TECHNICAL REPORT

ISO/TR 5340

First edition
2023-05

Motorcycles — Consideration for use cases of ISO 26262-12 MSIL classification

Motocycles — Considération des cas d'usages de l'ISO 26262-12 Classification MSIL

Reference number
ISO/TR 5340:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 38, *Motorcycles and mopeds*.

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

0.1 General

The ISO 26262 series is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. The ISO 26262 series does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

ISO 26262-12:2018 is the standard to address the sector-specific needs of E/E systems within series production motorcycles. The motorcycle industry recognizes the need to use appropriate safety-related techniques to avoid unreasonable risk resulting from random or systematic faults of E/E systems.

Motorcycle safety integrity level (MSIL) is the output of hazard analysis and risk assessment (HARA). This is then apportioned between the risk-reduction mechanisms and measures assigned to E/E systems using automotive safety integrity level (ASIL) and the risk reduction taken care of by external measures and/or other technologies. Specifically in the motorcycle industry, a greater proportion of the overall risk reduction is generally apportioned to external measures (for example, riding rules, training/qualification of riders, personal protective equipment, e.g. helmets and infrastructure features).

The worldwide established level of technology ("state-of-the-art") in the motorcycle industry suggests that ASIL requirements are not appropriate for motorcycles. This is addressed through the alignment between MSIL and ASIL. It is acknowledged that product development processes and technical solutions within the motorcycle industry are inhomogeneous with those of the automobile industry; therefore, the difference between MSIL and ASIL has been made to accommodate worldwide capability.

0.2 Objectives

Publicly-available research documents and references relating to the functional safety of motorcycles are fewer in number than those for passenger cars. The purpose of this document is to contribute to the functional safety of motorcycles by internationally collecting and providing examples for motorcycle HARA. This document provides an overview of the principles behind HARA using simplified examples to the concepts.

A prerequisite for HARA is the item definition, which is not the subject of this document. It also does not cover the safety goals of the item. This document takes examples of some items on motorcycles, but is also not exhaustive in terms of their function.

This document presents examples of potential accident scenarios and risk assessments, from the behaviour of an item when it fails and the hazard at vehicle level to its potential accident scenarios. Several methods have been published for each of these, and the aim is to provide a side-by-side comparison to assist in the implementation of HARA.

0.3 Points to note

In using this document, please note the following.

The hazard analysis results and MSIL described in this document is just a collection and does not specify the MSIL of a specific item. Although some examples are given in this document, they are the result of several approaches and do not specify the MSIL for a particular item. The same applies even if only one example is given for an item. Also, the information presented in this document is neither exhaustive nor complete. However, introducing some cases (i.e. analytical approaches and results) will help shape the image for applying the ISO 26262 series.

This document has taken as faithfully as possible the descriptions from published documents. Although there are formatting differences from the original text for the purpose of side-by-side comparison, severity(S), exposure(E), controllability(C) and MSIL described have not been altered or harmonised in any way. The information contained in this document is only part of the published material, and it is recommended to consult the original when referring to it in implementation. The use of these methods is neither mandatory nor recommended and is to be used at the user's own responsibility.

Motorcycles — Consideration for use cases of ISO 26262-12 MSIL classification

1 Scope

This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production motorcycles. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE The series production motorcycle is the vehicle that is intended to be used for public roads and is not a prototype.

This document covers HARA for one or more E/E systems installed in motorcycles. The approach of HARA defined in ISO 26262-12:2018, Clause 8 is applied to them in a motorcycle environment.

The intended user of this document is a functional-safety analyst complying with requirements in ISO 26262-12:2018. Therefore, this document does not intend to provide further necessary knowledge or guidelines in related fields including, but not limited to, item-specific knowledge, user and road profiling, medicine, statistics, accident research and human factors. Instead, it is intended to be related to the field of functional safety with the focus on the HARA examples only. It is the responsibility of the functional-safety analyst to achieve detailed knowledge about the item under investigation and the target application environment.

In this document, the values shown are for reference only. Any new HARA can use the latest relevant data and analyses. The values shown in this document were derived based on some, but not all segments of information expected within an item description, and thus are not considered as an item definition. The ISO 26262 series requires that a HARA be based on a specific item definition. This document is not to be constructed to suggest that conducting a HARA without a specific item definition is acceptable. The scope of the ISO 26262 series is limited to functional safety which is one aspect of the overall system safety assessment in safety risk management.

As for any risk assessment method, the methods mentioned in this document have inherent limitations. The HARA describes a simplified model of the real world, which is neither complete nor fully accurate. Although each assessment is based on available or applicable data as well as on expert judgment, the interpretation of such data can vary among analyses. For these reasons, the user of this document can bear in mind these limitations and judge the applicability of this document in any particular case.

2 Normative reference

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 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 26262-1 apply.

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

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

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

4 General topics for MSIL classification

Hazard analysis, risk assessment and MSIL determination are used to determine the safety goals for the item. For this, the item is evaluated with regard to its potential hazardous events. Safety goals and their assigned MSIL are determined by a systematic evaluation of hazardous events. The MSIL is determined by considering severity, probability of exposure and controllability. It is based on the item's functional behaviour; therefore, the detailed design of the item does not need to be known.

The dynamic behaviour of motorcycles differs greatly from that of other vehicles within the scope of the ISO 26262 series, and that controllability of motorcycle specific hazardous events could place more emphasis on the rider. It is recognised that the method of performing risk assessment requires to best suit motorcycle specific hazardous events.

ISO 26262-12:2018, Annex B gives a general explanation of the hazard analysis and risk assessment.

5 Use case of hazard analysis and risk assessment

5.1 Overview

This clause presents examples of HARA in motorcycles.

HARA is a method to identify and categorize hazardous events of items and to specify safety goals and MSILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk.

The method of performing a HARA is the same as that of a passenger car, but different hazardous events (such as falls down) can be identified depending on the situation peculiar to a motorcycle and the difference in controllability. Evaluation of severity and exposure to driver and others differs significantly from the case of passenger cars.

The case presented below is an example of analysing a scenario in a situation peculiar to motorcycles. These are just a few of the situations that motorcycles encounter, and each item can have other serious hazards. Also, the MSIL shown in the case is just the result of the case study and does not specify the MSIL of the item in general.

Safety goals are top-level safety requirements for the item. Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives. This document does not mention the items of functional objectives and safety goals.

5.1.1 Item definition

HARA is based on the item definition. The item without internal safety mechanisms is evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items are not considered in HARA.

5.1.2 Hazard identification

The purpose of hazard identification is to identify the potential source of harm caused by the malfunctioning behaviour of the item.

Hazards caused by malfunctioning behaviour of the item are defined at the vehicle level.

The hazards are determined systematically based on the possible malfunctioning behaviour of the item. Failure mode and effects analysis (FMEA) approaches and hazard and operability (HAZOP) are suitable to support hazard identification at the item level. These can be supported by brainstorming,

checklists, quality history, and field studies. One example to identify a possible malfunction behaviour with the HAZOP method can be to ask what can happen to the rider or other person if:

— the function is active when it is expected to be deactivated;

— the function is not active when it is expected to be activated;

— the output of the function is unintendedly too high;

— the output of the function is unintendedly too low;

— the output of the function came too late;

— the output of the function is changing too fast;

— the output of the function is in the wrong direction;

— the output of the function is alternating.

The identified malfunction behaviour that can cause harm to the rider or other person can be documented as relevant malfunction with their consequences.

The relevant situations can be identified by analysing the expected usage and the expected misuse of the motorcycle. The relevant situations can differ due to the design (e.g. superbike, enduro) or performance (e.g. 125 cm^3/10 kW, 1 000 cm^3/150 kW) of the analysed motorcycle. Be aware of the specific behaviour of a motorcycle (e.g. lean angle, separated front and rear brake), special manoeuvres (e.g. wheelie, stoppie) and misuses (e.g. towing other vehicle, overloaded luggage in the top case).

One approach to identify all relevant situation is to build-up a list with possible parameters raised from, for example:

Driving operation:

— driving speed;

— lean angle; and

— braking.

Road type:

— location (e.g. motorway, urban, crossing road); and

— road surface condition (e.g. dry, wet, ice).

Situations:

— overtaking;

— parking;

— wheelie;

— crash.

Be aware that a combination of parameters can change the consequences, because it can lead to an inappropriate lowering of the MSIL.

The relevant situations where the identified malfunction can cause harm the rider or other person are the hazardous events for the risk assessment. The consequences of hazardous events are identified.

EXAMPLE An unintended too-high torque output of the engine on a dry country road in a curve with large lean angle can lead to leaving the road lane and to a collision with obstacles.

For a detailed description of the approach, refer to the ISO 26262-3:2018, 6.4.2 and ISO 26262-12:2018, 8.4.2.

5.1.3 Risk assessment

Risk assessment is a series of classifications of potential harms caused by hazards in terms of severity, probability of exposure, or controllability.

The severity of the potential harm is estimated based on a defined rationale for each hazardous event. The severity is assigned to one of the severity classes: S0, S1, S2 or S3.

The probability of exposure of each operational situation is estimated based on a defined rationale for each hazardous event. The probability of exposure is assigned to one of the probability classes: E0, E1, E2, E3 or E4.

The controllability of each hazardous event, by the rider or other persons involved in the operational situation is estimated based on a defined rationale for each hazardous event. The controllability is assigned to one of the controllability classes: C0, C1, C2 or C3.

An MSIL is determined for each hazardous event based on the classification of severity, probability of exposure and controllability. Four MSILs are defined: MSIL A, MSIL B, MSIL C and MSIL D, where MSIL A is representing the least stringent and MSIL D the most stringent level. QM is not an MSIL, but can be specified in the hazard analysis and risk assessment.

Each assessment is based on available or applicable data as well as on expert judgment, the interpretation of such data can vary among analyses.

5.2 Examples of HARA

5.2.1 General

There are different approaches possible for selecting the appropriate values of E, S and C. Possible sources for values can be guidelines, technical papers, ISO 26262-12:2018 Annex B, government statistics, expert judgements or measured data from equivalent motorcycles. The source can be selected according to worldwide use or limited to the expected homologation areas.

For example, the maximum allowed motorway speed can differ in different countries and can change over time (e.g. India: 80 km/h, England: 110 km/h, Japan: 120 km/h, Italy: 130 km/h, USA: 137 km/h, Germany: partly >250 km/h allowed).

NOTE See Reference [6], Table A4: Speed Laws and Enforcement by Country / Area.

Different teams can use different approaches and can come to different results of what can be correct. The use of the data sources must be conservative and correspond to the vehicle, item and target market.

Each selected value of E, S and C can be argued. So, it is possible to follow the selection and the value can be adapted if there is a change.

5.2.2 Example for HARA procedure

a) Hazard identification

   Unintended acceleration of TBW function

b) Operational situation

   Driving on a German motorway with >130 km/h in close distance to vehicle in front (heavy traffic), 0°-5° lean angle

c) Affected persons

Rider and passenger

d) Classification of exposure

Duration E3; E4 for driving on motorway due to commuting use of the analysed motorcycle but -1 due to “close distance to vehicle in front (heavy traffic)” = E3; driving data records from an equivalent motorcycle have shown a driving duration of much less than 10 % at a speed >130 km/h = E3

e) Classification of severity

S3; serious injuries due to falling down with >130 km/h; no traffic in opposite direction expected on motorways = no increase

f) Classification of controllability

C3; rider can handle the brakes or engine stop switch to reduce the acceleration and can steer to avoid collision but not more than 90 % of all riders can react fast enough in this situation (heavy traffic)

5.2.3 Safety goal determination

To determine the safety goal, the MSIL for each hazard event is identified in accordance with ISO 26262-12:2018, 8.4.3.10 and the corresponding malfunction that must be prevented with a safety concept.

The safety goal can have the following information:

— it can be named what can be avoided by the safety function;

— the maximum ASIL can be named;

— the safe state can be defined (e.g. switch off function output for fail safe systems);

— the error threshold for the controllability estimation (e.g, acceleration more than 2,6 m/s^2) can be defined; and

— the fault tolerant time interval (e.g. 300 ms) can be defined.

The safety goal, its information and the safe state can be validated according to ISO 26262-12:2018, Clause 10. The transition to safe state and the safe state itself can provide sufficient controllability. If a test is used to validate the information or the safe state, the safety of the test rider has the highest priority.

5.2.4 Examples of HARA method

In this document, examples of HARA for some items are shown. These items are widely used in motorcycles, and there are also published examples of HARA research reports. By quoting and organizing them, it will help to understand in implementing HARA in practice.

This document cites ANCMA guidelines[4] and SAE technical paper[5].

In some tables, there are expressions of "Method (1)" and "Method (2)". This means that:

a) Method (1): is the approach shown in Reference [4];

b) Method (2): is the approach shown in Reference [5].