receiving level (vehicle and VRU) the age of data elements is a key parameter impacting the accuracy of the receiver perception. In particular, at receiving level, a VRU position and velocity are known via their latest received values. But as the VRU device in principle keeps moving, the actual values are changing. Consequently, the data sampling period at the origin and the end to end latency time are key parameters to be minimized.	[i.1] clause 7.5.
OSYS06	A receiver shall take the reported age of data into account when determining the appropriate reaction to a received message.	The correction can be performed via an interpolation mechanism based on a hypothesis of the VRU movement made at this level (e.g., on the mobile trajectory and velocity).	
OSYS07	Battery and other resources (CPU, memory, communication) at the VRU portable device level shall be dimensioned to provide the targeted VRU protection service under knowable conditions.	The resources dimensioning shall respond to ITS scalability requirements with the objective to continue offering the VRU basic service when the ITS deployment is progressing.	[i.1] clause 7.5
OSYS08	If a key resource required for the support of the VRU basic service is defective, whatever the cause, the VRU shall be informed of this failure.	A failure may occur following a lack of energy, a defective component or a cyberattack.	
OSYS09	The VRU system as defined in [i.1] shall be scalable and capable of evolving as necessary to support its deployment without impacting the VRUs' offered services. An already deployed VRU device may be updated or replaced to follow this evolution.	The system needs to be capable to support preventive, curative and evolutive maintenance operations without disturbing the VRU services during all its life cycle. This requires a configuration management capability at the level of all ITS elements.	[i.1] clause 7.7.
OSYS10	The VRU ITS-S shall support communications that are interoperable and as such respect one or several common set(s) of standards. The VRU system interoperability shall be verified before putting VRU system elements on the market.	Interoperability is a key feature of cooperative ITS.	[i.1] clause 6 use cases showing VRU system elements interactions.

DRAFT

OSYS11	The VRU system minimum performances shall be provided and testable before delivery of VRU system elements on the market.		Minimum performance requirements to be derived from [i.1] clause 7.5
OSYS12	A device shall be capable of processing an active collision risk event while simultaneously detecting new collision risk events.	This monitoring state may require under some condition the broadcasting of VAMs enabling the collision risk analysis following the reception of the respective current perceptions of involved VRU devices and the derived movement predictions.	A1, A2, B1, B2, B3, B5
OSYS13	The VRU movement reliable prediction shall be used to trigger the broadcasting of relevant VAMs when a risk of collision involving a VRU is detected at relatively short TTC.	Short TTC (calculated according to several parameters including road slippery conditions, weather conditions, traffic conditions…etc.) require highly dynamic exchanges of information between cooperative elements. So, such exchange shall start as soon as possible based on the reliable detection of a risk of collision obtained via local and remote perceptions as well as their resulting evolution predictions in terms of respective dynamic states (considering the mobiles trajectories and velocities).	[i.1] clauses 4.4, 7.2, 7.5, 7.8, 7.9.
OSYS14	An ITS station detecting a potential risk of collision with a VRU shall transmit a warning notification message to other road users only if the assessment confidence is higher than 95%.	95% is the value for confidence assessment used in other C-ITS standards for messages such as CAM, DENM or for applications such as the RHS [7].	A1
OSYS15	A VRU device shall be capable of processing at least 1000 incoming messages per second without degradation of its ability to detect potential collision risks.	Same as in the RHS minimum performance requirements [7]	

5.3.2 Communication requirements

DRAFT

Table 23: Operational communication requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
OCOM01	The transmission range of a VRU system shall depend on the specific application. Specific values are defined in sub-requirements OCOM01.1 to OCOM01.5	Here, "transmission range" means that an ITS-S that is intended to act in the indicated role is able to support a transmit power that is expected to result in successful transmission over the indicated distance. The range is defined as 360° round in direct line of sight with at least 95% probability to receive the packet in 1s.	Clause 7.5
OCOM01.1	A VRU ITS-S that supports communication with an infrastructure ITS-S for VRU protection purposes shall be capable of a transmission range of at least 25m	This supports the case where an infrastructure ITS-S detects VRU ITS-S by their messages and retransmits a VAM.	
OCOM01.2	A VRU ITS-S that supports communication with a standard V-ITS-S for pedestrian collision avoidance purposes shall be capable of a transmission range of at least 70m.	This allows support of VAMs with a TTC of 5s between a stationary pedestrian and a vehicle moving at 45 km/h	
OCOM01.3	A VRU ITS-S that supports communication with a standard vehicular ITS-S for cyclist collision avoidance purposes shall be capable of a transmission range of at least 150m.	This allows support of VAMs with a TTC of 5s between a cyclist moving at 30 km/h and a vehicle moving at 90 km/h	
OCOM01.4	A VRU ITS-S that supports communication with a standard vehicular ITS-S for motorcycle collision avoidance purposes shall be capable of a transmission range of at least 300m.	This is identical to the range used for V2V collision avoidance for standard vehicles	
OCOM01.5	A VRU ITS-S that supports collision avoidance use cases may be capable of adjusting the transmission range based on local conditions	To save battery a VRU ITS-S may adjust the transmit power. For example, a reasonable transmit power algorithm would base the anticipated transmit range on a TTC of 5s with the highest-speed vehicle detected in the previous 5s (possibly taking maps into account so that, for example, vehicles on a freeway on the other side of a wall don't cause the device to use more transmit power than would be useful).	
OCOM02	Communication latency shall be less than 5 milliseconds under open sky conditions with unobstructed transmission from sender to receiver	This is the latency between the start of the request to transmit a packet of data at access layer level until reception at access layer level in the peer. The requirement specifies "open sky conditions" and "unobstructed transmission" to make clear the test conditions related to this requirement; it will of course be the case that any implementation that meets the requirements	Clause 7.5

DRAFT

		under these conditions will also meet the requirements under a wide range of less favourable conditions.	
OCOM04	The VAM shall support dynamic length.	The length of the message depends on the content of its data elements and the actually deployed data elements This is according to standard messages requirements and takes consideration of the security needs. This is detailed in TS 103 300-3 [i.11].	
OCOM05	The VAM shall support dynamic timing.	The timing of VAM transmission depends on the context of the VRU. This is according to standard messages requirements and takes consideration of the security needs. This is detailed in TS 103 300-3 [i.11].	

5.3.3 Security requirements

Table 24: Operational security requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
OSEC01	The security processes shall support generating messages at a rate of 10 Hz, receiving messages at a rate of 2 KHz, latency of 300 ms end-to-end and an average sent packet size over 1 second of 300 bytes. .		Applies to all use cases [i.1] clause 6; see also security discussion in 7.6.

5.4 Additional recommendations

DRAFT

Table 25: Additional recommendations

Rec-Id	Recommendation text	Explanation	UC reference from [i.1]
REC01	A VRU ITS-S should be able to perform collision risk assessment if sufficient battery and processing power are available in the VRU device.	The VRU may not have sufficient processing power or battery to make this assessment. Accordingly, this is not a requirement for the VRU device.	A2
REC02	All elements of the VRU system should comply with the relevant spectrum regulation and related standards	Interoperability between interacting VRU system elements requires standardisation of communication profiles common to all participating elements. The used spectrum should be sufficient to support all standardized C-ITS services. This is necessary to enable the interoperability between VRU system elements and avoid EMI.	

DRAFT -

6 Functional architecture of the VRU system

6.1 VRU profile specification

In this clause four basic VRU profiles are defined. These profiles are the basis for the further definition of the VRU functional architecture. The profiles are derived from the use cases and from the analysis in clause 7.2 in TR 103 300-1.

A VRU can only be a living being. This living being is considered as a VRU only when it is in the context of a safety related traffic environment.

So, a living being in a house is not a VRU but as soon as it comes closer to the street (e.g. 2m or 3m), it is part of the safety related context and is in a role of a VRU.

This consideration is important since it will limit the amount of communications. A C-ITS communications device need only start to act as a VRU ITS-S when the living being associated with it starts acting in the role of a VRU.

Profile parameters:

- Maximum and average (typical) Speed values (may be with its standard deviation)
- Minimum and average (typical) Transmission range: The transmission range is calculated based on the assumption that an awareness time of 5 seconds is needed to warn / act on the traffic participants
- Environment e.g., type of area (urban, sub-urban, rural, highway)
- Average Weight and standard deviation
- **directivity/trajectory ambiguity:** give the level of confidence we may have in the predictability of the behaviour of the VRU in its movements
- **Cluster size:** Number of VRUs in the cluster. A VRU may be leading a cluster and then indicate its size (see clause 6.2.1). In such case, the leading VRU can be positioned as serving as the reference position of the cluster.

VRU Profile 1 - Pedestrian.

Typical VRUs in this profile: pedestrians, i.e. road users not using a mechanical device for their trip. It includes for example pedestrians on a pavement, but also children, prams, disabled persons, blind persons guided by a dog, elderly persons, riders off their bikes.

NOTE: The values given in the next VRU profile tables are indicative.

Table 26: Pedestrian VRU profile

Parameter:	Values	Typical value in operation	Comment
Speed:	< 12km/h < 25km/h	5km/h	This profile also includes running pedestrians and animals
Transmission range	Minimum supported maximum value: 70m	50m Urban and Suburban 250m Rural (if capable)	Main usage in Urban and Sub-urban environment lead to the typical range of 50m

DRAFT

Environment	Urban and Suburban Rural Highway	Urban/Suburban	Mainly in urban and sub-urban environment Highway after accident/ Road works
Weight class	Low: <10kg Medium: < 30 kg High: > 30kg	High (80kg)	The weight class is intended to distinguish between small children, larger children and adults. Similar different animals can be distinguished
Trajectory ambiguity	High	high	
Cluster size	Up to 50	> 1	50 is an arbitrary number brought in by common sense and performance requirements in clause 5. Above 50, the management of the cluster would be challenging. This may be changed under further study

VRU Profile 2 - Bicyclist.

Typical VRUs in this profile: bicyclist and similar e.g., light vehicles riders, possibly with an electric engine. It includes bicyclists, but also wheelchair users, horses carrying a rider, skaters, e-scooters, Segway's, etc.

Note: It has to be noted that a light vehicle itself doesn't represent a VRU but only the combination with a person will create the VRU.

Table 27: Bicyclist VRU profile

Parameter:	Values	Typical value in operation	Comment
Speed:	< 25km/h (all environments)	20km/h	Higher typical speeds do not have an impact on the profile.
Transmission range	Minimum supported maximum value: 150m	70m Urban and Suburban 250m Rural	Main usage in Urban and Suburban environment lead to the typical range of 50m Higher typical speed lead to higher range
Environment	Urban and Suburban Rural	Urban/Suburban	Mainly in urban and sub urban environment
Weight class	Low: <15kg Medium: < 40 kg High: > 40kg	High (90kg)	The weight class is intended to distinguish between small children, lager children and adults.

DRAFT

			Weight includes the driver (bicycle alone is not a VRU).
Trajectory ambiguity	Medium to high	medium	
Cluster size	20	> 1	20 is an arbitrary number brought in by common sense and performance requirements in clause 5. Above 20, the management of the cluster would be challenging. This may be changed under further study

VRU Profile 3 - Motorcyclist.

Typical VRUs in this profile: motorbikes, which are equipped with engines that allow them to move on the road. It includes Powered Two Wheelers (PTW) such as mopeds (motorized scooters) and motorcycles when they drive at low speed.

Note: It has to be noted that a light vehicle itself doesn't represent a VRU but only the combination with a person will create the VRU.

Table 28: Motorcyclist VRU profile

Parameter:	Values	Typical value in operation	Comment
Speed:	< 45km/h	35km/h	45km/h is the maximum speed of a scooter
Transmission range	Minimum supported maximum value: 300m	70m Urban and Suburban 250m Rural	Above a certain speed a motorcycle transitions to sending CAMs and is subject to the performance requirements related to CAMs.
Environment	Urban and Suburban Rural Highway	Urban/Suburban	Mainly in urban and sub urban environment
Weight class	Low: < 25kg Medium: < 140kg High < 300kg	medium (140kg)	The weight class is intended to distinguish between different types of scooters. Weight includes the driver (motorbike alone is not a VRU).
Trajectory ambiguity	Low to medium	low	

DRAFT

Cluster size	20	> 1	20 is an arbitrary number brought in by common sense and performance requirements in clause 5. Above 20, the management of the cluster would be challenging. This may be changed under further study

VRU Profile 4 - Animals presenting a safety risk to other road users

Typical VRUs in this profile: dogs, wild animals, horses, cows, sheep, etc. Some of these VRUs might have their own ITS-S (e.g. dog in a city or a horse) but most of the VRUs in this profile will only be indirectly detected. Especially wild animals in rural areas and highway situations.

Clusters of animals VRU might be herds of animals, like a herd of sheep or cows or wild boars. This profile has a lower priority when decisions have to be taken to protect a VRU.

Table 29: Animal VRU profile

Parameter:	Values	Typical value	Comment
Speed:	< 40km/h (all environments)	5km/h	
Transmission range	Minimum supported maximum value: 70m.	70m Urban and Suburban 250m Rural	
Environment	Urban and Suburban Rural	Urban/Suburban/Rural	In urban and sub urban environment, applies mainly to individual animals, e.g. dogs. In Rural environments, applies to individual animals (e.g. horses) but also to clusters of animals (e.g. cows, sheep).
Weight class	Low: <15kg Medium: < 40 kg High: > 40kg	Medium (25kg)	The weight class is intended to distinguish between small animals like a cat, medium animals like a dog or a big animal like a wild boar or a horse.
Trajectory ambiguity	high	High	
Cluster size	Up to 100	> 1	
Priority	Below profiles 1 to 3		

DRAFT

6.2 VRU cluster definition

6.2.1 VRU cluster concept

NOTE: The present clause defines the notion of VRU cluster. Its detailed specification will be part of the VRU basic service standard (TS 103 300-3 [i.11]).

The number of VRUs operating in a given area can get very high (see Use Case pedestrian crossing, up to 500) or the VRU can be combined with a VRU vehicle (e.g. rider on a bicycle). In order to reduce the amount of communication and thus the resource usage VRUs should be grouped together leading to VRU clusters. These clusters can be homogeneous VRU clusters (group of pedestrians) or heterogeneous VRU clusters (groups of pedestrians and bicycles with person). These clusters are considered as a single object/entity and only the cluster head will continuously transmit the VAM. The parameters of the VRU cluster will be communicated using the VAM. The VAM message contains an optional field that indicates whether the VRU is leading a cluster, which is not present for an individual VRU (other VRUs in the cluster should not transmit VAM). The leading VRU also indicates in the VAM whether it is a homogeneous cluster or heterogeneous, the latter one being of any combination of VRUs.

Indicating heterogeneous clusters is important because when it provides useful information about trajectory and behaviours prediction when the cluster is disbanded.

The use of a bicycle or motorcycle will significantly change the behaviour and parameters set of the VRU using this non-VRU object (or VRU vehicle) "bicycle"/"motorcycle". A combination of a VRU and a non-VRU object is called combined VRU.

The goal of a VRU cluster is to reduce the communication requirements (e.g. spectrum requirements), in the case of the combined VRU the change of the VRU parameter is the more important goal.

A VRU cluster is a set of 2 or more VRUs (e.g. pedestrians) such that the VRUs move in a coherent manner, i.e. with coherent velocity or direction and within a bounding box.

Coherent "cluster" velocity: velocity range of VRUs in a cluster such that the differences in speed and heading between any of the VRUs are below a predefined threshold.

VRU Bounding box: a rectangular area containing all the VRUs in the cluster and such that all the VRUs in the bounding box make contact with the surface at approximately the same elevation.

6.2.2 VRU cluster requirements

Table 30: VRU cluster requirements

Req-Id	Requirement text	Explanation	UC reference from [i.1]
RCL01	A VRU device shall be able to determine whether it should be acting as a clustered or isolated VRU.		
RCL02	Only the VRU-St device type (see clause 4.1) shall lead a cluster. The VRU device type (St or TX) shall be indicated in the VAM.	As VRU-TX only device cannot receive and decode the VAMs of other VRU ITS-S, they are not able to participate in a cluster.	
RCL03	A VRU shall continuously detect whether or not it is part of a VRU cluster.		
RCL04	If the VRU is part of a VRU cluster, only the VRU leading the cluster shall transmit the VAM(s).		B1
RCL05	The VRU cluster leader shall transmit the VAM(s), indicating the cluster total dimension and velocity.		

DRAFT

RCL06	If the VRU is part of a VRU cluster and not leading the cluster, the VRU shall transmit a VAM indicating that it is joining the cluster and stop the transmission of VAM.		
RCL07	If the VRU is no longer part of the VRU cluster which it belonged to, it shall resume the transmission of the VAM(s).		B3

6.2.3 VRU cluster reference position

The head of a VRU cluster is selected as the VRU with the most upfront reference position considering the VRU direction.

A VRU cluster is considered as a single entity in the overall VRU communication. Only a single VAM is generated per cluster containing the relevant information/parameter of the cluster. These parameters are:

- Number of participants in the cluster, $N_{cluster}$
- Dimension of cluster expressed as reference point including length and width of the bounding box
- Speed of cluster
- Position of cluster (in this case position of the cluster head, the VRU cluster reference position.

VRU reference position: The reference position of a cluster of VRUs shall refer to ground position at the centre point of the face side of the first VRU bounding box. This is consistent with the definition of reference points in EN 302 890-2 (PoTi) [5].

Figure 3: Example reference position in the case of a cluster of pedestrians

6.2.4 VRU cluster approach

A VRU device is able to determine whether it should be acting as a clustered or isolated VRU. If a VRU is part of a cluster, only the VRU leading the cluster, i.e. cluster head VRU, transmits the VAM, indicating the cluster's total dimension and velocity. A cluster head VRU leads and manages a cluster, e.g. forming and disbanding a cluster, and cluster member VRUs join and leave a cluster.

- Forming a VRU cluster: When a VRU determines to form a cluster based on the received VAMs from other VRUs, it shall send a VAM indicating that it will lead the cluster with the VRU cluster's identifier.
- Disbanding a VRU cluster: When a VRU determines to disband a cluster, it shall send a VAM indicating that it will disband the cluster with the VRU cluster's identifier.
- Joining a VRU cluster: When a VRU receives VAMs from a cluster head VRU, the VRU analyses the received VAMs and decides whether it is allowed to join the cluster or not. In order to join the cluster, the VRU shall send a VAM indicating that it is joining the cluster with the VRU cluster's identifier, stop transmission afterwards, and monitor the VAMs from the cluster head VRU. This allows the cluster head VRU to know whether the cluster is homogeneous or heterogeneous, and the profile, size, speed and reference position of the cluster, and etc.
- Leaving a VRU cluster: When a VRU in a cluster receives VAMs from the cluster head VRU of the cluster, the VRU analyses the received VAMs and decides whether it shall leave the cluster or not (see below). In

order to leave a cluster, it shall send a VAM, i.e. first VAM after its silence, indicating that it is leaving the cluster and resume the transmission of the VAM. A VRU is always allowed to leave a cluster with any reason.

Only the VRU-St device type (see clause 4.1) is allowed to lead a cluster, and the VRU device type (St or TX) is indicated in the VAM.

A VRU device determines whether it can join or should leave a cluster by comparing its measured position and speed with the position and speed indicated in the VAM of the cluster head VRU. If the compared information fulfils certain conditions, e.g. less than 3-5 meters away and speed difference less than 5% of own speed, the VRU device can join the cluster. After joining the cluster, when the compared information does not fulfil the conditions any longer, the VRU device shall leave the cluster.

6.3 VRU system functional architecture

The present document provides details of the VRU-related entities residing in the facilities and application layers of an ITS Station, as defined in ETSI EN 302 665 [1] (ITS station reference architecture) and ETSI TS 102 894-1 (Facilities layer specification) [2].

Figure 4 provides the global architecture of the VRU system, based on four levels, one for each category of ITS-S (personal, vehicle, roadside, central). At each level, it mandatorily includes an ITS-S for that level. Functional entities in Figure 4 located beside the ITS-S are not directly related to C-ITS (e.g. the HMI). Devices not including an ITS-S are considered only based on their relationship with an ITS-S. This architecture is inspired from the architecture described by the VRUITS project.

Figure 5 in clause 6.4 zooms in the ITS-S element of Figure 4 and shows the main functional entities of the ITS-S architecture specified in [1] that directly impact the VRU system operation. It introduces a new functional entity described in more details in TS 103 300-3 [i.11], the VRU Basic Service. Other functions as defined in ETSI TS 102 894-1 [2] may be present and support the operation of these services, e.g. the communication support facilities or the HMI support. Figure 5 also illustrates a possible functional split at the application layer level of the ITS-S.

Figure 4: VRU system functional architecture

Figure 4 presents the global VRU system architecture, based on one level for each category of ITS-S. At each level, it includes an ITS station for that level in addition to other relevant components. More details are provided in clause 6.5.

The figure shows from right to left the entities which operate at the same level but are NOT included in the ITS-S:

- The relevant users at that level;
- The relevant HMI;
- Vehicle motion control (at vehicle level only) for automated vehicles. This entity is optional and does not appear in human driven vehicles. Both HMI and vehicle motion control entity may be triggered by the ITS-S applications;
- Local device sensor system and IoT Platform that collects and shares IoT data. The sensor system can be composed of one or more cameras, radars, lidars, etc. in a vehicle or road site equipment. In the central station, it consists of sensors that may be located on the side of the road, but directly report their data to the central station, without the involvement of a V-ITS-S or a R-ITS-S. In the VRU device, it consists mainly of the gyroscope and accelerometer;
- Local device sensor fusion and actuator application, which may contain Artificial Intelligence and aggregates the data flow issued by the sensor system;
- Local perception and trajectory prediction applications which consume the output of the fusion application and feed the ITS-S applications;
- The relevant ITS-S, which contains all or part of the entities shown in Figure 5.

NOTE: Local perception is obtained from the output of the local sensors data fusion and AI applications entities.

6.4 VRU-related functions in the ITS station architecture

Figure 5 proposes the main components of the ITS-S architecture that directly impact the VRU system operation. Other functions as defined in ETSI TS 102 894-1 [2] may be present and support the operation of these services, e.g. the communication support facilities. More details are provided in clause 6.5.

DRAFT

Figure 5: VRU functionality mapped to the ITS Station architecture

The VRU-specific functionality, including interfaces mapped to the ITS-S architecture, is shown in Figure 5. It is centred around the **VRU Basic Service** located in the facilities layer; it consumes data from other services located in the facilities layer such as PoTi and LDM, Data Provider and is linked with other as application support facilities, e.g. CA service, DEN service, Collective Perception Service, Manoeuvre Coordination Service, Infrastructure service, etc… The VRU basic service is responsible to transmit the VAM message, to identify whether the VRU is part of a cluster and to enable the assessment of the potential risk of collision.

The VRU Basic Service interacts with the VRU profile management entity in the management layer to learn whether the ITS-S has the VRU role, whether it acts as a single or cluster VRU, etc…

The application layer proposes a possible distribution of functional entities that would be involved in VRU use cases.

6.5 Function descriptions (informative)

6.5.1 General overview

The present clause describes the functions illustrated in Figure 4 and Figure 5.

The proposed functional descriptions are conceptual models which may produce different implementations. The specification of some exposed interfaces would contribute to make the ITS functionally testable and measurable in terms of minimum performances requirements.

This sub-clause proposes some backward compatible evolutions of the communication architecture in EN 302 665 [1] to support the VRU basic service, mainly focusing on the application layer, facilities layer and the management plane (see Figure 5).

DRAFT

6.5.2 VRU sensor system - IoT platform

The VRU sensor system is at least composed of the PoTi management function present in each ITS-S of the system. The PoTi entity provides the global time common to all system elements and the real time position of the mobile elements.

Local sensors may also be embedded in other mobile elements as well as in the road infrastructure (e.g. camera in a smart traffic light). The IoT platform which can be distributed over the system elements may contribute to provide additional information related to the environment surrounding the VRU system.

6.5.3 Local Sensor data fusion and actuator (including AI)

The sensor data fusion function is the fusion of local perception data obtained from different local sensors. Sensor data fusion relies on the consistency of its inputs and then to their timestamping which needs to correspond to one common given time.

6.5.4 Local perception

The local perception function is provided by the local processing of information collected by local sensor(s) associated to the system element (VRU device, vehicle, RSE) considered. Its main purpose is to detect and characterize objects (static and mobile) which are likely to cross the trajectory of the considered moving objects.

The infrastructure and particularly the road infrastructure may offer services relevant to the VRU support service. The infrastructure may have its own sensors detecting VRUs evolutions and then computing a risk of collision if also detecting local vehicles' evolutions, either directly via its own sensors or remotely via a cooperative perception supporting services such as the CPS (ETSI TR 103 562 [i.4]).

Generally, road marking (e.g. zebra areas) and vertical signs need to be considered to increase the confidence level associated with the VRU detection and mobility as normally, VRU have to respect these marking / signs.

6.5.5 Motion dynamic prediction

The motion dynamic prediction function is related to the behaviour prediction of the considered moving objects. Motion dynamic includes the moving object trajectory resulting from evolution of the successive mobile positions. A change of the moving object trajectory or of the moving object velocity (acceleration / deceleration) impacts the motion dynamic prediction. In most cases, when VRUs are moving, they still have a large amount of possible motion dynamic in terms of possible trajectories and velocities. So, the problem of motion dynamic prediction is to identify as quickly as possible which motion dynamic will be selected by the VRU and if this selected motion dynamic is subject to a risk of collision with another VRU or a vehicle.

The motion dynamic prediction function analyses the evolution of mobile objects which trajectories may meet at a given time and so create a risk of collision between them.

The motion dynamic prediction works on the output of cooperative perception considering:

- The current trajectories of considered VRUs for the computation of the path prediction.
- The current velocities and their past evolutions for the considered mobiles for the computation of the velocity evolution prediction,
- The reliability level which can be associated to these variables.

In many cases, working only on the output of the cooperative perception is not sufficient to make a reliable prediction because of the uncertainty which exists in terms of VRU trajectory selection and its velocity. However, complementary functions may assist in increasing consistently the reliability of the prediction, for example:

- The use of the VRU device navigation system which provides assistance to the VRU to select the best trajectory for reaching its planned destination. With the development of MaaS (Mobility as a Service, see

DRAFT

note below), multimodal itinerary computation may also indicate to the VRU dangerous areas and then assist to the motion dynamic prediction at the level of the multimodal itinerary provided by the system.

- The knowledge of the VRU habits and behaviours as very often VRUs follow the same itineraries (see example in annex A2) using similar motion dynamics when going to the main POI (Point of Interest) which is related to their main activities (e.g.: going at school, going to work, doing some shopping, going to the nearest public transport station from their home, going to sport centre…etc). The VRU device or a remote service centre may learn and memorize these habits.
- The indication by the VRU itself of its selected trajectory in particular when changing it (e.g. using a right turn or left turn signal similar to vehicles when indicating a change of direction)

NOTE: MaaS is a new European developing concept supporting the development of transport multi-modality. This service includes the calculation of multimodal transport itineraries proposed to users for going from one origin to a final destination. In the case of a VRU, a multimodal transport itinerary is composed of a succession of multimode transport segments, some of them involving VRU motions (walking or using a bike / scooter). These VRU motion segments can be the object of clearly described itineraries stressing the collision risk areas located on the VRU path.

The output of this function is provided to the risk analysis function.

6.5.6 Vehicle motion control

The vehicle motion control is a function under the responsibility of the human driver or of the vehicle if it is able to drive in automated mode.

It is then possible to act on the trajectory of the vehicle or on its speed.

6.5.7 Human – Machine Interface (HMI)

The Human Machine Interface (HMI) is not mandatory, but when present it enables:

- The configuration of initial data (parameters) in the management entities (e.g. VRU profile management) and in other functions (e.g. VRU Basic service management).
- The communication to the device owner of external events related to the VRU Basic service.
- Signalling a risk of collision (TTC > 2 seconds) being detected by at least one element of the system.
- Alerting about an immediate risk of collision (TTC < 2 seconds) detected by at least one element of the system.

Note: The Time To Collision (TTC) value evaluation and how it is used is described in more details in clause 6.5.1.5 "collision risk analysis".

In the case of a VRU, similar to a vehicle driver, the HMI provides the information to the VRU, considering its profile (e.g. for a blind person, the information is presented with a clear sound level). In most of the cases, it is recommended to use visual and audible information for VRUs.

6.5.8 Connected System / Information System

The VRU system is a connected system made of up to 4 different levels of equipment as represented on Figure 4. It is also an information system which collects in real time information resulting from events, processes the collected information and stores them together with processed results.

DRAFT

At each level of the VRU system, the information collection, processing and storage is related to the functional and data distribution scenario which is implemented.

6.5.9 Traffic Management System

Traffic Management System (TMS) collects data from interconnected system elements, then processes them and provides traffic information to road users. The processing of collected data is performed for well-defined services and supporting applications.

In the case of VRU protection, a TMS allows to collect data and disseminate the presence of VRUs in a larger area than a single road-side equipment. This may be useful for example in the case of a highway where vehicles are driving at high speed and need to be informed of a potential risk of collision earlier than on a rural road, or in smart cities where monitoring specific areas allows to inform drivers that a march is ongoing on a specific street.

In case of the MaaS deployment, the Traffic Management System can be transformed / extended into a Mobility Service management centre providing multimodal transport navigation and associated payment platform. Multimodal transport navigation also considers the space / time associated to road users' vulnerability (e.g. when pedestrian or using a soft transportation mean (bicycle, scooter, etc.).

6.5.10 ITS Station Application Layer

6.5.10.1 Global overview

The following functions are proposed to be located at the application layer level. However, if there is a generic and justified need to share them between several other applications, some of these functions may be moved to the facilities layer.

6.5.10.2 Device role setting

A VRU can be equipped with a portable device which needs to be initially configured and may evolve during its operation following context changes which need to be specified. This is particularly true for the setting-up of the VRU profile and type which can be achieved automatically at power on or via an HMI. The change of the road user vulnerability state needs to be also provided either to activate the VRU basic service when the road user becomes vulnerable or to de-activate it when entering a protected area.

The initial configuration can be set-up automatically when the device is powered up. This can be the case for the VRU equipment type which may be:

- VRU-Tx with the only communication capability to broadcast messages (yet complying with the DCC).
- VRU-Rx with the only communication capability to receive messages.
- VRU-St with full duplex communication capabilities.

During operation the VRU profile may also change due to some clustering or de-assembly. Consequently, the VRU device role will be able to evolve according to the VRU profile changes.

6.5.10.3 Remote Sensor data fusion and actuator (including AI)

The local perception obtained by the computation of data collected by local sensors may be augmented by remote data collected by elements of the VRU system (vehicles, RSE) via the ITS-S. These remote data are transferred using standard services such as the CPS. In such case it is necessary to fuse these data. The data fusion may provide at least three possible results:

- After a data consistency check, the received remote data are not coherent with the local data. In such case, the system element has to decide which source of data can be trusted and ignore the other.
- Only one input is available (e.g. the remote data). This means that the other source has not the possibility to provide information. In such case, the system element may trust the only available source.

- After a data consistency check, the two sources are providing coherent data which augment the individual inputs provided.

The use of AI is necessary to recognize and classify the detected objects (VRU, motorcycle, type of vehicle, etc.) but also their associated dynamics. The AI can be located in any element of the VRU system.

The same approach is applicable to actuators, but in this case, the actuators are the destination of the data fusion.

6.5.10.4 Cooperative Perception

The perception chain can be the fusion of several perception function results at predefined times (see Figure 6):

- The local perception is provided by the collection of information from the environment of the considered ITS element (VRU device, vehicle, infrastructure). This information collection is achieved using relevant sensors (optical camera, thermal camera, radar, lidar…etc.).
- The remote perception is provided by the provision of perception data via C-ITS (mainly V2X communication). Existing basic services like the Cooperative Awareness or more recent services such as the Collective Perception Service can be used to transfer a remote perception.
- Several perception sources may then be used to achieve the cooperative perception function. It is then necessary to verify the consistency of these sources at predefined instants and if not consistent, select the best one according to the confidence level associated with each perception variable.
- Generally, the relevant perception data elements are: the mobile object trajectory (succession of positions), the mobile object heading and the mobile object velocity at each sampling time.
- If various data elements coming from different sources are fused, it is necessary to identify common sampling periods (e.g. 100 milliseconds) that can be synchronized via the time management service proposed by POTI
- The result of the cooperative perception needs to respect the required level of accuracy such as specified by PoTi.

Figure 6: Example of a cooperative perception conceptual model

The associated confidence level is necessary to build the cooperative perception resulting from the fusion in case of differences between the local perception and the remote perception. It will be also necessary for the exploitation by other functions (e.g. risk analysis) of the cooperative perception result.

The perception functions from the device local sensors processing to the end result at the cooperative perception level may present a significant latency time of several hundred milliseconds. For the characterization of a VRU trajectory and

its velocity evolution, there is a need for a certain number of the vehicle position measurements and velocity measurements thus increasing the overall latency time of the perception. Consequently, it is necessary to estimate the overall latency time of this function to take it into account when selecting a collision avoidance strategy.

6.5.10.5 Collision risk analysis

The collision risk analysis analyses the motion dynamic prediction of the considered moving objects associated to their respective levels of confidence (reliability). The objective is to estimate the likelihood of a collision and then to identify as precisely as possible the Time To Collision (TTC) (see also note for using other variables in clause 3.1) if the resulting likelihood is high. Figure 7 provides an example of TTC calculation and use.

Figure 7: Example of TTC calculation

The two following conditions are mandatory to be able to calculate the TTC:

- Two or more considered moving objects follow trajectories which intersect somewhere at a position which can be called "potential conflict point".
- If the moving objects maintain their motion dynamics (trajectories, speeds) it is possible to predict that they will collide at a given time which can be estimated through the computation of the time (called TTC) necessary for them to arrive simultaneously at the level of the identified potential conflict point.

From Figure 7, it can be derived that:

- A TTC prediction can only be reliably established when the VRU enters the collision risk area, that is to say very late in this example (1.75 seconds before reaching the potential conflict point). This is due to the uncertainty nature of the VRU pedestrian motion dynamic (mainly its trajectory) before deciding to cross the road.
- At the potential conflict point level, another measurement, the TDTC (Time Difference for pedestrian and vehicle travelling to the potential conflict point) can be used to estimate the collision risk level. For example, if it is not acted on the motion dynamic of the pedestrian or / and on the motion dynamic of the vehicle, TDTC is equal to ZERO and the collision is certain. Increasing the TDTC reduces the risk of collision between the VRU and the vehicle.

- The potential conflict point is in the middle of the collision risk area which can be defined according to the lane width (e.g. 3.5 meters) and vehicle width (maximum 2 meters for passenger cars).

The TTC is one of the variables that can be used to define a collision avoidance strategy and the operational collision avoidance actions to be undertaken. Other variables may be considered such as the road state, the weather conditions, the triple of {Longitudinal Distance (LoD), Lateral Distance (LaD), Vertical Distance (VD)} and the mobile objects capabilities to act to avoid a collision.

The likelihood of a collision associated to the TTC may also be used as a triggering condition for the broadcast of messages (e.g. an infrastructure element getting a complete perception of the situation may broadcast DENM, IVI (contextual speed limit), CPM or MCM).

6.5.10.6 Collision risk avoidance

The collision risk avoidance includes the collision avoidance strategy to be selected according to the TTC value and the identification of manoeuvre coordination / vehicle motion control to achieve the collision avoidance.

The collision avoidance strategy needs also to consider several environmental conditions:

- Visibility conditions related to the local weather,
- Vehicle stability conditions related to the road state (e.g. slippery),
- Vehicle braking capabilities.

The collision avoidance strategy needs to consider the action capabilities of the VRU according to its profile, the remaining TTC, the road and weather conditions as well as the vehicle autonomous action capabilities.

For example, when in good conditions, it is possible to trigger a collision avoidance action when the TTC is greater than two seconds (one second for the driver reaction time and one second to achieve the collision avoidance action). Below two seconds it can be considered being in a “pre-crash” situation and so needing to trigger a mitigation action to reduce the severity of the collision impact for the VRU.

The possible collision avoidance actions and impact mitigation actions have been listed in requirement FSYS08 in clause 5.

A road infrastructure element such as a Road Side Equipment may include a collision risk analysis function as well as a collision avoidance function, and provide collision avoidance actions to the neighbouring VRUs and vehicles. The collision avoidance actions can be proposed using MCM as done in the French PAC V2X project.

The road infrastructure may also offer services to support the road crossing by VRU such as traffic lights. When a VRU starts to cross a road at a traffic light level authorizing him, the traffic light should not change of phase as long as the VRU has not completed its crossing. Accordingly, the VRU awareness message (VAM) should contain data elements enabling the traffic light to determine the end of the road crossing by the VRU.

6.5.10.7 Event detection

The event detection function assists the VRU basic service during its operation when transiting from one state to another (see **Error! Reference source not found.**).

The main events to be considered are:

- change of a VRU role when a road user becomes vulnerable (activation) or when a road user is not any more vulnerable (de-activation).
- change of a VRU profile when a VRU enters a cluster with other VRU(S) or with a new mechanical element (bicycle, scooter, moto…etc), or when a VRU cluster is disassembling.

DRAFT

- risk of collision between one or several VRU(s) and at least one other VRU (using a VRU vehicle) or a vehicle. Such event is detected via the perception capabilities of the VRU system.
- change of the VRU motion dynamic (trajectory or velocity) which will impact the TTC and the reliability of the previous prediction.
- change of the status of a road infrastructure piece of equipment (e.g. a traffic light phase) impacting the VRU movements.

6.5.10.8 Infrastructure services

Existing infrastructure services such as those described below can be used in the context of the VRU basic service:

- The broadcast of the SPAT (Signal Phase And Timing) & MAP (SPAT relevance delimited area) is already standardized and used by vehicles at intersection level. In principle they protect VRUs crossing. However, signal violation warnings may exist and can be detected and signalled using DENM. This signal violation indication using DENMs is very relevant to VRU devices as indicating an increase of the collision risk with the vehicle which violates the signal. If it uses local captors or detects and analyses VAMs, the traffic light controller may delay the red phase change to green and allow the VRU to safely terminate its road crossing.
- The contextual speed limit using IVI (In Vehicle Information) can be adapted when a large cluster of VRUs is detected (ex: limiting the vehicles' speed to 30 km / hour). At such reduced speed a vehicle may act efficiently when perceiving the VRUs by means of its own local perception system.

6.5.10.9 Manoeuvre coordination

This function executes the collision avoidance actions which are associated to the collision avoidance strategy which has been decided. This function should be present at the vehicle level and may be present at the VRU device level according to the VRU profile.

At the vehicle level, this function interfaces the vehicle electronics controlling the vehicle dynamic state in terms of heading and velocity.

At the VRU device level, this function may interface the HMI support function, according to the VRU profile, to be able to issue a warning or alert to the VRU according to the TTC.

Manoeuvre coordination can be proposed to vehicles from an infrastructure element which may obtain a better perception of the motion dynamic of involved moving objects by means of its own sensors or their fusion with remote perception obtained from standard messages such as CAMs.

6.5.11 ITS Station Facilities Layer

6.5.11.1 VRU basic service

The VRU basic service is supported by a set of functions illustrated in Figure 8: VRU basic service functional conceptual model

. They will be further detailed in TS 103 300-3.

The VRU basic service interacts with functions such as represented in Figure 5.

DRAFT

Figure 8: VRU basic service functional conceptual model

VRU basic service management

The basic service management function performs the following operations:

- Store the assigned ITS AID and the assigned Network Port to use for the VRU Basic service.
- Store the VRU parameters received at initialisation time or updated later for the coding of VAM data elements.
- Receive information from and transmit information to the HMI.
- Activate / deactivate the VRU basic service according to the device role parameter (for example, the service is deactivated when a pedestrian enters a bus)
- Manage the triggering conditions of VAM transmission in relation to the network congestion control. For example, after activation of a new cluster, it may be decided to stop the transmission of element(s) of the cluster.

VRU Cluster management

The VRU cluster management function performs the following operations:

- Detect if the associated VRU can be the leader of a cluster.
- Compute and store the cluster parameters at activation time for the coding of VAM data elements specific to the cluster.
- Manage the state machine associated to the VRU according to detected cluster events (see the state machines examples provided in 6.2.4).
- Activate or de-activate the broadcasting of the VAMs or other standard messages (DENMs) according to the state and types of associated VRU.

VAM Reception management

The VAM reception management function performs the following operations after VAM messages decoding:

- Check the relevance of the received message according to its current mobility characteristics and state.
- Check the consistency, plausibility and integrity (see the liaison with security protocols) of the received message semantic.
- Destroy or store the received message data elements in the LDM according to previous operations results.

DRAFT

VAM Transmission management

The VAM Transmission management function is only available at the VRU device level not at the level of other ITS elements. Even at the VRU device level, this function may not be available according to its initial configuration (see device role setting function).

The VAM transmission management function performs the following operations upon request of the VRU basic service management function:

- Assemble the message data elements in conformity to the message standard specification.
- Send the constructed VAM to the VAM encoding function.

VAM Encoding

The VAM encoding function encodes the Data Elements provided by the VAM transmission management function in conformity with the VAM specification.

The VAM encoding function is available only if the VAM transmission management function is available.

VAM Decoding

The VAM decoding function extracts the relevant Data Elements contained in the received message. These data elements are then communicated to the VAM reception management function.

The VAM decoding function is available only if the VAM reception management function is available.

6.5.11.2 LDM

The Local Dynamic Map (LDM) is the repository of all the dynamic data elements which are required to perform the functions supporting the VRU basic service.

Consequently, the LDM content should be accessible directly from dedicated VRU and vehicle facilities layer functions and via an exposed interface (FA SAP: Facilities – Application service access point) from application layer functions. This LDM access is controlled by the LDM management function (see Figure9). These functions are also able to store and update data elements in the LDM.

Figure9: Example of LDM conceptual model

Dynamic objects are VRUs, vehicles, road infrastructure objects (e.g. traffic lights) etc. They are identified by a unique identifier and are characterized by dynamic data elements (DE) which need to be updated in real time (e.g. with a sampling period of 100 milliseconds).

Dynamic object characteristics may be kept in the LDM for some time (Past) to build the path history of the dynamic object evolutions (vehicles, VRUs) which is necessary to predict their evolutions in the future (motion dynamic prediction). The motion dynamic prediction can be achieved by navigation function knowing the VRU itinerary and by learning VRU behaviour during frequently used itineraries.

6.5.11.3 PoTI

PoTi (Position and Time Management) is specified in ETSI EN 302 890-2 [5].

The PoTi function is present in vehicles ITS-S and VRU ITS-S. It may also be present in an infrastructure ITS-S and be used to develop a positioning augmentation service.

Position accuracy and confidence level are key performance indicators which are part of PoTi specification.

6.5.11.4 Other Application Support Facilities: CA, DEN, CPS, MCS, SPaT, etc.

Other application support facilities functions are responsible to trigger the transmission of their related messages and forward the messages received to the relevant applications.

6.5.11.5 Decentralized Congestion Control (DCC-FAC)

The Decentralized Congestion Control (DCC) function acts to optimize the use of the available channel bandwidth during peak traffic, thus avoiding its congestion.

For this purpose, according to current and anticipated channel load, the DCC cooperates with the VRU Basic service function to adjust the VAM transmission to limit the use of the VRU service selected channel to the strict necessity. This requires developing rules defining transmission triggering conditions when necessary with the objective to respect the DCC specifications (ETSI TS 103 175 [i.18]).

6.5.12 ITS Station Management Entity

6.5.12.1 VRU profile management

The VRU profile management function is an important support element for the VRU basic service as managing the VRU profile during a VRU active session. The profile management is part of the ITS-S configuration management and is then initialized with necessary typical parameters' values to be able to fulfil its operation. The ITS-S configuration management is also responsible of updates (ex: new standard versions) which are necessary during the whole life cycle of the system.

When the VRU basic service is activated (vulnerability configured), the VRU profile management needs to characterize a VRU personalized profile based on its experience and on provided initial configuration (generic VRU type). The VRU profile management may then continue to learn about the VRU habits and behaviours with the objective to increase the level of confidence (reliability) being associated to its motion dynamic (trajectories and velocities) and to its evolution predictions.

The VRU profile management is able to adapt the VRU profile according to detected events which can be signalled by the VRU basic service management and the VRU cluster management (cluster building or cluster disassembly).

According to its profile, a VRU may or may not be impacted by some road infrastructure event (e.g., evolution of a traffic light phase), so enabling a better estimation of the confidence level to be associated to its movements. For example, an adult pedestrian will likely wait at a green traffic light and then cross the road when the traffic light turns to red. An animal will not take care of the traffic light colour and a child can wait or not according to its age and level of education.

DRAFT

6.6 Security considerations

6.6.1 Security mechanisms by information flow

Information flows are identified in this section by the alphanumeric identifiers used in clause 4.5. In the electronic version of this document, each information flow identifier is a clickable link that links to the security analysis in the relevant part of clause 4.5.

The following information flows / entity activities are implemented with a broadcast transmission pattern and can be secured with the standard mechanisms of TS 103 097 [6].

- EA1-1.1, EA2-1.1, EA2-1.2, EA2-2.1, EB1-1.1, EB1-1.2, EB1-1.3, EB1-1.4, EB1-1.5, EB2-1.1, EB2-1.2, EB2-1.3, EB3-1.2, EB3-1.3, EB4-1.1, EB5-1.1, EB5-1.2, EC1-2.1, ED1-1.1, ED1-2.1, ED2-1.1, ED3-1.1, ED3-3.1, ED4-2.1, EF1-1.1, EF1-1.2, EF1-2.1, EF2-2.1, EF2-2.2

The following information flows may be implemented with a broadcast transmission pattern or with a unicast transmission pattern. Which approach is taken is a design decision. Security mechanisms for these flows will therefore be specified in the Stage 3 document.

- EB3-1.1, EF2-1.1

The following information flows are implemented by a siren and have no communications security mechanism associated with them:

- ED1-2.2, EF1-2.2

The following information flows are implemented as part of communications with a cloud service. For these information flows, the present document does not specify a particular communications security mechanism. However, any communications security mechanism implemented must be capable of meeting the integrity requirements of the flow. This can be accomplished with standard internet security mechanisms such as Transport Layer Security (TLS) [i.8, i.9]

- EE1-1.1, EE1-2.1, EE2-1.1, EE2-2.1, EE2-2.2

The following information flows are implemented by sensor perception and communication of that sensor information to an ITS-S. These information flows shall be protected by a persistent communications security mechanism that meets the integrity requirements of the flow. This standard does not specify a particular communications security mechanism to be used.

- EC1-1.1, ED3-2.1, ED4-1.1

6.6.2 Roles

6.6.2.1 Overall roles

A “role” is an identifier corresponding to a set of activities such that any actor with that role may carry out any of the activities in the set. One goal of the security analysis is to identify natural roles in the system from a security perspective, i.e. collections of activities such that if an actor can do one of the activities maliciously, there is no significant increase in system risk if that actor can do all of those activities maliciously. Other methods to determine roles are possible – for example, a natural way to choose roles is to select those roles to have a correspondence to “real-world” roles within the application – but it is recommended to derive the “natural security roles” as described in this paragraph so that whatever application roles are eventually selected, the security properties of those roles are properly understood.

The security analysis indicates that the following roles are appropriate:

- VRU
  - Person with reduced / impaired mobility
- Vehicle
  - Vehicle associated with a rider
  - Sensor-equipped vehicle (see UC-C1)
- Priority Vehicle
- Infrastructure device

DRAFT

  - Infrastructure device equipped with sensors (Note: This will be authorized using the Collective Perception ITS-AID).
- Cloud service

The associated requirement is that the final design is able to identify the role of each actor whether by different ITS-AIDs, or by different Service Specific Permissions (SSPs) associated with a shared ITS-AID, or by some other mechanism if appropriate. The mechanism used to identify the roles of particular actors in particular uses cases will be specified in TS 103 300-3 [i.11].

6.6.2.2 Entitlement to roles

The identification of roles creates two design requirements:

- The design shall provide a mechanism for participants in use cases to determine that counterparties are entitled to act in the appropriate role
- The design shall provide a mechanism for credential issuance systems (in the terms of TS 102 940, Authorization Authorities (AAs) that issue Authorization Tickets (ATs)) to determine that end-entities requesting ATs are entitled to act in the role requested.

The Stage 3 document will contain guidance for how end-entities can, as appropriate, provide assurance to AAs. The details of this will depend on the design choices made in that document.

6.6.3 Pseudonymity

As noted in the security analysis, actors acting in the VRU and Vehicle role require pseudonymity. For actors in both of these cases, for all broadcast information flows, pseudonymity is provided by having multiple certificates.

For actors in the Vehicle role, the messages sent and the associated communications patterns are specified in other documents and pseudonymity (number of certificates, certificate change algorithms and mechanisms) is specified in those or related documents.

For actors in the VRU role, the requirement for pseudonymity should be interpreted taking the following into account:

- VRU devices are even more tightly coupled to individuals than are vehicle-resident devices
- VRU devices can give away more information about movements than vehicle-resident devices: vehicle-resident devices can show where you park at the mall, but VRU devices can show which exact shop you go into.
- VRUs transmit only intermittently in many scenarios.
- Most VRU devices will have good connectivity to a network.
- Most VRU devices will have the ability to demonstrate to an AA that they are in a known valid state (this is known as “attestation”)
- A VRU device will accompany its VRU for a large number of hours per day and may be active or potentially active for a long period of time (during a shopping expedition in a city centre, or while the device owner is out for a long run or bike ride)

Based on these properties, the following goals are identified:

- A VRU device should have more flexibility to change certificates than vehicles do under the current certificate policy. For example:
  - A VRU device should be able to change certificates whenever it has been silent for more than 5s.
- A VRU should be able to request new certificates during the course of its operations, subject to policy about (a) whether the VRU device has reached an upper limit on the number of certificates requested (b) whether the VRU device has demonstrated that previous certificates have been disposed of (using, for example, the attestation mechanism referred to above) (c) other considerations.

These goals will be translated into design specifications in the Stage 3 document.

DRAFT

6.6.4 Misbehaviour Detection

The Stage 3 document will not contain a specification for misbehaviour detection and reporting, although these should be included in a future standard. A VRU device that causes false alerts, or a VRU device that creates messages that are physically inconsistent with each other, should be considered for reporting and blacklisting.

6.7 Impact of the deployment and automation level roadmap

6.7.1 Introduction

The C-ITS platform final report [i.5] has defined a set of C-ITS services for Day-1 and Day 1.5 deployments. The protection of VRUs (pedestrian and cyclists) is considered in the list of Day 1.5 services. In parallel, OEMs are enhancing the vehicle security by increased ADAS capabilities, with a higher level of automation of the vehicles (see SAE J3016 [i.19]) and geo-positioning is getting a higher precision.

It is considered at CEN TC 226 WG12 that the horizontal marking and vertical signs are not sufficiently reliable for the automated vehicle to move in a safe automated driving. It is then decided to add a redundant method consisting of an accurate digital map (twin of the road marking and vertical signs) which should be extended with relevant information dedicated to automated vehicles. The digital map accuracy needs to be better than 10 centimetres leading to have a similar accuracy level for the vehicle positioning system to be able to make an accurate map matching of the mobile object.

NOTE: The map matching is the method used to position a mobile object on the digital map of the vehicle. The horizontal marking and vertical signs are currently used by the automated vehicle to move on the roads. However, these resources are not reliable enough as they are not always visible. Therefore, vehicle manufacturers and their suppliers are now developing a redundant accurate digital map. But they need to obtain a vehicle positioning system which enables to position the vehicle at the lane level (map matching of the vehicle positions). Then the vehicle needs to stay in the selected lane especially when turning at an intersection.

The objective of clause 6.7 is to clarify how the VRU functional architecture can be transposed in this roadmap and provide the protection of VRUs starting from the very early deployments.

6.7.2 Functional architecture of VRU system with Day 1 services

Services for Day-1 deployment - assumptions

These services target vehicle safety, motorway and urban use cases. They are based on awareness messages (CAM, MAP, SPaT), notifications (DENM) and in vehicle information.

The C-ITS communication is essentially V2V or I2V.

The level of vehicle automation is expected to be at a low SAE level between 0 and 2 (see SAE J3016 [i.19]). The vehicle is equipped with local sensors only, directly connected to the vehicle on-board system. RSE containing an ITS-S may be equipped with cameras or presence sensors to increase green times at crossings or send contextual speed messages (CSM).

Components of the VRU functional architecture

Even though VRU protection is not part of Day 1 services, the following components of the VRU system architecture are already available in this phase:

Referring to Figure 4:

- The VRU level is not C-ITS enabled
- The vehicle level includes the V-ITS-S and the following functions: Local Perception, Ego-trajectory prediction, HMI and vehicle connected system

DRAFT

- The roadside level includes the R-ITS-S and the following functions: Local Perception, mobile objects trajectory prediction, HMI (optional) and RSE connected system
- The central level includes the C-ITS-S and all the functions displayed at this level in Figure 2

Methods to detect VRU at risk

The risk of a potential collision shall be detected using one of the following methods:

- In vehicle, detection by a local sensor interacting with the V-ITS-S
- In vehicle, reception of a CAM or DENM signalling the presence of VRUs (pedestrians, cyclists) on the road
- In infrastructure (roadside and central level), detection of VRUs in designated areas (zebra crossing, road), while vehicles are authorised on the same areas (and vice versa).

NOTE: Detecting a VRU at risk requires to be able to predict reliably the motion dynamic of the VRU as soon as possible. In most cases, this is not possible before a short TTC because of the large number of possible trajectories and velocities at the VRU level. To increase the TTC and avoid either false positive information or very late valid positive information, it is then necessary to rely on other functions such as the VRU navigation system, or machine learning system memorizing VRU habits and behaviour from repetitive motion dynamic.

Methods to signal VRU at risk or prevent the risk

The risk of a potential collision with a VRU shall be notified or mitigated using one of the following methods:

- Direct warning to the vehicle driver through the HMI
- DENM sent by a R-ITS-S or a V-ITS-S to the neighbouring ITS-S
- Action from an R-ITS-S on a traffic light controller.

6.7.3 Functional architecture of VRU system with Day 1.5 services

Services for Day-1.5 deployment - assumptions

The roadmap of service deployment is incremental. Accordingly, the Day 1 services are present in this phase. Additional services of interest are the CPS and the VRU basic service. New messages are available to the ITS stations: CPM and VAM.

The C-ITS communications additionally includes VRU2VRU, V2VRU/VRU2V as well as I2VRU/VRU2I.

The level of vehicle automation is at a medium SAE level between 2 and 4 (see SAE J3016 [i.19]). Actions can be performed on the vehicle, C-ITS warnings can be displayed on the on-board system, but the driver has still the control of the vehicles. RSE containing an ITS-S may be equipped with cameras or presence sensors and actively participate to the C-ITS traffic safety.

Components of the VRU functional architecture

The following components of the VRU system architecture are available in this phase:

Referring to Figure 4:

- The VRU level includes all the functions present in the figure
- The vehicle level includes all the functions present in the figure, except for the vehicle motion control function

DRAFT

- The roadside level includes all the functions present in the figure
- The central level includes all the functions present in the figure

Methods to detect VRU at risk

The risk of a potential collision shall be detected using one of the following methods:

- All methods used with Day 1 services
- In the VRU device, reception of a CAM or DENM signalling the presence of a vehicle crossing the VRU predicted trajectory
- In the VRU device, reception of a VAM signalling the presence of a VRU crossing the VRU predicted trajectory. However, this does not apply when the two VRUs are from Profile 1 (see clause 6.1).
- In vehicle, reception of a CPM signalling the presence of a vehicle crossing the VRU predicted trajectory. This may be correlated with information received from local sensors.
- In infrastructure (roadside and central level), analysis of predicted trajectories for the mobile objects and identification of a potential collision.

Methods to signal VRU at risk or prevent the risk

The risk of a potential collision with a VRU shall be notified or mitigated using one of the following methods:

- All methods used with Day 1 services;
- Direct warning to the VRU through the HMI or through an HMI located in the R-ITS (for example a beep from the traffic light);
- VAM sent by the ITS-S in the VRU-device;
- CPM sent by a R-ITS-S or a V-ITS-S to the neighbouring ITS-S;
- Action on the vehicle depending on its level of automation (slowing down, braking, changing lane, etc.).

6.7.4 Functional architecture of VRU system with beyond-Day 1.5 services

Services for beyond-Day-1.5 deployment - assumptions

The roadmap of service deployment is incremental. Accordingly, the Day 1.5 services are present in this phase. As this is not yet fully defined, the expectation is that all planned C-ITS services are available, for example the MCM.

The C-ITS communications additionally includes all types of exchanges as defined in Figure 1.

The level of vehicle automation is from a medium to high (i.e. fully automated) SAE level between 3 and 5 (see SAE J3016 [i.19]). Actions can be performed on the vehicles, warnings can be displayed on the on-board system, but the driver may not have the control of the vehicle. RSE containing an ITS Station actively participate to the C-ITS traffic safety.

Components of the VRU functional architecture

The following components of the VRU system architecture are available in this phase:

Referring to Figure 4:

- The VRU level includes all the functions present in the figure
- The vehicle level includes all the functions present in the figure

DRAFT

- The roadside level includes all the functions present in the figure
- The central level includes all the functions present in the figure

Methods to detect VRU at risk

The risk of a potential collision shall be detected using one of the following methods:

- All methods used with Day 1.5 services

Methods to signal VRU at risk or prevent the risk

The risk of a potential collision with a VRU shall be notified or mitigated using one of the following methods:

- All methods used with Day 1.5 services
- MCM sent by a R-ITS-S or a V-ITS-S to the neighbouring ITS-S
- If the level of automation of the vehicle is high and the driver does not have the control of the vehicle, it may be questionable to display a direct warning to the vehicle driver through the HMI, but this is out of scope of the present specification.

6.8 Interfaces between entities

6.8.1 Introduction

The interfaces between different ITS stations of different levels of the architecture, i.e. external interfaces, and those between different functional components of each level, i.e. internal interfaces, are illustrated in Figure 3. The interfaces between the VRU Basic Service and other facilities layer entities in the ITS-S architecture are illustrated in Figure 4.

,

6.8.2 External interfaces

Parameters of the external interfaces shall include the descriptive, physical and dynamic state information of a VRU so that the collision risk can be estimated and warned, and the strategy for collision avoidance can be deduced. The parameters may also include additional information of a VRU cluster for efficient network traffic.

Table 31: External interfaces

Interface	Description
Personal ITS Station ←→ Vehicle ITS Station	CAM and VAM messages are sent bidirectional to exchange information on type of road user, absolute position, velocity etc. between nearby road users. For a collision risk warning at intersections, a Vehicle ITS Station can send a DENM message with intersection collision warning for left/right turning or crossing scenarios.
Personal ITS Station ←→ Roadside ITS Station	VAM messages are broadcasted by Personal ITS Stations and can be used by the Roadside ITS Stations. The Roadside ITS Stations can send warnings on signal violations or intersection collision risk via DENM. The Roadside ITS Stations can send CPMs regarding the presence of VRUs.
Personal ITS Station ←→ Central ITS Station	This interface can be used for applications to exchange non-geographical related information via a central system. The central ITS-S can detect a risk of collision by using VAM sent by a personal ITS-S and information from vehicles.

DRAFT

Vehicle ITS Station ←→ Roadside ITS Station	CAM messages are broadcasted by Vehicle ITS Stations and can be used by the Roadside ITS Stations to estimate the collision risk. The Roadside ITS Stations can send warnings on signal violations or intersection collision risk via DENM. Assistance messages via SPaT for turning and/or crossing where a Personal ITS Station can be present along the trajectory (as defined in ETSI TS 103 301 [i.13]) are focussing on I2V. Roadside ITS-S may also broadcast CPMs (awareness) or MCMs (automated vehicle motion control) regarding the presence of VRUs.
Vehicle ITS Station ←→ Central ITS Station	This interface is used to exchange appropriate ETSI C-ITS messages specified for the Vehicle ITS Station and Central ITS Station.
Roadside ITS Station ←→ Central ITS Station	This interface is used to exchange appropriate ETSI C-ITS messages specified for the Roadside ITS Station and Central ITS Station.
Vehicle ITS Station ←→ Vehicle ITS Station	This interface is used to disseminate CPMs regarding the presence of VRUs. A vehicle perceiving a VRU may broadcast a CPM signalling the VRU to other vehicles. If a vehicle receiving a CPM identifies a risk of collision with the signalled VRU, a collision avoidance action can be triggered.

Further details for the VAM message are provided in clause 6.9.

6.8.3 Internal interfaces

Data exchanged via the internal interfaces of the VRU system are used to generate the parameters to be sent via the external interfaces and used to estimate/predict the collision risk and avoid the predicted collision from the parameters received via the external interfaces.

1) VRU level

Table 32: Internal interfaces at VRU level

From	To	Parameters
VRU device sensor system	Sensor data fusion and actuator Local Perception Personal ITS Station	Data obtained from various local sensors of the VRU level
Sensor data fusion and actuator	Motion prediction Local Perception Personal ITS Station	Fusion data from information obtained from various local sensors of the VRU level
Local Perception	Personal ITS Station	Perception data processed from information obtained from various local sensors of the VRU level
Motion prediction	Personal ITS Station	Manoeuvre prediction of the VRU level
Personal ITS Station	VRU Connected System and HMI	Information of the Personal ITS Station to advise or instruct the associated road user such as a pedestrian, cyclist or PTW driver via an external HMI (e.g. smartphone)

2) Vehicle level

DRAFT

Table 33: Internal interfaces at vehicle level

From	To	Parameters
Vehicle sensor system	Sensor data fusion and actuator Local Perception Vehicle ITS Station	Data obtained from various local sensors of the Vehicle level
Sensor data fusion and actuator	Motion prediction Local Perception Vehicle ITS Station	Fusion data from information obtained from various local sensors of the Vehicle level
Local Perception	Vehicle ITS Station	Perception data processed from information obtained from various local sensors of the Vehicle level
Motion prediction	Vehicle ITS Station Vehicle motion control	Manoeuvre prediction of the Vehicle level
Vehicle ITS Station	Vehicle motion control	Information to control the Vehicle level
Vehicle ITS Station	Vehicle Connected System and HMI	Information of the Vehicle ITS Station to advise or instruct the associated road user such as a vehicle driver and motorcycle driver via an external HMI

3) Roadside level

Table 34: Internal interfaces at roadside level

From	To	Parameters
Roadside sensor system	Sensor data fusion and actuator Local Perception Roadside ITS Station	Data obtained from various local sensors of the Roadside level
Sensor data fusion and actuator	Mobile object prediction Local Perception Roadside ITS Station	Fusion data from information obtained from various local sensors of the Roadside level
Local Perception	Roadside ITS Station	Perception data processed from information obtained from various local sensors of the Roadside level
Mobile object prediction	Roadside ITS Station	Manoeuvre prediction of mobile objects
Roadside ITS Station	RSE Connected System and HMI	Information of the Personal ITS Station to advise or instruct the associated road user such as a roadside operator

4) Central level

DRAFT

Table 35: Internal interfaces at Central level

From	To	Parameters
Sensor	TMS (Traffic Management System)	Data obtained from various local sensors of the Central level.
TMS (Traffic Management System)	Central Traffic Management Console and HMI Local	Traffic and road state information, i.e. the actual status of flow/velocity/travel times and measures, warnings and status of traffic signs.
Central Traffic Management Console and HMI	Central ITS Station	Information on (road works) warnings or route advice to cooperative vehicles via Central ITS Station – Roadside ITS Station – Vehicle ITS Station. Optionally dynamic road signalling information could be sent over this interface.
Central ITS Station Central Traffic Management Console and HMI	Internet Information System	Specific information or request for specific information for internet-based applications
Internet Information System	Central ITS Station Central Traffic Management Console and HMI	Specific information or response for specific information for internet-based applications

Further details for the parameters of the internal interfaces are described in clause 6.5.2 to 6.5.8.

6.8.4 VRU Basic Service interfaces

The interactions between the VRU Basic Service and other facilities layer entities in the ITS-S architecture are used to obtain information for the generation of the VAM. The interfaces for these interactions are described in the Table X below.

Table 36: VRU Basic Service interfaces

Interfaced functionality	Parameters
PoTi	Information of the positioning and timing are sent to the VRU Basic Service. Further details are described in clause 6.5.10.3.
DCC-FAC	Information to optimize the use of the available channel are sent to the VRU Basic Service. Further details are described in clause 6.5.10.5.
HMI support	Information to be exchanged with a VRU. Further details are described in clause 6.5.7.
LDM	LDM data are sent to the VRU Basic Service. Further details are described in clause 6.5.10.2.
Other Application Support Facilities	Information to trigger the transmission of messages are sent to the VRU Basic Service. The VRU Basic Service forwards received messages to the relevant applications. Further details are described in clause 6.5.10.4.

6.9 Vulnerable Road User Awareness Message, VAM

This new message specified for the VRUs awareness is very close to the existing Cooperative Awareness Messages (CAM) defined in EN 302 637-2 [3]. The use shall be limited to the VRU profiles given in clause 6.1.

DRAFT

The Vulnerable Road User Awareness Message (VAM) shall contain all required data depending on the VRU profile and the actual environmental conditions. The following data field should be available in the VAM:

- VAM header including VRU identifier (mandatory)
- VRU position (mandatory)
- Generation time (mandatory)
- VRU profile (mandatory)
- VRU type e.g. VRU profile is pedestrian, VRU type is infant, animal, adult, child, etc. (mandatory)
- VRU cluster identifier (optional)
- VRU cluster position (optional)
- VRU cluster dimension (geographical size) (optional)
- VRU cluster size (number of members in the cluster) (optional)
- VRU size class (mandatory if outside a VRU cluster, optional if inside a VRU cluster)
- VRU weight class (mandatory if outside a VRU cluster, optional if inside a VRU cluster)
- VRU speed (mandatory)
- VRU direction (mandatory)
- VRU orientation (mandatory)
- Predicted trajectory (succession of way points) (optional)
- Predicted velocity (including 3D heading and average speed) (optional)
- Heading change indicators (turning left or turning right indicators) (optional).

7 Impact on existing standards and protocols

7.1 Introduction

In this clause the requirements onto the existing C-ITS standards and protocols for the messages used for the VRUs are presented.

7.2 Facilities Layer

- In the Facilities Layer [i.12] [i.13] [i.14]
  - VRU Basic Service (new standard needed for this service as TS 103 300-3)
    - VAM generation rules and triggering management
    - VAM RX and VAM TX
    - VAM encoding and construction
    - VAM decoding and decomposition
    - Adding new definitions of data elements in the Common Data Dictionary (CDD, ETSI TS 102 894-2 [i.14]) if necessary.
  - PoTI

DRAFT

    - Add specification of VRU clusters reference point

- LDM
- Other Application Support Facilities: CA, DEN, CPS, MCS, SPaT, etc.
    - CA: No specific requirements and impacts are foreseen at this stage, since a separate message has been used for the VRU standard message (i.e. the VAM).
    - DEN: Detail the cause code values according to the VRU profile (for example, the sub-cause codes of humanPresenceOnTheRoad (12), collisionRisk (97)). Triggering conditions should be revised as well.
    - CPS: Align the classification of VRUs according to the profiles specified in clause 6.1.
    - MCS: Future use of VAM information in the MCS processing for reliability enhancements
    - SPaT: processing of SPaT information received by the VRU for awareness and e.g. red-light violation warning
    - MAP: High resolution map of actual crossing (better than 10cm)

7.3 Networking & Transport Layer

The VAM and the related functionalities are Networking & Transport layer agnostic. No specific requirements and impacts on the Networking & Transport layer are expected.

Note: For GeoNetworking a higher resolution of the addressing might be needed. In addition, a separate cluster addressing might be needed.

7.4 Access Layer

The VAM and the related functionalities are access layer agnostic. No specific requirements and impacts on the access layer are expected.

Note: No specific VRU related functionalities are foreseen. Nevertheless, a better positioning capability of the access layer as provided by IEEE 802.11bd might be useful.

7.5 Management Entity

Take into account the VRU profile management??

7.6 Security Entity

This requirements analysis does not indicate that any changes are necessary to the security entity as specified in ETSI EN 302 665 [1].

8 Conclusion

The present document introduces a complete VRU ITS system concept including:

- safety analyses of the use case in clause 4.5,
- requirement set for the use with VRUs, combined VRUs and VRU clusters in clause 5,

DRAFT

- a functional architecture specification in clause 6 and,
- the relevant interfaces and interactions with other relevant ITS standards and entities in clause 7. The system concept is based on the use cases in TR 103 300-1 [i.1].

The originally proposed 3 VRU profiles in TR 103 300-1 [i.1] have been extended by a Profile 4 covering the specifies of animals participating in the traffic. These profiles are descripted in clause 6.1.

The content of the present document will be used as input to ETSI TS 103 300-3: "Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 3: VRU Basic service; Release 2". where the communication protocols, message format, semantics and syntax as well as key interfaces and protocol operation for the VRU awareness service will be specified.

DRAFT

Annex (informative): Bibliography

-

DRAFT

Annex (informative): Change History

Date	Version	Information about changes
July 2019	0.0.2	Initial draft with the skeleton of the planned TS uploaded for ETSI ITS WG1#48.
September 2019	0.1.0	Pre-stable draft uploaded for ETSI ITS WG1 #49
October 2019	0.2.0	Stable draft uploaded for ETSI drafting meeting of November 5, 2019
December 2019	0.3.0	Updated stable draft uploaded for ETSI drafting meeting of December 16, 2019
January 2020	0.4.0	Final draft submitted to ETSI ITS WG1 #50

DRAFT

History

Document history		
<Version>	<Date>	<Milestone>

DRAFT