FINAL DRAFT

INTERNATIONAL STANDARD

ISO/FDIS 23132

ISO/TC **22**/SC **31**

Secretariat: DIN

Voting begins on:
2020-04-21

Voting terminates on:
2020-06-16

Road vehicles — Extended Vehicle (ExVe) time critical applications — General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)

Véhicules routiers — Applications temps critiques du véhicule étendu (ExVe) — Exigences générales, définitions et méthodologie de classification des situations sous contrainte de temps liées à la sécurité routière et à la sûreté du véhicule étendu (RExVeS)

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/FDIS 23132:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Preventing death and serious injury in road traffic crashes is a global priority. With the advent of vehicular data communications, road vehicles become connected vehicles, and safety is one of the key issues in the development of such road vehicles. ISO 26262-1 defines the vehicle safety as the absence of unreasonable risks that arise from malfunctions of the E/E system. The absence of unreasonable risk due to these potentially hazardous behaviours related to specific limitations (identified in ISO/PAS 21448[7]) is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

This document defines a complementary methodology for the prioritization of safety-related external communication use-cases to help to design extended vehicle time-critical interfaces described in the ISO 20077-1.

NOTE 1 ISO 20077-1 defines the concepts and terms related to the extended vehicle (ExVe), whereas ISO 20077-2 specifies general rules and basic principles that the manufacturer of the ExVe considers when elaborating its own design method.

NOTE 2 ISO 20077-1 defines an "extended vehicle" (ExVe) as an "entity, still in accordance with the specifications of the vehicle manufacturer, that extends beyond the physical boundaries of the road vehicle and consists of the road vehicle, off-board systems, external interfaces, and the data communication between the road vehicle and the off-board systems". Road vehicles without off-board systems and road vehicles equipped with telematics units are extended vehicles.

Recent developments in the field of connected vehicles, in various parts of the world, bring hope of being able to improve road safety, e.g. by reducing the number of road fatalities through collision avoidance cooperation. Connected vehicles taking into account ISO 20077-1 and ISO 20077-2 take their part in this global effort.

Due to the limited per design embedded resources, a priority management is necessary to apply these resources to the function and request with the highest criticality.

For these connected vehicles, the use of the "ExVe time critical interfaces" is firstly associated with safety-critical functions (e.g. emergency braking, steering) that are functions for which the priorities are based on a criticality concept.

It is important that all the functions using the "ExVe time critical interfaces" take into account the capabilities of the vehicles in which they are installed.

During the design phase, the connected vehicle behaviour regarding all safety-critical situations and its interactions with the external environment should be defined. Its implementation can be based on the methodology proposed in this document.

Road vehicles — Extended Vehicle (ExVe) time critical applications — General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)

1 Scope

This document defines the classification methodology of time-constrained situations and their requirements, that are to be addressed by the “ExVe time critical interfaces" described in ISO 20077-1. Time-constrained situations include safety-critical situations.

It is important for the design of the vehicle to have priority management of "ExVe time critical interface" resources in order to comply with time constrained situations requirements.

The methodology provides a classification, which determines application priorities for optimal vehicle resource allocation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 20077-1, *Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information*

ISO 20077-2, *Road Vehicles — Extended vehicle (ExVe) methodology — Part 2: Methodology for designing the extended vehicle*

ISO 26262-1, *Road vehicles — Functional safety — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 20077-1, ISO 20077-2, ISO 26262-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
road and ExVe safety
RExVeS
set of means (e.g. use cases), conditions and requirements to be considered by the “ExVe time-critical interfaces” described in ISO 20077-1, including time-constrained and *safety-critical situations* (3.4)

Note 1 to entry: The intent is to minimise risk of harm (as described in ISO 26262-1) in road safety-related situations.

Note 2 to entry: In the context of RExVeS, a use case is a set of *scenarios* (3.2) that have a common goal.

3.2
scenario
<RExVeS> sequence of *connected vehicle* (3.11) actions, events, reactions, and interactions, in a road safety setting

3.3
time-constrained situation
<RExVeS> combination of a road safety-related *connected vehicle* (3.11) *scenario* (3.2) and RExVeS-related time constraints, in which lack of communication capability or excessive (communication) latency can lead to malfunctions or other injurious consequences

3.4
safety-critical situation
<RExVeS> combination of a road safety-related *connected vehicle* (3.11) *scenario* (3.2) and an unacceptable risk of harm

3.5
situation priority class
<RExVeS> one of six situation priority classes (P1, P2, P3, P4, P5 or P6) determined according to the severity, the probability of exposure, and the controllability associated with an evaluated *time-constrained situation* (3.3)

3.6
safety-critical situation priority class
<RExVeS> one of the four *situation priority classes* (3.5) (P3, P4, P5 or P6) determined according to the severity, the probability of exposure, and the controllability associated with an evaluated *safety-critical situation* (3.4)

3.7
time-constrained safety-related function
<RExVeS> function under strict time constraints that contributes to the achievement of safety objectives

EXAMPLE "CAM generation" (see ETSI EN 302 637-2[1]) and "BSM generation" (see SAE J2735[2]and SAE J2945[3]). "DENM generation" (see ETSI EN 302 637-3[4]) is another example of time-constrained safety-related function.

3.8
peri-vehicular
<RExVeS> near or around a vehicle

3.9
peri-vehicular data communication
<RExVeS> vehicular data communications in the geographic vicinity of a vehicle

3.10
safety-critical situation reaction time interval
<RExVeS> time-interval from the detection of a *safety-critical situation* (3.4) to the broadcast to neighbouring road users at risk of an appropriate safety-critical message via *time-constrained safety-related functions* (3.7) and *peri-vehicular data communications* (3.9)

3.11
connected vehicle
<RExVeS> road vehicle using *peri-vehicular data communications* (3.9)

4 Symbols and abbreviated terms

ADAS	Advanced Driver-Assistance Systems
BSM	Basic Safety Message
CAM	Cooperative Awareness Message
DENM	Decentralized Environmental Notification Message
ExVe	Extended Vehicle
RExVeS	Road and ExVe safety
TAI	International Atomic Time
UTC	Coordinated Universal Time

5 Conventions and guidelines for specifying RExVeS-related requirements

In this document, requirements are formalized as follow:

REQ	*Number*	**RExVeS** – *Name*
Description		

“Number” represents the individual requirement number.

“Name” is the name of requirement, if needed.

“Description” is the requirement itself.

Requirements in this document are generic and technology agnostic. No actual testing is to be done against them, but they should be used as a guide to define the technology-dependent requirements.

Some technology-dependent requirements may not enable to address all priority classes of RExVeS-related time-constrained situations (see 6.3.5).

Unless otherwise stated, the requirements in this document apply to all priority classes.

6 The RExVeS methodology

6.1 General

The RExVeS methodology brings forward means to identify and classify time-constrained situations (safety-critical or not) that are addressed by the “ExVe time critical interfaces” described in ISO 20077-1. The methodology provides an automotive-specific risk-based approach to determine the priority class of a RExVeS-related time-constrained situation. It is adapted from ISO 26262-3[5] hazard analysis and risk assessment (HARA) and enriched with systems-theoretic process analysis (STPA) insights. The major difference is that in ISO 26262-3[5], the results of the analysis are ASILs while in this document the results are time-constrained situation priority classes.

NOTE 1 The appropriate use of the RExVeS methodology is intended to fulfil RExVeS-related requirements and a set of connected vehicle design prerequisites (see Clause 7).

NOTE 2 Unless otherwise stated, in this document, connected vehicle means connected vehicle taking into account ISO 20077-1 and ISO 20077-2.

The RExVeS methodology starts with the analysis of road safety-related connected vehicle scenarios in which time-constrained situations (safety-critical or not) may occur. Then, a systematic evaluation

of each identified time-constrained situation is performed to determine the RExVeS-related situation priority class to which it pertains. The RExVeS-related situation priority class is determined by considering severity, probability of exposure and controllability criteria.

Figure 1 provides an example of use of the RExVeS methodology in the context of the ExVe design methodology.

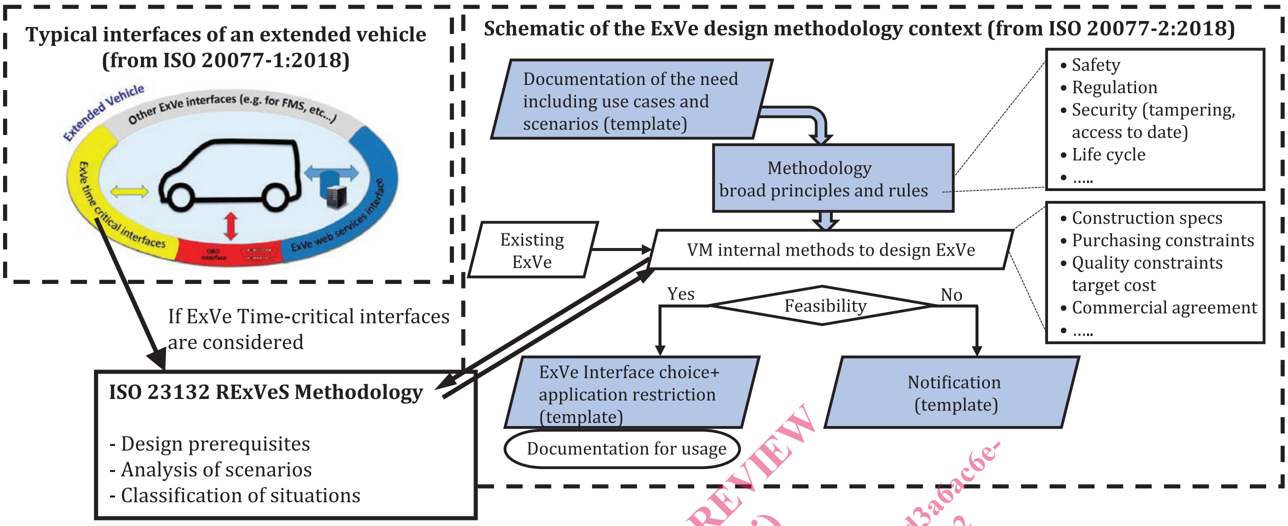

Figure 1 — The RExVeS methodology in the ExVe design methodology context (example)

The RExVeS methodology complements ISO 20077-1 and ISO 20077-2 guidelines for the design of an extended vehicle, from which a vehicle manufacturer can derive its own methods and procedures to design an extended vehicle that addresses a specific set of use cases and scenarios. These methods and procedures remain part of the know-how of each vehicle manufacturer.

According to ISO 20077-2, any ExVe functionality request is described through use cases and scenarios (see ISO 20077-2 template for technical request), in order to support a precise description of the need. Detailed descriptions of relevant RExVeS-related scenarios are important in this respect.

According to ISO 20077-2, for a given use case and scenario, the ExVe manufacturer is responsible for defining the appropriate extended vehicle's interfaces for the considered functionality (see ISO 20077-2). When an ExVe time critical interface is considered, the identified time-constrained situations can be analysed with the RExVeS methodology. As a result, the criticality of the situations is evaluated (severity, probability of exposure, controllability) and, along with any applicable regulations, it gives an indication of relevance and priority to the vehicle manufacturer considering the development of the functionality with an ExVe time-critical interface.

NOTE 3 As RExVeS-related scenarios with safety-critical situations give the biggest causes for concern, they are considered first in the methodology description and dealt with in more detail.

6.2 Analysis of RExVeS-related scenarios

Complex and dynamic processes and interactions are often involved in road accidents. RExVeS-related safety-critical situations may occur when processes or interactions do not meet safety objectives, e.g. because appropriate objectives have not been selected.

The goal of the analysis of RExVeS-related scenarios is to identify time-constrained situations (safety-critical or not) that are to be addressed by the “ExVe time critical interfaces” described in ISO 20077-1. This requires accumulating information about how such situations can occur.

A RExVeS-related time-constrained situation is a combination of a road safety-related connected vehicle scenario and RExVeS-related time constraints, in which a lack of communication capability or excessive

(communication) latency can lead to malfunctions or other injurious consequences. In a RExVeS-related safety-critical situation, there is additionally an unacceptable risk of harm.

NOTE 1 There is not necessarily an unacceptable risk of harm in all time-constrained situations.

Rapidly changing environments where there is a potential for safety-critical situations are examples of RExVeS-related scenarios. "Imminent collision" is a characteristic of many RExVeS-related problematic scenarios. "Loss of vehicle control" is a less recurring one, but it is important to take it into account.

An imminent front collision with another vehicle at high speed on a country road is an example of a RExVeS-related safety-critical situation.

Even when the vehicle is stationary, a RExVeS-related safety-critical situation can be present if it is stopped in an unsafe location.

RExVeS-related use cases and scenarios where safety-critical situations can happen, and where a worst-case set of environmental conditions may lead to "loss of vehicle control" or "imminent collision", should be analysed before taking action.

NOTE 2 RExVeS-related use cases encompass all connected vehicle use cases (including cooperative collision avoidance use cases) where at least one RExVeS-related problematic scenario exists. As a result, RExVeS-related use cases are not limited to already identified and standardized connected vehicle and road safety use cases (in ISO, SAE, ETSI etc.). The potential applicability of RExVeS-related requirements is much broader.

NOTE 3 ISO 26262-3:2018[5], Annex B provides examples of RExVeS-related scenarios and of safety-critical situations.

Factors to be considered in the hazard analysis and risk assessment of RExVeS-related scenarios include:

— vehicle usage scenarios, for example high speed driving, urban driving, parking, off-road;

— environmental conditions, for example rain, snow, wind, road surface condition;

— reasonably foreseeable driver use and misuse;

— interactions between operational systems, particularly those implementing RExVeS-related time-constrained safety-related functions;

— cybersecurity attacks leading to malicious communications or default of the vehicle ITS station. See also ISO/SAE 21434[6][1)];

— if there is an impact, timing constraints resulting from functional safety, “safety of the intended functionality” and cybersecurity activities;

— in this analysis, the vehicle and its communication capabilities are considered by default in working order. See also ISO/PAS 21448[7].

REQ	23132-01	**RExVeS** – 01
The consequences of each evaluated RExVeS-related time-constrained situation shall be identified, focusing on the harm to each person potentially at risk, including the driver and the passengers of the vehicle, but also the other persons potentially at risk such as cyclists, pedestrians or occupants of other vehicles.		

6.3 Classification of RExVeS-related time-constrained and safety-critical situations

6.3.1 Classification scheme

The classification scheme comprises the determination of the severity, the probability of exposure, and the controllability associated with the RExVeS-related time-constrained situations (safety-critical or not).

1) Under preparation. Stage at the time of publication: ISO/SAE DIS 21434:2020.