ETSI TS 103 724 V2.1.1 (2021-08)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
Facilities layer function;
Interference Management Zone Message (IMZM);
Release 2

Reference

DTS/ITS-001947

Keywords

interoperability, ITS, safety, service, transport

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
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

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

No part may be reproduced 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 2021.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

1 Scope

The present document defines the "Interference Management Zone Message" (IMZM) that is used to identify an interference management area with the aim to optimize the spectrum sharing between road ITS and other services/applications. The objective is to support the dynamic band sharing in co-channel and adjacent channel scenarios between ITS stations and other services and applications.

The message structure will be based on the existing CAM *ProtectedCommunicationZones* structure.

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 302 636-3: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture".

[2] 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".

[3] Recommendation ITU-T X.691/ISO/IEC 8825-2 (1997-12): "Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".

[4] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

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

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

NOTE: This reference is to be replaced by reference to Common Data Dictionary for Release 2 when available.

[7] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

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

[9] ETSI EN 302 636-5-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol".

[10] IEEE 1609.2™: "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages".

2.2 Informative references

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

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

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

[i.1] ETSI TR 103 580: "Urban Rail ITS and Road ITS applications in the 5,9 GHz band; Investigations for the shared use of spectrum".

[i.2] ETSI TR 102 863: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".

[i.3] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.4] ETSI EN 302 636-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.5] ETSI TS 102 894-1: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications".

[i.6] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

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

[i.8] ETSI TS 101 539-2: "Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification".

[i.9] ETSI TS 101 539-3: "Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification".

[i.10] ETSI TS 102 723-5: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 5: Interface between management entity and facilities layer".

[i.11] ETSI TS 102 723-11: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 11: Interface between networking and transport layer and facilities layer".

[i.12] ISO EN 17419: "Intelligent Transport Systems -- Cooperative Systems -- Classification and management of ITS applications in a global context".

[i.13] ETSI EN 302 663 (V1.2.1): "Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.14] ETSI EN 303 613 (V1.1.1): "Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.15] ETSI EN 302 571: "Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU".

[i.16] ETSI TS 102 792: "Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range".

[i.17] EC Implementation Decision EU 2020/1426: "Commission Decision on the harmonised use of radio spectrum in the 5875-5935 MHz frequency band of safety-related applications of Intelligent Transport Systems (ITS) and repealing Decision 2008/671/EC".

[i.18] ECC DEC (08)01: ECC Decision "The harmonised use of the 5875-5935 MHz frequency band for Intelligent Transport Systems (ITS)", approved 14 March 2008, Amended 6 March 2020.

[i.19] ECC Report 101: "Compatibility studies in the band 5855- 5925 MHz between Intelligent Transport Systems (ITS) and other systems, Bern, February 2007".

[i.20] ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.21] FIPS PUB 199: "Standards for Security Categorization of Federal Information and Information Systems".

[i.22] SAE Surface Vehicle Standard J2945/5: "Service Specific Permissions and Security Guidelines for Connected Vehicle Applications".

[i.23] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.24] CEN ISO/TS 19321: "Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures".

[i.25] ETSI TS 103 175: "Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium".

[i.26] SAE J2735 (11-2009): "Dedicated Short Range Communications (DSRC) Message Set Dictionary".

[i.27] ETSI TS 103 301: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services; Release 2".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 302 665 [i.3], ETSI TR 102 863 [i.2], SAE J2735 [i.26] and the following apply:

DMC Toff limit: idle time limit for Decentralized Mitigation Control, using a procedure similar to what is defined in ETSI TS 103 175 [i.25] for DCC

Interference Management Zone (IMZ): geographical area where spectrum can be shared dynamically to enable co-channel and adjacent channel scenarios between ITS stations and other services and applications

Interference Management Zone Message (IMZM): IMZ basic service PDU

Interference Management Zone Message (IMZM) data: partial or complete IMZM payload

ITS-G5: access technology to be used in frequency bands dedicated for European intelligent transport System (ITS)

NOTE: As defined in ETSI EN 302 663 [i.13].

LTE-V2X: access technology to be used in frequency bands dedicated for European intelligent transport System (ITS)

NOTE: As defined in ETSI EN 303 613 [i.14].

V2X: either vehicle to vehicle (V2V), or vehicle to infrastructure (V2I) and/or infrastructure to vehicle (I2V)

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Application Programming Interface
ASN.1	Abstract Syntax Notation 1
BTP	Basic Transport Protocol
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
C-ITS	Cooperative ITS
DCC	Decentralized Congestion Control
DE	Data Element
DF	Data Frame
DMC	Decentralized Mitigation Control
FA-SAP	Facilities/Applications Service Access Point
FL-SDU	Facility-layer Service Data Unit
GN	GeoNetworking
HMI	Human Machine Interface
I2V	Infrastructure-to-Vehicle
IMZ	Interference Management Zone
IMZM	Interference Management Zone Message
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITS-S	ITS Station
LDM	Local Dynamic Map
LTE	Long Term Evolution
MF-SAP	Management/Facilities Service Access Point
MIB	Management Information Base
MSB	Most Significant Bit
N&T	Networking & Transport layer
NF-SAP	Networking & Transport/Facilities Service Access Point
OSI	Open System Interconnection
PCI	Protocol Control Information
PDU	Packet Data Unit
PER	Packed Encoding Rules
POTI	Position and Time management
SAE	Society of Automotive Engineers
SAP	Service Access Point
SF-SAP	Security Facilities - Service Access Point
SHB	Single-Hop Broadcasting
SSP	Service Specific Permissions
UPER	Unaligned Packed Encoding Rules
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-everything

4 Introduction to Interference Management Zone (IMZ) basic service

4.1 Background

Cooperative ITS systems operate in license exempt frequency bands (e.g. 5 855 MHz to 5 925 MHz ETSI EN 302 571 [i.15], 63,72 GHz to 65,88 GHz) and have to share at least part of the spectrum with other co-primary services (for example, Urban Rail systems in the band 5 915 MHz to 5 925 MHz (see ETSI TR 103 580 [i.1]), 5 875 MHz to 5 925 MHz with Fixed Satellite Services (FSS) uplink). The interference impact can be two-fold: from ITS stations to co-primary services or from co-primary service to ITS-S. In the first case, a mitigation action can be required from the ITS-S to protect the co-primary service from being harmed (see next paragraph in clause 4.1). In the second case, the action may be expected from the ITS-S to protect itself or to inform the driver that the ITS-S is subject to an interference zone. In the present document, both types of zones are called interference management zones.

In order to be able to identify geographically limited areas where sharing is required, this geographical information needs to be communicated in a secure manner by a trusted entity using known certificates to the ITS stations intending to operate in these shared bands. Depending on the regulatory status of the services and applications to share with, actions can be taken by ITS stations to mitigate the impact of interference. These actions could be one or a combination of the following:

- Duty Cycle restrictions.
- Power restrictions.
- Switch off or receive only operation.
- Increase transmitter idle time to reduce the channel load (e.g. through DCC Toff limit).
- Change of radio channel / radio band change, e.g. 5,9 GHz to 60 GHz.
- Awareness message to the user (human or machine) providing a clear information that in a given area there might be an issue (no specific mitigation action is required from the ITS-S in this case).

Similar operations can be envisaged for the protection of adjacent band (e.g. CEN DSRC tolling applications in the band 5 795 MHz to 5 815 MHz, see ETSI TS 102 792 [i.16]).

The Interference Management Zone service defined in the present document provides information about interference management zones where band sharing and coexistence are required. This is done through an Interference Management Zone Message (IMZM) which is in addition or substitutive to the CAM from infrastructure devices (see ETSI TS 103 301 [i.27] than the focused information contained in an infrastructure CAM. The message can be transmitted by existing Roadside Equipment (RSE) or by specific RSE managed by either the operator of the system to be protected or by road operators. It could also be transmitted by Onboard Equipment (OBE) as long as it is authorized and in the trusted domain. This may happen, for example, on a train that sends out IMZM when needed, or in an emergency vehicle or portable device of enforcement personnel, which then gets the possibility to provide protection of emergency messages when needed. In summary, the present document proposes a global description of the message that can be used as a toolbox by the relevant organizations to customize the IMZM suited to the interference management and sharing regulation they want to enforce. Accordingly, mitigation requirements specific to identified use cases are out of scope of the present document.

A specific interference management zone is defined locally around a well-defined position and is only valid for a limited time duration. Both depend on the type of interference management zone:

- Geographical extension: the interference management zone should only be taken into account as long as the ITS-S is travelling within the defined zones.
- Time validity of an interference management zone message: the validity can be from a few seconds to unlimited. For example, in the case of a warning to the user such as for interference in the vicinity of satellite stations, the zone is quasi static and always present. But this is only a warning, so no mitigation measures are necessary from the ITS-S, which is reflected in the specifications of the present document (see clause 7).

An RSE or relevant OBE can also send out an IMZM information related to other zones in the area which are not directly linked to its own position. This is similar to the protected zone information specified in the Cooperative Awareness Message (CAM, see ETSI EN 302 637-2 [5]), where there can be up to 16 areas in a single message.

A receiving ITS-S (vehicle or personal ITS-S) should be able to store the information of about up to 32 interference management zones in its memory.

Certification and trust domains: Since an IMZM can limit the performance of the ITS system or even prevent its operation, the operations linked to the IMZM should be authenticated by certificates as specified in ETSI TS 103 097 [4]. The message should be generated by infrastructure operators, using the same policies as other C-ITS messages, e.g. the CAM (see ETSI EN 302 637-2 [5]). The IMZM transmission shall be part of the overall ITS trust domain. The message generation entity can also be part of the potential victims' trust domain, whether this is implemented as a manual or automated integration. In the case of Urban Rail, the information about the needed IMZ would come from the Urban Rail trust domain as encrypted information and be sent out to the ITS-S in the surrounding area using a valid ITS certificate complying with ETSI TS 103 097 [4].

NOTE: Spectrum regulatory matters are out of scope of the present document. The spectrum regulators are to define the zones when the band sharing mechanisms are relevant from the regulatory point of view. For other zones (like potential interference from satellite uplink), the road operators have to define potential warning zones.

4.2 Services provided by IMZ basic service

The IMZ basic service is a Facilities layer entity that operates the IMZM protocol. It provides different services:

- reception of trigger from the application to start the IMZM transmission;
- reception of interference management zone information from the management entity and encoding of that information;
- sending of IMZMs;
- receiving of IMZMs; and
- provision of the decoded information to the relevant entities in the ITS-S, depending on the action to be taken.

The IMZ basic service uses the services provided by the protocol entities of the ITS networking & transport layer to disseminate the IMZM.

4.3 Sending IMZM

Sending of IMZM consists of two activities: generation of IMZMs and transmission of IMZMs.

In IMZM generation, the originating ITS-S shall compose the IMZM, which is then delivered to the ITS networking & transport layer for dissemination.

The IMZM shall be transmitted over one or more communication media using one or more transport and networking protocols.

Security measures such as authentication shall be applied to the IMZM during the transmission process in coordination with the security entity.

4.4 Receiving IMZM

Upon receiving an IMZM, the IMZ basic service shall make the content of the IMZM available to the ITS applications via the MIB of the Management entity and to other facilities within the receiving ITS-S, such as the Local Dynamic Map (LDM) (see specification of the interface in clause 5.3.1). It shall apply all necessary security measures such as relevance or message integrity check in coordination with the security entity.

5 IMZ basic service functional description

5.1 IMZ basic service in the ITS architecture

All authorized ITS-S: authorized roadside ITS-S, authorized vehicle ITS-S and authorized personal ITS-S (for example, an OBE in a train or a portable device in an emergency vehicle), shall be capable of sending IMZMs.

As illustrated in Figure 1, the IMZ basic service shall have the following interfaces:

- the NF-SAP with the Networking & Transport layer (N&T) for the exchange of IMZM messages with other ITS-S;
- the SF-SAP with the Security entity to access security services for IMZM transmission and IMZM reception;
- the FA-SAP with the application layer to receive a transmission trigger from ITS applications;
- the MF-SAP with the management entity to retrieve configuration and profile data, and to provision the received IMZM data.

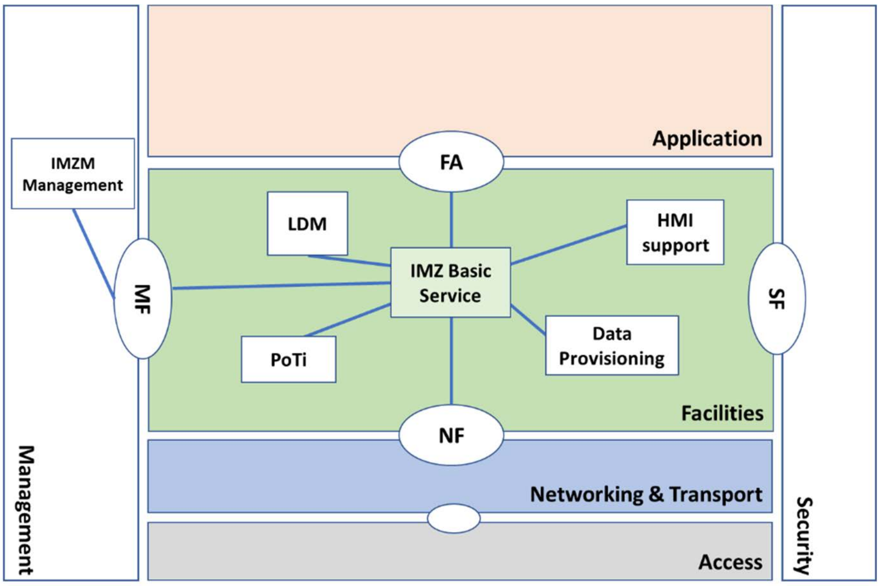

Figure 1: IMZ basic service within the ITS-S architecture

5.2 IMZ basic service functional architecture

The IMZ basic service is part of the Application Support domain of the Facilities Layer according to ETSI TS 102 894-1 [i.5]. Figure 2 shows the functional block diagram with the functional blocks of the IMZ basic service and interfaces to other entities and layers. The IMZ basic service interacts with other Facilities layer functions as represented in Figure 1 through the IF.OFa interface. It also interacts with other entities in the ITS-S through the interfaces defined in ETSI EN 302 665 [i.3]. The interfaces to other entities and layers are specified in clause 5.3.

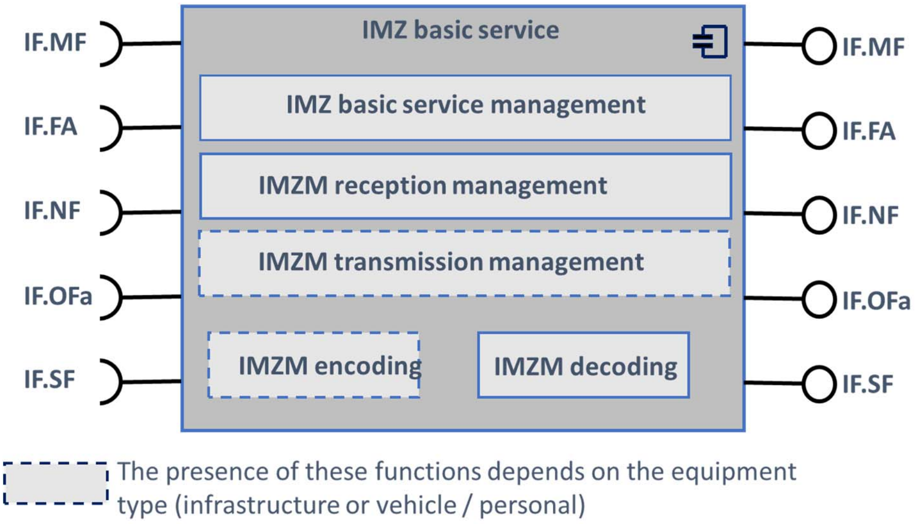
IMZ basic service
IMZ basic service management
IMZM reception management
IMZM transmission management
IMZM encoding
IMZM decoding
IF.MF
IF.FA
IF.NF
IF.OFa
IF.SF
IF.MF
IF.FA
IF.NF
IF.OFa
IF.SF
The presence of these functions depends on the equipment type (infrastructure or vehicle / personal)

Figure 2: Functional block diagram of the IMZ basic service

For sending and receiving IMZMs, the IMZ basic service shall provide the following sub-functions:

- Encode IMZM:
  - This sub-function constructs the IMZM according to the format specified in annex A.
- Decode IMZM:
  - This sub-function decodes the received IMZMs.
- IMZM transmission management:
  - This sub-function implements the IMZM protocol operation of the originating ITS-S, including in particular:
    - Activation and termination of IMZM transmission operation.
    - Determination of the IMZM generation frequency.
    - Triggering of the IMZM generation.
- IMZM reception management:
  - This sub-function implements the IMZM protocol operation of the receiving ITS-S, including in particular:
    - Triggering the "decode IMZM" function at the reception of a IMZM.
    - Provisioning the received IMZM data to LDM or to ITS management entity of the receiving ITS-S (see clause 5.3).
    - Triggering the required mandated mitigation actions in the ITS-S based on the interference management zone type field.
- IMZ basic service management:
  - Store the configuration received at ITS-S initialization time or updated later for the coding of IMZM data elements.

The IF.OFa interface to other facilities and the FA interface to ITS applications are implementation dependent (see clause 5.31 and clause 5.3.2).

5.3 Interfaces of the IMZ basic service

5.3.1 Interface to ITS applications

An ITS application is an application layer entity that implements the logic for fulfilling one or more ITS use cases. For example, ITS Release 1 applications are defined in ETSI TS 101 539-1 [i.7], ETSI TS 101 539-2 [i.8] and ETSI TS 101 539-3 [i.9].

ITS applications can provide the trigger to transmit IMZM.

For the provision of received data, the IMZ basic service provides the interface IF.OFa to LDM or the MF interface to ITS management entity, as illustrated in Figure 2 (indirect interaction). The purpose of the LDM is defined in ETSI TR 102 863 [i.2].

NOTE: The interface to the ITS application layer may be implemented as an API and data are exchanged between the IMZ basic service and ITS applications via this API. In another possible implementation, the interface to the application layer may be implemented as FA-SAP. Specifications of the FA-SAP and the corresponding protocols and APIs are out of scope of the present document.

5.3.2 Interface to data provisioning facilities

For the generation of IMZMs, the IMZ basic service interacts with other facilities layer entities in order to obtain the required data. This set of facilities that provides data for IMZM generation is referred to as data provisioning facilities. Data are exchanged between the data provisioning facilities and the IMZ basic service via the interface IF.OFa, defined in Figure 2.

NOTE: Specifications of the interface to the data provisioning facilities and the corresponding protocols are out of scope of the present document.

5.3.3 Interface to the networking & transport layer

The IMZ basic service exchanges information with ITS networking & transport layer via the interface IF.NF (Figure 2). A specification of the interface IF.NF as NF-SAP (Figure 1) is provided in ETSI TS 102 723-11 [i.11].

At the originating ITS-S, the IMZ basic service shall provide the IMZM embedded in a Facility-Layer Service Data Unit (FL-SDU) together with Protocol Control Information (PCI) to the ITS networking & transport layer, according to ETSI EN 302 636-5-1 [9]. At the receiving ITS-S, the ITS networking & transport layer will pass the received IMZM to the IMZ basic service, if available.

The data set that shall be passed between IMZ basic service and ITS networking & transport layer for the originating and receiving ITS-S is specified in Table 1.

Table 1: Data passed between CA basic service and the ITS networking & transport layer

Category	Data	Data requirement	Mandatory/Optional
Data passed from the IMZ basic service to the ITS networking & transport layer	IMZM	*{imzm}* as specified in annex A	Mandatory
	PCI	Depending on the protocol stack applied in the networking & transport layer as specified in clause 5.3.4	Mandatory
Data passed from the ITS networking & transport layer to the IMZ basic service	Received IMZM	*{imzm}* as specified in annex A	Mandatory

The interface between the IMZ basic service and the networking & transport layer relies on the services of the GeoNetworking/BTP stack as specified in clause 5.3.4.1 or on the IPv6 stack and the combined IPv6/GeoNetworking stack as specified in clause 5.3.4.2.

5.3.4 Interfaces to the protocol stacks of the networking & transport layer

5.3.4.1 Interface to the GeoNetworking/BTP stack

A IMZM may rely on the services provided by the GeoNetworking/BTP stack. If this stack is used, the GN packet transport type Single-Hop Broadcasting (SHB) shall be used. In this scenario, only nodes in direct communication range may receive the IMZM.

PCI being passed from IMZ basic service to the GeoNetworking/BTP stack shall comply with Table 1 and Table 2.

Table 2: PCI from IMZ basic service to GeoNetworking/BTP at the originating ITS-S

Category	Data	Data requirement	Mandatory/Conditional
Data passed from the IMZ basic service to GeoNetworking/BTP	BTP type	BTP header type B (ETSI EN 302 636-5-1 [9], clause 7.3.2)	Conditional The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	Destination port	As specified in ETSI EN 302 636-5-1 [9] (see note 1)	Conditional The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	Destination port info	As specified in ETSI EN 302 636-5-1 [9]	Conditional The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	GN Packet transport type	GeoNetworking SHB	Conditional The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	GN Communication profile	Unspecified, ITS-G5 [i.13], or LTE-V2X [i.14]	Conditional The data shall be passed if the value is not provided by the ITS-S configuration, e.g. defined in a Management Information Base (MIB) or if the value is different from the default value as set in the MIB.
	GN Security profile	SECURED (see note 2)	Mandatory

Category	Data	Data requirement	Mandatory/Conditional
	GN Traffic Class	As defined in ETSI EN 302 636-4-1 [i.4]	Mandatory
	GN Maximum packet lifetime	Shall not exceed 5 000 ms (equal to maximum generation period, see clause 6.1.3)	Mandatory
	Length	Length of the IMZM	Mandatory
NOTE 1: When a global registration authority for ITS application as specified in ISO EN 17419 [i.12] is operational, the BTP destination port registered with this authority shall be used. NOTE 2: The IMZM message shall always use the SECURED option of the security profile.			

5.3.4.2 Interface to the IPv6 stack and the combined IPv6/GeoNetworking stack

A IMZM may use the IPv6 stack (and possibly GeoNetworking over IPv6) or the combined IPv6/GeoNetworking stack for IMZM dissemination as specified in ETSI EN 302 636-3 [1].

NOTE: When the IMZM dissemination makes use of the combined IPv6/GeoNetworking stack, the interface between the IMZ basic service and the combined IPv6/GeoNetworking stack may be identical to the interface between the IMZ basic service and IPv6 stack. The transmission of IMZM over the IPv6 stack is out of scope of the present document.

5.3.5 Interface to the Management entity

The IMZ basic service may exchange primitives with the management entity of the ITS-S via the MF-SAP interface (Figure 1).

At receiving ITS-S and when relevant, the IMZ basic service may transfer the received mitigation information to the Management entity. In the case of the ITS-G5 access layer, the IMZ basic service may provide control information for the DMC operation to the management entity. The Decentralized Mitigation Control (DMC) operates with a procedure similar to what is defined in ETSI TS 103 175 [i.25] for the DCC. The parameters contained in the mitigation information are specified in clause 7.5, Table 7.

Interactions with the management entity are provided via the IF.MF interface (see Figure 2).

NOTE 1: A specification of the MF-SAP and a list of primitives exchanged with the management layer are provided in ETSI TS 102 723-5 [i.10].

NOTE 2: Specifications of the MF-SAP and the corresponding protocol are out of scope of the present document.

5.3.6 Interface to the Security entity

The IMZ basic service may exchange primitives with the Security entity of the ITS-S via the SF-SAP interface (Figure 1) using the IF.SF interface provided by the Security entity (Figure 2).

The IMZ basic service shall align with the CA basic service to determine whether to subscribe or not to the identity change service provided by the security entity as specified in ETSI TS 102 731 [8], depending on the originating ITS-S type and to determine whether it should implement message signature in the IMZ basic service.

NOTE: Specifications of the SF-SAP and the corresponding protocol are out of the scope of the present document.

6 IMZM dissemination

6.1 IMZM dissemination concept

6.1.1 IMZM dissemination requirements

Point-to-multipoint communication, specified in ETSI EN 302 636-3 [1], shall be used for transmitting IMZMs. The IMZM shall be transmitted only from the originating ITS-S in a single hop to the receiving ITS-Ss located in the direct communication range of the originating ITS-S. As specified for the interface to the protocol stacks of the N&T layer in clause 5.3.3, a received IMZM shall not be forwarded to other ITS-Ss.

6.1.2 IMZ basic service activation and termination

For vehicle and personal ITS-S, the IMZ basic service shall be activated with the ITS-S activation of the platform hosting the facilities layer (e.g. swich ON the ITS-S). The IMZ basic service shall be terminated when the ITS-S is deactivated.

6.1.3 IMZM generation frequency management

The IMZM generation frequency is managed by the IMZ basic service. The time interval between two consecutive IMZM generations shall be greater than or equal to *T_genImzmMin* [1 000 ms] and shall not be superior to *T_genImzmMax* [5 000 ms]. This corresponds to an IMZM generation rate of 0,2 Hz to 1 Hz.

6.1.4 IMZM generation time requirement

In order to ensure proper interpretation of received IMZMs, each IMZM shall be time-stamped.

The time required for generating an IMZM shall be less than 50 ms. The time required for generating an IMZM refers to the time difference between the time at which an IMZM generation is triggered and the time at which the IMZM is delivered to networking & transport layer.

6.1.5 IMZM triggering conditions

As long as the IMZ basic service is active in infrastructure ITS-S, the IMZM generation shall be triggered and managed by the IMZ basic service or by a relevant application.

The IMZM generation can be triggered in different ways, as set in the IMZM configuration:

- Continuous generation, e.g. continuous generation and thus protection of the potential victim in the interference management zone.
- Time window triggered generation, e.g. continuous generation during specific time slots.
- Application triggered generation, e.g. based on the reception of a secure triggering signal from the victim system to be protected (e.g. Urban Rail signal).

Depending on the triggering operation used, different levels of interference management can be assumed. For an optimized use of the spectrum resources, a limited time window of operation would be beneficial.

6.2 IMZM dissemination constraints

6.2.1 Security constraints

6.2.1.1 Introduction

A security analysis of IMZ use cases is provided in annex B.

IMZMs that are transmitted over links that cannot be fully trusted (see clause 7 of ETSI TS 102 941 [i.6]), such as radio links, shall be signed using ITS certificates as specified in ETSI TS 103 097 [4]. In particular, IMZM that are transmitted over BTP with the GeoNetworking protocol shall be signed at the GeoNetworking layer.

In general, within the Authorization Ticket, the permissions and privileges are indicated by a pair of identifiers, the Intelligent Transportations Systems Application Identifier (ITS-AID) and the Service Specific Permissions (SSP). The ITS-AID, as specified in ETSI TS 102 965 [7], shall indicate the application for which permissions are being granted. The SSP is a field that indicates specific sets of permissions, corresponding to roles and privileges, within the overall permissions indicated by the ITS-AID.

IMZM shall be identified with the ITS-AID specified in ETSI TS 102 965 [7] for the Interference Management Zone Service.

6.2.1.2 Authorization Ticket requirements and Service Specific Permissions (SSP)

The Authorization Ticket that is contained in the component signer of SignedData shall have the component appPermissions of type SequenceOfPsidSsp containing the ITS-AID and SSPs for the Interference Management Zone Service.

The SSP shall be a BitmapSsp as specified in ETSI TS 103 097 [4].

The SSP for the IMZM is defined by a variable number of octets and shall correspond to the octet scheme of Table 3. For each octet, the Most Significant Bit (MSB) shall be the leftmost bit. The transmission order shall always be the MSB first. The interpretation of the SSP octet scheme is defined as depicted in Figure 3.

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="8">Octet 0</td><td colspan="8">Octet 1</td><td>…</td><td colspan="8">Octet 9</td></tr>
</table>

Figure 3: Format for the Octets

Table 3: Octet Scheme for IMZM SSPs

<table>
<tr><th>Octet #</th><th>Component</th><th>Value</th></tr>
<tr><td>0</td><td>SSP version control</td><td>1</td></tr>
<tr><td>1 to 3</td><td>jurisdictionId</td><td>Identification of entity that rules the jurisdiction for which the IMZM is sent out and which defines the value of DutyCycleSecurityThreshold, powerSecurityThreshold and dmcSecurityThreshold.
jurisdictionId is of type Provider from CEN ISO/TS 19321 [i.24], coded in ASN.1 UPER</td></tr>
<tr><td>4 to 8</td><td>InterferenceManagement ZoneChannel</td><td>InterferenceManagementZoneChannel shall have three components and be coded in UPER as a sequence of three integers:
<table>
<tr><th>Parameter</th><th>Description</th><th>INTEGER Range</th></tr>
<tr><td>centreFrequency</td><td>centre frequency of the channel to be managed.</td><td>1 .. 99 999 (in units of 10^{exp+2} Hz)</td></tr>
<tr><td>channelWidth</td><td>width of the channel to be managed.</td><td>1 .. 9 999 (in units of 10^{exp} Hz)</td></tr>
<tr><td>exponent</td><td>exponent of the power of 10.</td><td>0..15</td></tr>
</table></td></tr>
<tr><td>9</td><td>Service-specific parameter</td><td>see Table 4.</td></tr>
</table>

The Service-specific parameter shall be as defined in Table 4.

Table 4: IMZ service SSPs

Octet Position	Bit Position	IMZM data Item	Bit Value
4	0 (80h) (MSBit)	Broadcast of lowDutyCycle < DutyCycleSecurityThreshold Broadcast of powerReduction < powerSecurityThreshold Broadcast of dmcToffLimit < dmcSecurityThreshold	1: The sending ITS-S is authorized 0: The sending ITS-S is not authorized
4	1 (40h)	Broadcast of lowDutyCycle ≥ DutyCycleSecurityThreshold Broadcast of powerReduction ≥ powerSecurityThreshold Broadcast of dmcToffLimit ≥ dmcSecurityThreshold	1: The sending ITS-S is authorized 0: The sending ITS-S is not authorized
NOTE: All other bits of the SSP are not used and set to 0.			

NOTE: The use of a BitmapSsp allows for the SSP to be extended in the future without the need to increase the SSP version number.

The Authorization Ticket shall also contain the component region of type GeographicRegion as defined in IEEE 1609.2 [10] describing a region in which the interference management zone defined in the IMZM component *zoneDefinition* shall be located.

6.2.1.3 Message security requirements

The Authorization Ticket associated to the private key used to sign the IMZM shall be attached to every IMZM, in the component signer of SignedData.

The generic security profile as defined in ETSI TS 103 097 [4] shall be applied. Additional HeaderField types are not allowed.

6.2.2 General priority constraints

The priority constraint is given by the Traffic Class as specified in ETSI EN 302 636-4-1 [i.4].

7 IMZM Format Specification

7.1 General Structure of a IMZM PDU

An IMZM is composed of:

- a common ITS PDU header;
- a generation delta time;
- a basic container;
- an IMZM container;
- The IMZM is extensible, but no extensions are defined in the present document.

An illustration of the IMZM structure is provided in Figure 4. Detailed data presentation rules shall be as specified in annex A.

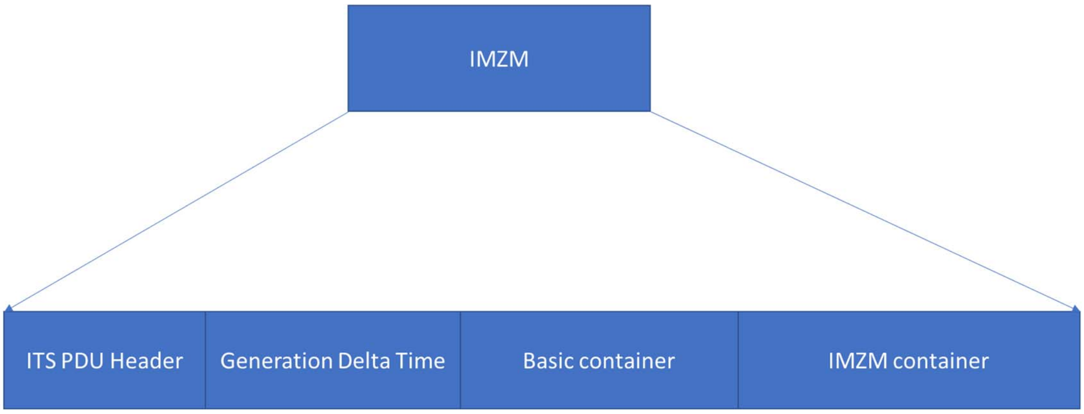

Figure 4: General structure of an IMZM

7.2 ITS PDU header

The ITS PDU header shall be as specified in ETSI TS 102 894-2 [2]. Detailed data presentation rules of the ITS PDU header in the context of IMZM shall be as specified in annex A.

7.3 Generation Delta Time

The generation time in the IMZM shall be a GenerationDeltaTime as used in ETSI EN 302 637-2 [5] for the CAM. This is a measure of the number of milliseconds elapsed since the ITS epoch, modulo 2^{16} (i.e. 65 536).

7.4 Basic container

The basic container provides basic information of the originating ITS-S:

- type of the originating ITS-S (e.g. roadSideUnit(15));
- the latest geographic position of the originating ITS-S as obtained by the IMZ basic service at the IMZM generation.

The basic container shall be present in each IMZM generated by ITS-Ss implementing the IMZ basic service.

Detailed data presentation rules of the basic container shall be as specified in annex A.

7.5 IMZM container

IMZM generated by infrastructure ITS-S shall include the IMZM container. The IMZM container shall include a sequence of interference management communication zones, as specified in annex A.

For each interference management communication zone (*DF_InterferenceManagementZone*), it shall contain a sequence of the zone definition (*DF_ZoneDefinition*) together with the interference management information (*DF_InterferenceManagementInfo*). The *DF_InterferenceManagementInfo* itself is further split per affected channel (*DF_InterferenceManagementInfoPerChannel)*. These DFs shall be presented as specified in annex A.

Detailed setting rules are provided below:

- The *DF_InterferenceManagementInfoPerChannel* is designed using the *DF_ProtectedCommunicationZone* in ETSI TS 102 894-2 [2] as a reference, but with additional parameters, as listed in annex A.
- The *DF_InterferenceManagementChannel* indicates which shared frequency channel should be managed in the zone. The value of *DF_InterferenceManagementChannel* is set as in Table 5 (and identical to the setting in Table 4).

Table 5: Frequency channel of the interference management communication zone

Name	Parameter	Description	Range
DF_InterferenceManagementChannel	centreFrequency	centre frequency of the channel to be managed	1 .. 99 999 (in units of 10^{exp+2} Hz)
	channelWidth	width of the channel to be managed	1 .. 9 999 (in units of 10^{exp} Hz)
	Exponent	Exponent of the power of 10	0..15

- The *DE_InterferenceManagementZoneType* is extended from ETSI TS 102 894-2 [2] to cover additional applications. This type could be e.g. a tolling zone (permanent or temporary, as defined in ETSI TS 102 792 [i.16]), an Urban Rail protected zone or a Fixed satellite interference management zone. Other types could be added depending on the regulatory needs or interference management needs. The value of *DE_InterferenceManagementZoneType* is set as in Table 6.

  Depending on the type of the zone, there would be different regulatory obligations:

  - **urbanRail:** sharing requirements as defined in EC DEC 2020/1426 [i.17] and ECC DEC (08)01 [i.18].
  - **satelliteStation:** warning of potential interference towards ITS systems as identified in ECC report 101 [i.19] from satellite earth-to-space transmissions.
  - **fixedLinks:** potential sharing requirements when operating ITS applications in fixed service bands, e.g. Urban Rail ITS in the band 5 925 MHz to 5 935 MHz, see ECC decision (08)01 [i.18].

Table 6: Type of interference management communication zones

Name	Value	Description
DE_InterferenceManagementZoneType	0	permanentCenDsrcTolling
	1	temporaryCenDsrcTolling
	2	unavailable
	3	urbanRail
	4	satelliteStation
	5	fixedLinks

NOTE 1: The field *DE_InterferenceManagementZoneType* has been harmonised with the field *ProtectedCommunicationZone* in the CDD (ETSI TS 102 894-2 [2]), which can take the following values: permanentCenDsrcTolling(0), temporaryCenDsrcTolling(1). Both DEs may be merged when Common Data Dictionary for Release 2 is available.

NOTE 2: This field could be useful for plausibility check at reception side together with the SSP analysis.

- The *DF_InterferenceManagementMitigationType* is defined in Table 7 as a flexible set of parameters that allows to specify with a fine granularity the necessary mitigation to be activated. As mitigation actions may be different according to the access layer technology, it allows to have several sub-containers, one for each technology.

- The content of the DF may be set to unavailable (see Table 7 below) or contain one or more sub-container (as *DF_MitigationForTechnologies*) specifying the information and commands that the receiving ITS-S shall use in the defined interference management zone to protect the potential victim. As mitigation may be different for the access layer technologies, a sub-container (of type *DF_MitigationPerTechnologyClass*) is defined for each access layer technology class. Each of the sub-container includes the parameters defined in Table 8. They shall be presented as specified in annex A.

Table 7: Type of IMZ mitigations

Name	Choice values	Description
DF_InterferenceManagementMitigationType	unavailable	Mitigation type to use unavailable (default). It means that no mitigation technique is necessary, for example in the case where only a warning is presented to the user.
	mitigationForTechnologies	Sequence of sub-containers, one per relevant access layer technology class (DF_MitigationPerTechnologyClass).

Table 8: IMZ mitigation sub-container per channel access technology class

Name	Parameter	Description	Range
DF_MitigationPerTechnologyClass	accessTechnologyClass	Channel access technology in which this mitigation is applied.	See values in Table 9
	lowDutyCycle	Reduction of duty cycle from normal mode, optional.	0 .. 10 000, in 0,01 % steps
	powerReduction	Transmit power reduction from normal mode, (parameter defined in ETSI TS 102 792 [i.16]), optional.	0 .. 30, in dB
	dmcToffLimit	Idle time limit, as defined in ETSI TS 103 175 [i.25] for DCC, optional.	0 .. 1 200, in ms
	dmcTonLimit	Transmission duration limit, as defined in ETSI EN 302 571 [i.15], optional.	0 .. 20, in ms

The presence of the different parameters depends on the mitigation to be applied (see Table 9).

Table 9 indicates the channel access technology classes under consideration in the present document as well as the parameters that shall be included in the *DF_MitigationPerTechnologyClass* sub-container. The letter in the table indicates the condition for the parameter inclusion: C for conditional optional (i.e. at least ONE of the parameters marked with C shall be present if the corresponding *accessTechnologyClass* is present in the message).

"dmcToffLimit: M" means that if *dmcToffLimit* is present, then *dmcTonLimit* shall be mandatory.

This table may be extended with additional access technologies as they become relevant.

Table 9: Parameters per channel access technology class

Parameter	any	ITS-G5 Class (see ETSI EN 302 663 [i.13])	LTE-V2X Class (see ETSI EN 303 613 [i.14])	NR-V2XClass
accessTechnologyClass	0	1	2	3
lowDutyCycle	C	C	C	C
powerReduction	C	C	C	C
dmcToffLimit		C		
dmcTonLimit		dmcToffLimit: M		
NOTE: When the *accessTechnologyClass* is equal to 0, it means that the selected parameters apply to all the channel access technology classes transmitting in the selected geographical area and in the selected channel.				

- The *DE_expiryTime* indicates the time at which the validity of the interference mitigation zone will expire when this zone is temporarily valid. It shall be presented as specified in annex A.
- Inside the *DF_ZoneDefinition*, the *DF_Interference ManagementZoneShape* defines the bounding box of the interference management zone. It shall be presented as specified in annex A.

7.6 IMZM format and coding rules

7.6.1 Common data dictionary

The IMZM format shall make use of the common data dictionary as defined in ETSI TS 102 894-2 [2]. Where relevant, it shall also make use of additional DEs and DFs defined in ETSI EN 302 637-2 [5] and ETSI TS 103 300-3 [6].

Where applicable, DEs and DFs that are not defined in the present document shall be imported from the common data dictionary as specified in ETSI TS 102 894-2 [2].

NOTE: Detailed descriptions of all new DEs and DFs in the context of IMZM are presented in the comments associated to the specification in annex A of the present document.

7.6.2 IMZM data presentation

The IMZM format is presented in ASN.1. Unaligned Packed Encoding Rules (UPER) as defined in Recommendation ITU-T X.691/ISO/IEC 8825-2 [3] shall be used for IMZM encoding and decoding.

The ASN.1 representation of IMZM shall be as specified in the annex A of the present document.

Annex A (normative): ASN.1 specification of IMZM

This annex provides the ASN.1 specification of the IMZM.

The ASN.1 module specified in the present document is available at the following URL:

- https://forge.etsi.org/rep/ITS/asn1/imzm_ts103724/blob/v2.1.1/IMZM-PDU-Descriptions.asn

Its SHA256 sum is 82fe09b47a91d65ea14ff52e2d0c97ce092d957b36982ea25d7acf416ed8f5a5.

Annex B (informative): Security analysis of IMZ use cases

B.1 Introduction

This annex presents the security analysis of the IMZM use cases corresponding to the background presentation in clause 4.1.

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/IEC 27001 [i.20] and Federal Information Processing Standard (FIPS) 199 [i.21]:

- 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.

NOTE: 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 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" (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" (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.

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 performed in the present document does not reflect this potential scalability and focuses on messages used to raise warnings to human drivers. The assumption 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 the present 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 should 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.22].

Separately, the security analysis for the information flows 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.23] 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.

B.2 Use Case: Frequency band interference management in a dedicated geographical zone

Table B.1: Risk analysis: Use Case: Frequency band interference management in a dedicated geographical zone

Use case: Frequency band interference management in a dedicated geographical zone (e.g. for Urban rail or CEN DSRC systems)			
Actors: R-ITS-S, V-ITS-S (Road Vehicle), Urban Rail Vehicle, RLAN system			
Information flow	**Entity activities**	**Description**	**Impact**
IMZM	R-ITS-S → Road Vehicle	Broadcast of IMZM with mitigation parameters lower than security thresholds.	C: None - broadcast model. I: Low - false IMZM does not prevent C-ITS communication. A: Low - Unavailability of IMZM does not impact C-ITS
	R-ITS-S → Road Vehicle	Broadcast of IMZM with mitigation parameters higher than or equal to security thresholds.	C: None - broadcast model. I: medium - false IMZM may completely prevent C-ITS communication. A: Low - Unavailability of IMZM does not impact C-ITS
	Urban Rail Vehicle → Road Vehicle	Broadcast of IMZM with mitigation parameters lower than security thresholds.	C: None - broadcast model. I: Low - false IMZM does not prevent C-ITS communication. A: Low - Unavailability of IMZM does not impact C-ITS
	Urban Rail Vehicle → Road Vehicle	Broadcast of IMZM with mitigation parameters higher than or equal to security thresholds.	C: None - broadcast model. I: medium - false IMZM may completely prevent C-ITS communication. A: Low - Unavailability of IMZM does not impact C-ITS

<table>
<tr><td colspan="4">Use case: Frequency band interference management in a dedicated geographical zone (e.g. for Urban rail or CEN DSRC systems)</td></tr>
<tr><td colspan="4">Actors: R-ITS-S, V-ITS-S (Road Vehicle), Urban Rail Vehicle, RLAN system</td></tr>
<tr><th>Information flow</th><th>Entity activities</th><th>Description</th><th>Impact</th></tr>
<tr><td></td><td>Roadside → RLAN System</td><td>Broadcast of IMZM with any mitigation parameters value.</td><td>C: None - broadcast model.
I: Low - false IMZM may impact entertainment use cases.
A: Low - Unavailability of IMZM does not impact RLAN</td></tr>
</table>

History

Document history		
V2.1.1	August 2021	Publication