INTERNATIONAL STANDARD

ISO 21448

First edition
2022-06

Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue

Reference number
ISO 21448:2022(E)

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 32, *Electrical and electronic components and general system aspects*.

This first edition cancels and replaces the first edition of ISO/PAS 21448:2019, which has been technically revised.

The main changes are as follows:

— the scope has been extended to include all levels of driving automation;

— the clauses and annexes have been reworked and expanded for clarification and additional guidance;

— the definitions (Clause 3) have been reworked, in particular to clarify the hazard model; and

— Clause 13 has been added to address the operation phase after the function has been activated for end users.

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

The safety of road vehicles is a concern of paramount importance for the road vehicle industry. The number of automated driving functionalities included in vehicles is increasing. These rely on sensing, processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E) systems.

An acceptable level of safety for road vehicles requires the absence of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, including both hazards due to failures and due to insufficiencies of specification or performance insufficiencies.

For the achievement of functional safety, ISO 26262-1 defines functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of the E/E system. ISO 26262-3 describes how to conduct a hazard analysis and risk assessment (HARA) to determine vehicle-level hazards and associated safety goals. The other parts of the ISO 26262 series provide requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some E/E systems, e.g. systems which rely on sensing the external or internal vehicle environment to build situational awareness, the intended functionality and its implementation can cause hazardous behaviour, despite these systems being free from the faults addressed in the ISO 26262 series. Example causes of such potentially hazardous behaviour include:

— the inability of the function to correctly perceive the environment;

— the lack of robustness of the function, system, or algorithm with respect to sensor input variations, heuristics used for fusion, or diverse environmental conditions;

— the unexpected behaviour due to decision making algorithm and/or divergent human expectations.

In particular, these factors are relevant to functions, systems or algorithms that use machine learning.

The absence of unreasonable risk resulting from hazardous behaviours related to functional insufficiencies is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and the SOTIF are complementary aspects of safety (see A.2 for a better understanding of the respective scopes of the ISO 26262 series and this document).

To address the SOTIF, measures to eliminate hazards or reduce risks are implemented during the following phases:

— the specification and design phase;

EXAMPLE 1 Modification of vehicle functionality or of sensor performance requirements, driven by identified system insufficiencies or by hazardous scenarios identified during the SOTIF activities.

— the verification and validation phase; and

EXAMPLE 2 Technical reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering conditions, in the loop testing (e.g. SIL: software in the loop / HIL: hardware in the loop / MIL: model in the loop) of selected SOTIF-relevant scenarios.

EXAMPLE 3 Long-term vehicle testing, test-track vehicle testing, simulation testing.

— the operation phase.

EXAMPLE 4 Field monitoring of SOTIF incidents.

These hazards can be triggered by specific conditions of a scenario, defined as triggering conditions, which can include reasonably foreseeable misuse of the intended functionality. Additionally, the interaction with other functions at the vehicle level can lead to hazards (e.g. activation of the parking brake while the automated driving function is active).

Therefore, a proper understanding by the user of the functionality, its behaviour and its limitations (including the human/machine interface) is essential to ensure safety.

EXAMPLE 5 Lack of driver attention while using a Level 2 automated driving system.

EXAMPLE 6 Mode confusion (e.g. the driver thinks the function is activated when it is deactivated) can directly lead to a hazard.

NOTE 1 Reasonably foreseeable misuse excludes intentional alterations made to the system's operation.

Information provided by the infrastructure (e.g. V2X – Vehicle2Everything communication, maps) is also part of the evaluation of functional insufficiencies if it can have an impact on the SOTIF. See D.4 for guidance on V2X features.

EXAMPLE 7 For automated valet parking systems, the functionalities of route planning and object detection could be achieved jointly by the infrastructure and the vehicle.

NOTE 2 Depending on the application, elements of other technologies can be relevant when evaluating the SOTIF.

EXAMPLE 8 The location and mounting of a sensor on the vehicle can be relevant to avoid noisy sensor output resulting from vibration.

EXAMPLE 9 The windshield optical properties can be relevant when evaluating the SOTIF of a camera sensor.

It is assumed that the random hardware faults and systematic faults (including hardware and software faults) of the E/E system are addressed using the ISO 26262 series.

One could interpret the functional insufficiencies addressed in this document as systematic faults. However, the measures to address these functional insufficiencies are specific to this document and complementary to the ones described in the ISO 26262 series. Specifically, the ISO 26262 series assumes that the intended functionality is safe, and addresses E/E system faults that can cause hazards due to a deviation from the intended functionality. The requirement-elicitation process for the system and its elements can include aspects of both standards.

Table 1 illustrates how the possible causes of hazardous events map to existing standards.

Table 1 — Overview of safety relevant topics addressed by different standards

Source of hazard	Cause of hazardous events	Within scope of
System	E/E system faults	ISO 26262 series
	Functional insufficiencies	This document
	Incorrect and inadequate Human-Machine Interface (HMI) design (inappropriate user situational awareness, e.g. user confusion, user overload, user inattentiveness)	This document European Statement of Principles on human-machine interface[1]
	Functional insufficiencies of artificial intelligence-based algorithms	This document
	System technologies EXAMPLE Eye damage from the beam of a lidar.	Specific standards EXAMPLE IEC 60825
External factor	Reasonably foreseeable misuse by the user or by other road participants	This document The ISO 26262 series
	Attack exploiting vehicle security vulnerabilities	ISO/SAE 21434
	Impact from active infrastructure and/or vehicle to vehicle communication, and external systems	This document ISO 20077; ISO 26262 series, IEC 61508 series
	Impact from vehicle surroundings (e.g. other users, passive infrastructure, weather, electromagnetic interference)	This document The ISO 26262 series ISO 7637-2, ISO 7537-3 ISO 11452-2, ISO 11452-4, ISO 10605 and other relevant standards

Road vehicles — Safety of the intended functionality

1 Scope

This document provides a general argument framework and guidance on measures to ensure the safety of the intended functionality (SOTIF), which is the absence of unreasonable risk due to a hazard caused by functional insufficiencies, i.e.:

a) the insufficiencies of specification of the intended functionality at the vehicle level; or

b) the insufficiencies of specification or performance insufficiencies in the implementation of electric and/or electronic (E/E) elements in the system.

This document provides guidance on the applicable design, verification and validation measures, as well as activities during the operation phase, that are needed to achieve and maintain the SOTIF.

This document is applicable to intended functionalities where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, especially functionalities of emergency intervention systems and systems having levels of driving automation from 1 to 5[2].

This document is applicable to intended functionalities that include one or more E/E systems installed in series production road vehicles, excluding mopeds.

Reasonably foreseeable misuse is in the scope of this document. In addition, operation or assistance of a vehicle by a remote user or communication with a back office that can affect vehicle decision making is in scope of this document when it can lead to safety hazards.

This document does not apply to:

— faults covered by the ISO 26262 series;

— cybersecurity threats;

— hazards directly caused by the system technology (e.g. eye damage from the beam of a lidar);

— hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, release of energy and similar hazards, unless directly caused by the intended functionality of E/E systems; and

— deliberate actions that clearly violate the system's intended use, (which are considered feature abuse).

This document is not intended for functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist (e.g. dynamic stability control systems, airbags).

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 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 and the following 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/

3.1
acceptance criterion
criterion representing the absence of an unreasonable level of *risk* (3.23)

Note 1 to entry: The acceptance criterion can be of qualitative as well as quantitative nature, e.g. physical parameters that define when a specific behaviour is considered as hazardous behaviour, maximum number of incidents per hour, as low as reasonably practicable (ALARP).

EXAMPLE 1 From traffic statistics, a reasonable level of risk of one accident per X km is derived.

EXAMPLE 2 The comparison with an equivalent vehicle-level effect that is proven in use to be controllable by the driver can support the definition of an acceptance criterion. For instance, the trajectory perturbation due to an unwanted lane keeping assist function intervention might be compared to a lateral wind gust to define an acceptable level of authority for the function.

3.2
action
single act or behaviour that is executed by any actor in a *scene* (3.27)

Note 1 to entry: The temporal sequence of actions/*events* (3.7) and scenes are parts of the definition of a *scenario* (3.26).

EXAMPLE *Ego vehicle* (3.6) activates the hazard warning lights.

Note 2 to entry: In the context of this definition, an actor can be a person, another object, another system or any element in interaction with the considered function.

3.3
driving policy
strategy and rules defining acceptable *actions* (3.2) at the vehicle level

3.4
dynamic driving task
DDT
real-time operational and tactical functions required to operate a vehicle in traffic

Note 1 to entry: The following functions are part of the DDT:

— lateral vehicle motion control (operational);

— longitudinal vehicle motion control (operational);

— monitoring the driving environment (operational and tactical) and object and *event* (3.7) response execution (operational and tactical), see *object and event detection and response (OEDR)* (3.20);

— manoeuvre planning (tactical); and

— enhancing conspicuity via lighting, signalling or gesturing, etc. (tactical).

Note 2 to entry: The concept was originally defined in SAE J3016[2].

3.5
DDT fallback
response by the driver or automation system to either perform the *dynamic driving task (DDT)* (3.4) or transition to a *minimal risk condition (MRC)* (3.16) after the occurrence of a failure(s) or detection of a *functional insufficiency* (3.8) or upon detection of a potentially hazardous behaviour

EXAMPLE An *operational design domain (ODD)* (3.21) exit or a sensor blocked by ice can lead to hazardous behaviour which requires a response by the driver.

Note 1 to entry: The concept was originally defined in SAE J3016[2].

3.6
ego vehicle
vehicle fitted with functionality that is being analysed for the *SOTIF* (3.25)

3.7
event
occurrence at a point in time

Note 1 to entry: The temporal sequence of *actions* (3.2)/events and *scenes* (3.27) are parts of the definition of a *scenario* (3.26).

Note 2 to entry: While every action is also an event, not every event is an action, i.e. the set of all actions is a subset of all events.

EXAMPLE 1 Tree falling on a street 50 m ahead of a vehicle.

EXAMPLE 2 Traffic light turning green at a given time.

3.8
functional insufficiency
insufficiency of specification (3.12) or *performance insufficiency* (3.22)

Note 1 to entry: Functional insufficiencies include the insufficiencies of specification or performance insufficiencies at the vehicle level or the E/E elements of the system.

Note 2 to entry: The *SOTIF* (3.25) activities include the identification of functional insufficiencies and the evaluation of their effects. Functional insufficiencies lead to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable *misuse* (3.17) by definition (see 3.12 and 3.22). The term “potential functional insufficiency” can be used when the ability to contribute to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable misuse is not yet established.

Note 3 to entry: Figures 1 to 3 describe the SOTIF cause and effect model, in which the relation of *triggering conditions* (3.30), functional insufficiencies, output insufficiencies, hazardous behaviour, inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse, *hazard* (3.11), hazardous *event* (3.7) and harm is described.

Note 4 to entry: In the case of indirect misuse contributing to the occurrence of harm, two functional insufficiencies are typically involved. One is the functional insufficiency leading to the hazardous behaviour of the system in combination with triggering conditions, the other is the functional insufficiency leading to the inability to prevent or detect and mitigate the reasonably foreseeable indirect misuse. See Figures 1, 2 and 3.

EXAMPLE A vehicle is equipped with a Level 2 highway driving assist functionality. A driver monitoring camera to detect the inattentiveness of the driver is part of the system. For sake of simplicity let us assume that the following statements are true:

— the sense element has a functional insufficiency that, if activated by the triggering condition 1, leads to the hazardous behaviour – execution of an incorrect vehicle trajectory; and

— the driving monitoring camera has a functional insufficiency that, if activated by the triggering condition 2, leads to the inability of the system to detect and mitigate a reasonably foreseeable indirect misuse.

For the harm to occur the *scenario* (3.26) needs to contain the following:

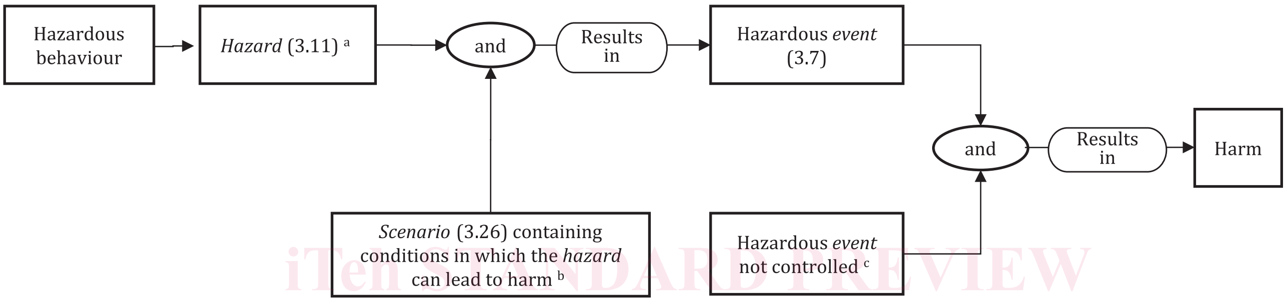
— presence of an indirect misuse by the driver: driver is inattentive and does not detect the hazardous behaviour of the system in time to be able to control it;

— presence of triggering condition 2 leading to the inability of the system to detect and mitigate the present reasonably foreseeable indirect misuse in time; and

— presence of triggering condition 1 leading to the hazardous behaviour of the system.

Note 5 to entry: If a functional insufficiency at the vehicle level is activated by a triggering condition, it results in either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse. See Figure 3 (A).

Note 6 to entry: If a functional insufficiency on element level is activated by a triggering condition, it results in what is referred to as an output insufficiency. See Figure 3 (B). An output insufficiency, either by itself or in combination with one or more output insufficiencies of other elements, contributes to either a hazardous behaviour at the vehicle level or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse. See Figure 3 (B).



Key

[a] The hazard is the potential source of the harm, caused by a hazardous behaviour at the vehicle level.

[b] The scenario containing conditions in which the hazard can lead to harm is a contributing factor to the occurrence of harm, but not its source.

[c] The inability to gain sufficient control of the hazardous event is a contributing factor to the occurrence of harm, but not its source.

Figure 1 — Correlation between hazard and occurrence of harm

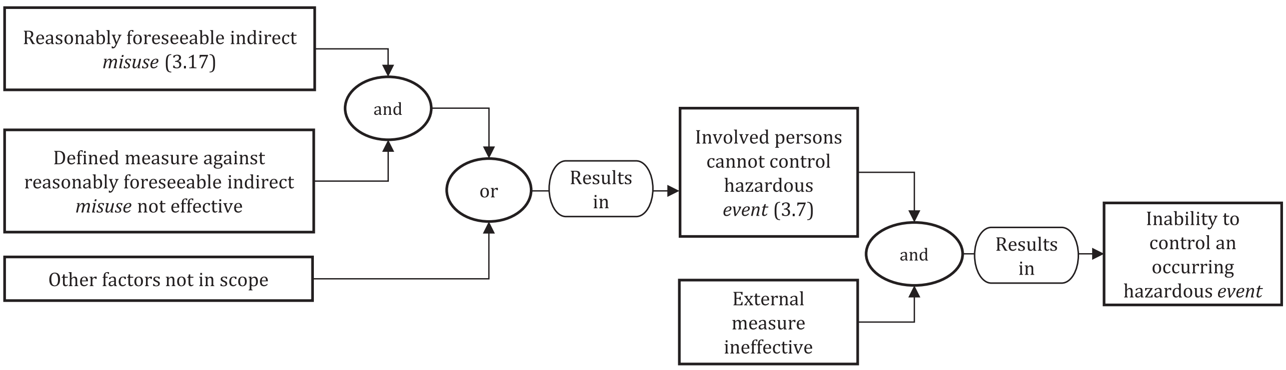
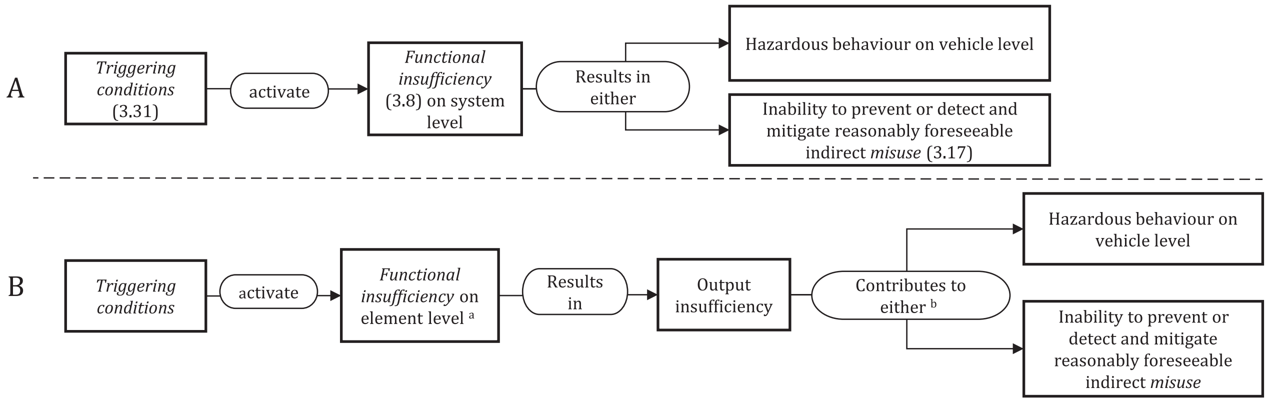


Figure 2 — Reasons for the hazardous event not being controlled



Key

a Depending on the architecture of the system this functional insufficiency on an element level can be recognized either as a *single-point functional insufficiency* (3.28) or *a multiple point functional insufficiency* (3.19).

b An output insufficiency, either by itself or in combination with one or more output insufficiencies of other elements, contributes to either a hazardous behaviour at the vehicle level or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse.

Figure 3 — The SOTIF cause and effect model

3.9
functional modification

alteration of a functional specification

Note 1 to entry: Functional modification is not the same as the term "modification" defined in ISO 26262-1:2018. The "functional modification" of this document would be referred to as "change" in ISO 26262 terms.

3.10
fallback-ready user

user who is able to operate the vehicle and is capable of intervening to perform the *DDT fallback* (3.5) as required and within a time span appropriate for the defined non-driving occupation

Note 1 to entry: The concept was originally defined in SAE J3016[2].

3.11
hazard

potential source of harm caused by the hazardous behaviour at the vehicle level

[SOURCE: ISO 26262-1:2018, 3.75, modified — The word "malfunctioning" has been replaced by "hazardous", the phrase "of the item" has been replaced by "at the vehicle level" and the Note 1 to entry has been removed.]

3.12
insufficiency of specification

specification, possibly incomplete, contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

EXAMPLE 1 An incomplete specification of the adaptive cruise control headway distance results in the *ego vehicle* (3.6) not keeping a safe distance to the vehicle in front.

EXAMPLE 2 System inability to handle uncommon road signs due to specification gaps, i.e. the uncommon road sign is not part of the specification and thus the system cannot process it appropriately.

Note 1 to entry: Insufficiency of specification can be either known or unknown at a given point in the system lifecycle.

Note 2 to entry: The *SOTIF* (3.25) activities include the identification of insufficiencies of specification and the evaluation of their effects. The term “potential insufficiency of specification” can be used when the ability to contribute to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable misuse is not yet established.

Note 3 to entry: Requirements derived from the specification, from the assumptions of other systems or elements, or from systematic analyses (such as those included in Clause 6 or other analyses that elicit design and implementation requirements for the SOTIF) can be included in formal databases to support assurance of verification. These requirements might not be designated as the “specification” in many organizations but are necessary to ensure the SOTIF. The usage of the term “insufficiency (insufficiencies) of specification” in this document includes insufficiencies in such derived requirements.

3.13
intended behaviour
behaviour of the *intended functionality* (3.14)

Note 1 to entry: The intended behaviour is that which the developer considers to be the nominal functionality considering capability limitations due to inherent characteristics of the components and technology used.

Note 2 to entry: The intended behaviour specified by the developer, while not representing *unreasonable risk* (3.31), might not match the driver’s expectation of the system behaviour.

3.14
intended functionality
specified functionality

Note 1 to entry: Intended functionality is defined at the vehicle level.

3.15
levels of driving automation
mutually exclusive set of driving automation levels, ranging from Level 0 (no automation) to Level 5 (full automation), defining the roles of the driver or user and automation system in relation to each other

Note 1 to entry: See Table 2.

Note 2 to entry: The concept was originally defined in SAE J3016[2].

Table 2 — Levels of driving automation

		DDT (3.4)			
Level	Name	Lateral and longitudinal vehicle motion control	*OEDR* (3.20)	*DDT fallback* (3.5)	*ODD* (3.21)
0	No driving automation	Driver	Driver	Driver	Not applicable
1	Driver assistance	Driver and system	Driver	Driver	Limited
2	Partial driving automation	System	Driver	Driver	Limited
3	Conditional driving automation	System	System	*Fallback-ready user* (3.10)	Limited
4	High driving automation	System	System	System	Limited
5	Full driving automation	System	System	System	Unlimited

3.16
minimal risk condition
MRC
vehicle state in order to reduce the *risk* (3.23), when a given trip cannot be completed

Note 1 to entry: This is one expected outcome of a *DDT fallback* (3.5).

Note 2 to entry: The functional safety analogue of the ISO 26262 series would be the safe state.

Note 3 to entry: The concept was originally defined in SAE J3016[2].

3.17
misuse
usage in a way not intended by the manufacturer or the service provider

Note 1 to entry: Misuse includes human behaviour that is not intended but does not include deliberate system alterations or use of the system with the intention to cause harm.

Note 2 to entry: Misuse can result from overconfidence in the performance of the system.

Note 3 to entry: Depending on the causal relationship to the hazardous behaviour, there are two kinds of misuse, direct and indirect.

Note 4 to entry: Direct misuse, which could be a cause for the occurrence of a hazardous behaviour of the system, is considered to be a potential *triggering condition* (3.30). If its ability to contribute to the occurrence of a hazardous behaviour is established, then it is considered to be a triggering condition. It is also possible that the direct misuse is part of a triggering condition, i.e. next to the direct misuse additional specific conditions of a scenario need to be present for the hazardous behaviour of the system to occur.

EXAMPLE 1 Direct misuse: activating a functionality intended for the highway in an urban setting results a *scenario* (3.26) in which the vehicle does not detect and react to a STOP sign.

EXAMPLE 2 Direct misuse: driver activates automated system when outside the *operational design domain (ODD)* (3.21) specified in the user manual. This is considered direct misuse independent of whether the system includes an *ego vehicle* (3.6) localization component that prevents activation outside the specified ODD.

Note 5 to entry: Indirect misuse leads to a reduced controllability of the hazardous behaviour, to a potentially increased severity of an occurring accident, or a combination of both. It is not considered to be a potential triggering condition since it cannot contribute to the hazardous behaviour of the system itself.

EXAMPLE 3 Indirect misuse: a hands-free Level 2 highway assistant with known perception issues, requires the driver to continuously monitor the correct execution of the *dynamic driving task (DDT)* (3.4) by the system and intervene if necessary. Indirect misuse is the driver falling asleep and not monitoring. This is considered indirect misuse independent of whether or not the situation is detected and mitigated by a driver monitoring system.

EXAMPLE 4 Indirect misuse: passenger unbuckling the seat belt while ego vehicle is in motion and driving autonomously. This is indirect misuse due to the potential to increase the severity of an accident while not being a triggering condition.

Note 6 to entry: Refer to Figures 1 to 3.

3.18
misuse scenario
scenario (3.26) in which *misuse* (3.17) occurs

3.19
multiple-point functional insufficiency
functional insufficiency (3.8) of an element leading to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17) only in conjunction with functional insufficiencies of other elements when activated by one or more *triggering conditions* (3.30)

3.20
object and event detection and response
OEDR
tasks of the *dynamic driving task (DDT)* (3.4) that include monitoring the driving environment and executing an appropriate response to objects and *events* (3.7) to complete the DDT and/or the *DDT fallback* (3.5)

[SOURCE: SAE J3016:2021, 3.19[2], modified — The phrase "(detecting, recognizing, and classifying objects and events and preparing to respond as needed)" located after "environment" was removed.]