INTERNATIONAL STANDARD

ISO 34502

First edition
2022-11

Road vehicles — Test scenarios for automated driving systems — Scenario based safety evaluation framework

Véhicules routiers — Scénarios d'essai pour les systèmes de conduite automatisée — Cadre d'évaluation de la sécurité basé sur des scénarios

Reference number
ISO 34502:2022(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 33, *Vehicle dynamics and chassis components*.

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

In order to safely introduce automated driving systems (ADS) into the market, socially acceptable and technically sound scenario-based safety evaluation methodologies need to be developed. A number of national and international governmental institutions are gradually releasing technical safety guidelines[7][8][9] to support the development of these methodologies, as well as associated regulations and standards.

In order to evaluate whether ADSs are free from unreasonable risks, it is beneficial to develop safety evaluation methodologies. Considering emphasis on limited access highways, scenario-based safety evaluation methodologies are suitable for assessing safety in a repeatable, objective and evidence-based manner and that is compatible with existing standards.

Functional safety is defined as the absence of unreasonable risks that arise from malfunctions of an electric/electronic (E/E) system. The ISO 26262 series specifies a hazard analysis and risk assessment to determine vehicle level hazards. This evaluates the potential risks due to malfunctioning behaviour of the system and enables the definition of top-level safety requirements, i.e. the safety goals, necessary to mitigate the risks.

For some E/E systems, which rely on sensing the external or internal environment to build situational awareness, there can be potentially hazardous behaviour caused by or within the intended functionality. Examples of the causes of such potentially hazardous behaviour include the inability of the function to correctly comprehend the situation and operate safely or insufficient robustness of the function, system, or algorithm. 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 (the ISO 26262 series) and SOTIF (ISO 21448) are distinct, necessary, and complementary aspects of safety. This document is conformant with SOTIF and adds specificity to its content, by incorporating a scenario-based safety evaluation process that identifies risk factors and related critical scenarios that affect the intended functionality, and apply them to evaluate whether the ADS is free from unreasonable risks.

The International Organization for Standardization (ISO) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO. Information may be obtained from the patent database available at www.iso.org/patents.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO shall not be held responsible for identifying any or all such patent rights.

Road vehicles — Test scenarios for automated driving systems — Scenario based safety evaluation framework

1 Scope

This document provides guidance for a scenario-based safety evaluation framework for automated driving systems (ADSs). The framework elaborates a scenario-based safety evaluation process that is applied during product development. The guidance for the framework is intended to be applied to ADS defined in ISO/SAE PAS 22736 and to vehicle categories 1 and 2 according to Reference [10]. This scenario-based safety evaluation framework for ADS is applicable for limited access highways.

This document does not address safety-related issues involving misuse, human machine interface and cybersecurity.

This document does not address non-safety related issues involving comfort, energy efficiency or traffic flow efficiency.

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 34501, *Road vehicles — Test scenarios for automated driving systems — Vocabulary*

ISO 21448, *Road vehicles — Safety of the intended functionality*

ISO 26262-3, *Road vehicles — Functional safety — Part 3: Concept phase*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 34501 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
critical scenario
scenario including one or more *risk factors* (3.3)

3.2
hazardous scenario
scenario in which harm occurs unless prevented by an entity other than the ADS

3.3
risk factor
factor or condition of a scenario that, if present, increases either the probability of the occurrence of harm, or the severity of harm, or both

3.4
safety test objective
safety property of the ADS to be shown via a set of tests

Note 1 to entry: The safety test objectives can be derived from the validation targets or the acceptance criteria of ISO 21448.

Note 2 to entry: The safety test objectives also include the aspect of the test end criteria.

Note 3 to entry: Depending on the kind of the safety test objectives the pass/fail-criteria of a concrete test scenario can be included within the safety test objectives.

4 Test scenario-based safety evaluation process

4.1 Integration into the overall development process

4.1.1 Objectives

The objectives of this clause are:

a) to provide an overview of the overall safety tasks and content of this document;

b) to provide an overview of the scenario-based safety evaluation process;

c) to explain the relationship between this framework and other standards and legislation.

4.1.2 General

4.1.2.1 Overall safety tasks and content of this document

Figure 1 presents the overall safety task "Identification and risk evaluation of the hazardous scenarios of the ADS" and its derived subtasks.

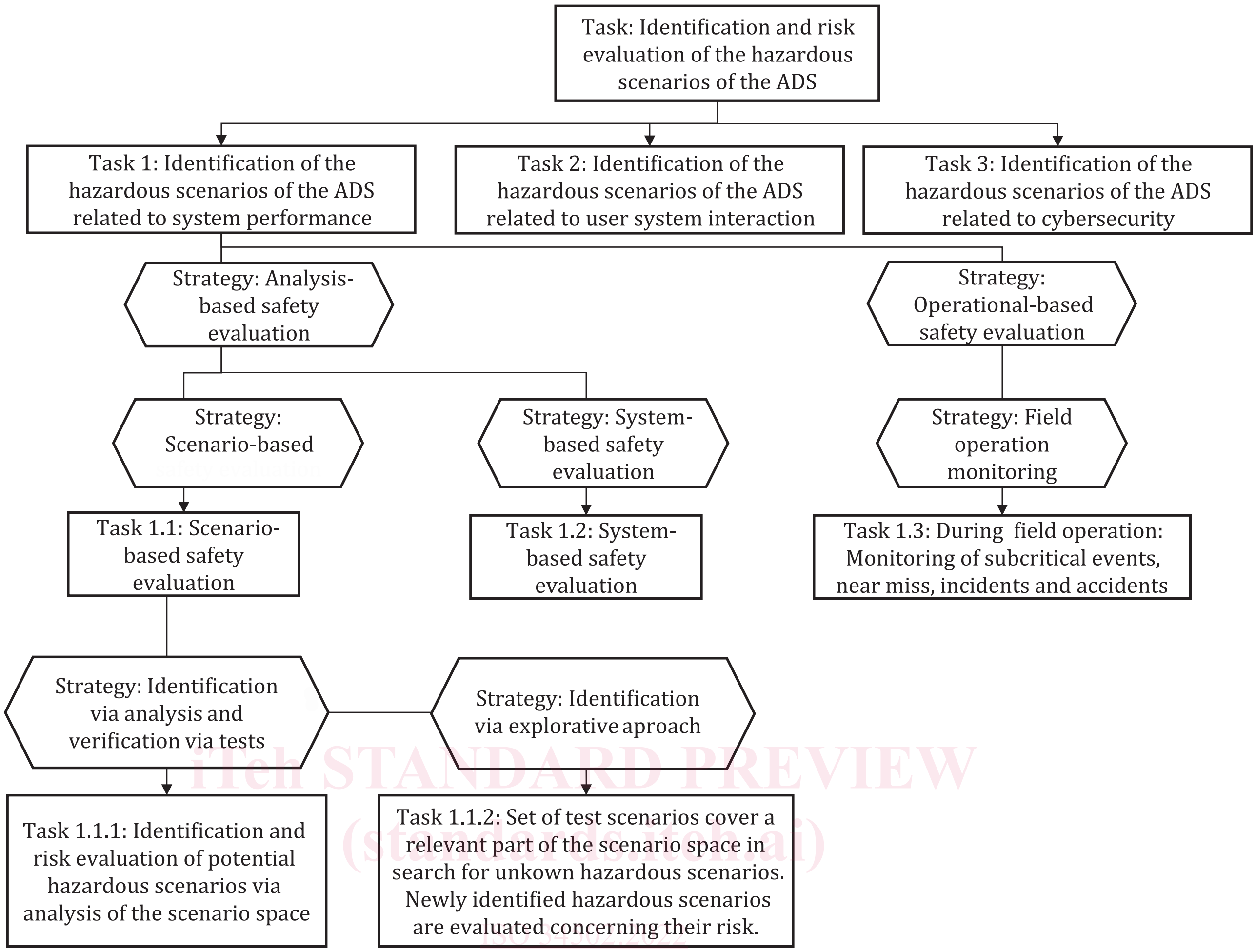


Figure 1 — Overview of the different safety tasks to identify hazardous scenarios for the ADS

This document proposes to address the identification of potential hazardous scenarios via analysis from two different starting points:

1. the relevant scenario space (task 1.1);

2. the system (task 1.2).

This approach is similar to the approach found in functional safety where the safety analysis is executed from two different and complementary perspectives: The deductive approach (e.g. Fault Tree Analysis, FTA) and the inductive approach (e.g. Failure Modes and Effects Analysis, FMEA).

In system-based approaches (task 1.2), the starting point of the analysis is the system itself. In scenario-based approaches (task 1.1), which are the focus of this document, the starting point is the analysis of the scenarios belonging to the relevant scenario space. For this approach the relevant scenario space is analysed to identify risk factors. Only general physical limitations of the systems are considered, for example, a sensor has a field of view based on the physics of its detection system, but other implementation specific issues, e.g. the limitations of a machine learning algorithm to classify a detected object correctly or sensor failures due to random hardware faults, are neglected. These system specific aspects can be better analysed with system-based approaches. One advantage of the scenario-based approach is that it can be applied with minimal dependency on the implementation of the system itself (e.g. for regulatory use). As such, the results of a given analysis can be reused for different systems as long as the relevant scenario space is the same, considering that the concrete parameters maximizing the risk factor for a given scenario still have system dependencies (e.g. exact number and positions of sensors).

NOTE 1 Knowledge gained during the execution of one approach (e.g. the system-based approach) can be used to support the analysis by another approach (e.g. the scenario-based approach).

NOTE 2 The results of the system-based safety analysis can also be test scenarios to be executed.

Not all the relevant tasks for ADS safety evaluation are addressed by this document. This document predominantly focuses on:

— task 1.1.1: identification and risk evaluation of potential hazardous scenarios via analysis of the relevant scenario space (see 4.3); and

— task 1.1.2: derivation of a representative set of test scenarios to argue a sufficient coverage of the relevant scenario space in search for unknown hazardous scenarios (see Annex K).

Guidelines for the execution of the remaining safety tasks can be found in other standards, e.g.

— task 2: ISO 21448;

— task 3: ISO/SAE 21434;

— task 1.2 and task 1.3: ISO 21448, the ISO 26262 series.

NOTE 3 Some safety issues can be assigned to multiple tasks.

EXAMPLE An adversarial attack, also known as “physical hack”, for example, in which sensors are spoofed with the help of stickers on traffic signs, can be assigned to task 3 and task 1. Within task 3, the relevant attack scenarios are identified. Within task 1.1 and task 1.2, it is evaluated whether the system is sufficiently robust against the identified relevant attack scenarios.

NOTE 4 The result of task 1.2, the system based analysis, can also be scenarios that need to be tested in order to evaluate the safety of the system.

NOTE 5 Overall guidance concerning safety for ADS considering SOTIF, functional safety and security can be found in, e.g. ISO/TR 4804.

4.1.2.2 Overall flow of this document

Figure 2 shows the overall flow of this document within the scope of product development processes. Within the figure:

— the first column from the left represents the inputs to the scenario-based safety evaluation process elaborated within this document;

— the second column represents the preparation phase preceding the identification of critical scenarios phase in which safety test objectives are specified;

— the third column provides an overview of the specification of the relevant scenario space, and identification of risk factors and critical scenarios for safety evaluation according to the scenario-based safety evaluation framework;

— the fourth column shows the interconnections among the scenario-based safety testing and evaluation process (safety analysis phase) and the remaining product development phases;

— the fifth column represents how the output of the scenario-based safety evaluation framework fits into the overall vehicle safety approval process that includes other safety validation steps;

— lines indicate iteration loops and influence conditions; they can contain new findings and trigger necessary adaptations, when, for example, functional modifications are necessary due to safety reasons.

The subclauses in Clause 4 aim at addressing the following points to contribute to an overall scenario-based safety evaluation process.

— 4.1 **Integration into the overall development process:** How the framework integrates into existing product development processes.

— 4.2 **Safety test objectives:** Specification of safety test objectives that the system needs to fulfil.

— 4.3 **Specification of the relevant scenario space:** How the relevant scenario space is defined.

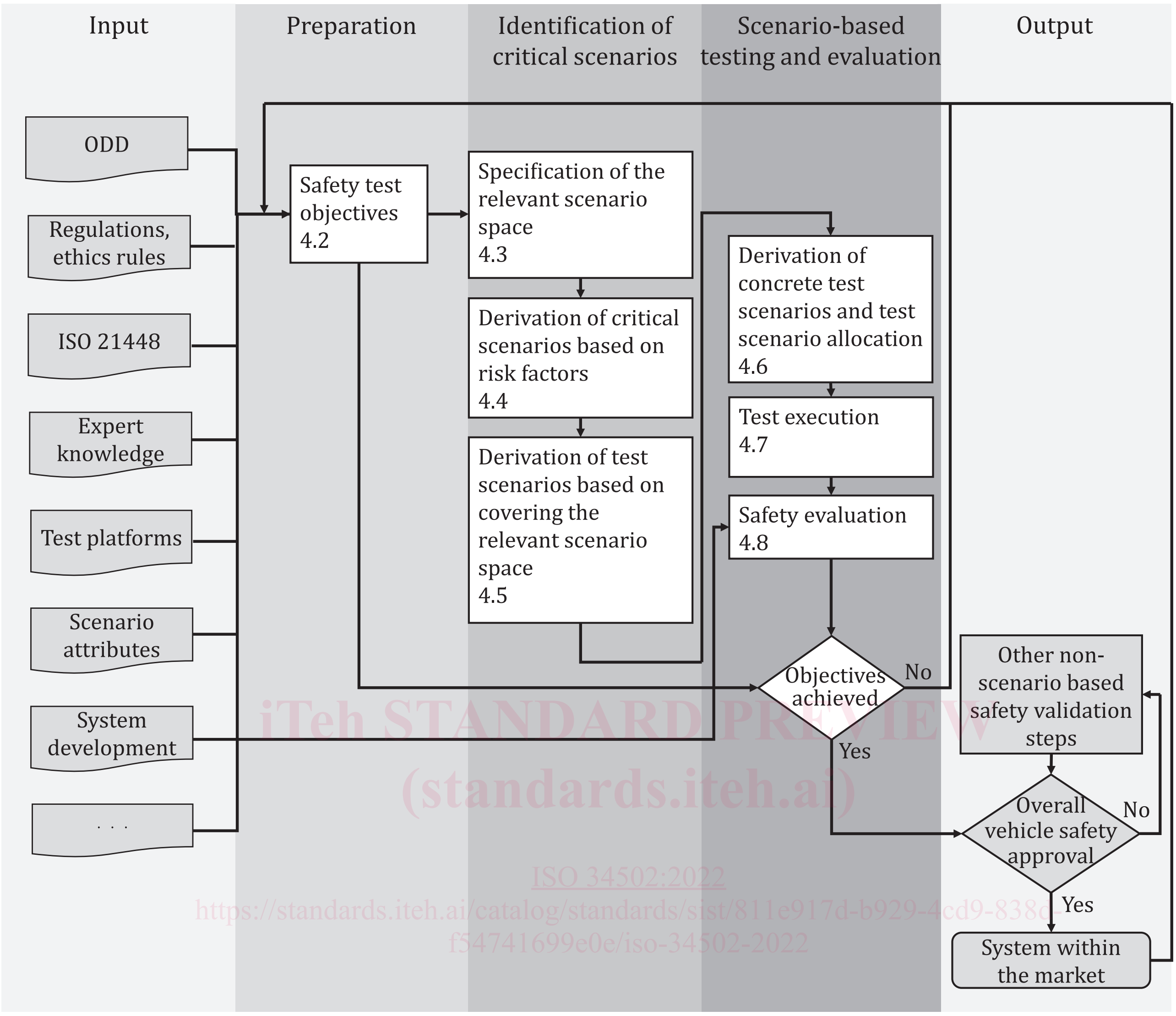
— 4.4 **Derivation of critical scenarios based on risk factors:** How to define a set of critical scenarios from which a set of test scenarios are derived.

— 4.5 **Derivation of test scenarios based on covering the relevant scenario space:** The identification of critical scenarios to potentially be tested.

— 4.6 **Derivation of concrete test scenarios and test scenario allocation:** How test scenarios are generated and allocated to different testing platforms.

— 4.7 **Test execution:** Requirements that need to be fulfilled while running test scenarios.

— 4.8 **Safety evaluation:** How the test results are evaluated to achieve an overall result.



Key

input

step in this document (clause number)

decision in this document

decision in this document

external decision

Figure 2 — ISO 34502 flow

Figure 3 illustrates the relationship between ISO 21448 and this document.

4.3 adds specificity to ISO 21448:2022, Clause 7, by identifying reasonably foreseeable risk factors that may lead to hazardous scenarios. By structuring these risk factors, critical scenarios are generated and compiled into a scenario catalogue for testing purposes. Therefore, the approach to identifying and structuring risk factors in this document contributes to maximize the coverage of known hazardous scenarios in SOTIF.

4.5 contributes to address ISO 21448:2022, Clause 9, by defining the concrete scenarios that need to be tested and their corresponding platforms, which is an essential step to define the verification and validation strategy.

Finally, 4.3 to 4.8 contribute to address ISO 21448:2022, Clauses 10 and 11. By using the known hazardous scenario as additional input to the safety evaluation process, and varying some of the properties/attributes of these scenarios, unknown hazardous scenarios can also be explored, and the space and amount of unknown scenarios can be reduced.

NOTE The scenario-based safety evaluation process or parts of it can be applied to the system, subsystem or component level, in addition to the vehicle level. Accordingly, the process is adapted to the corresponding ADS under test.

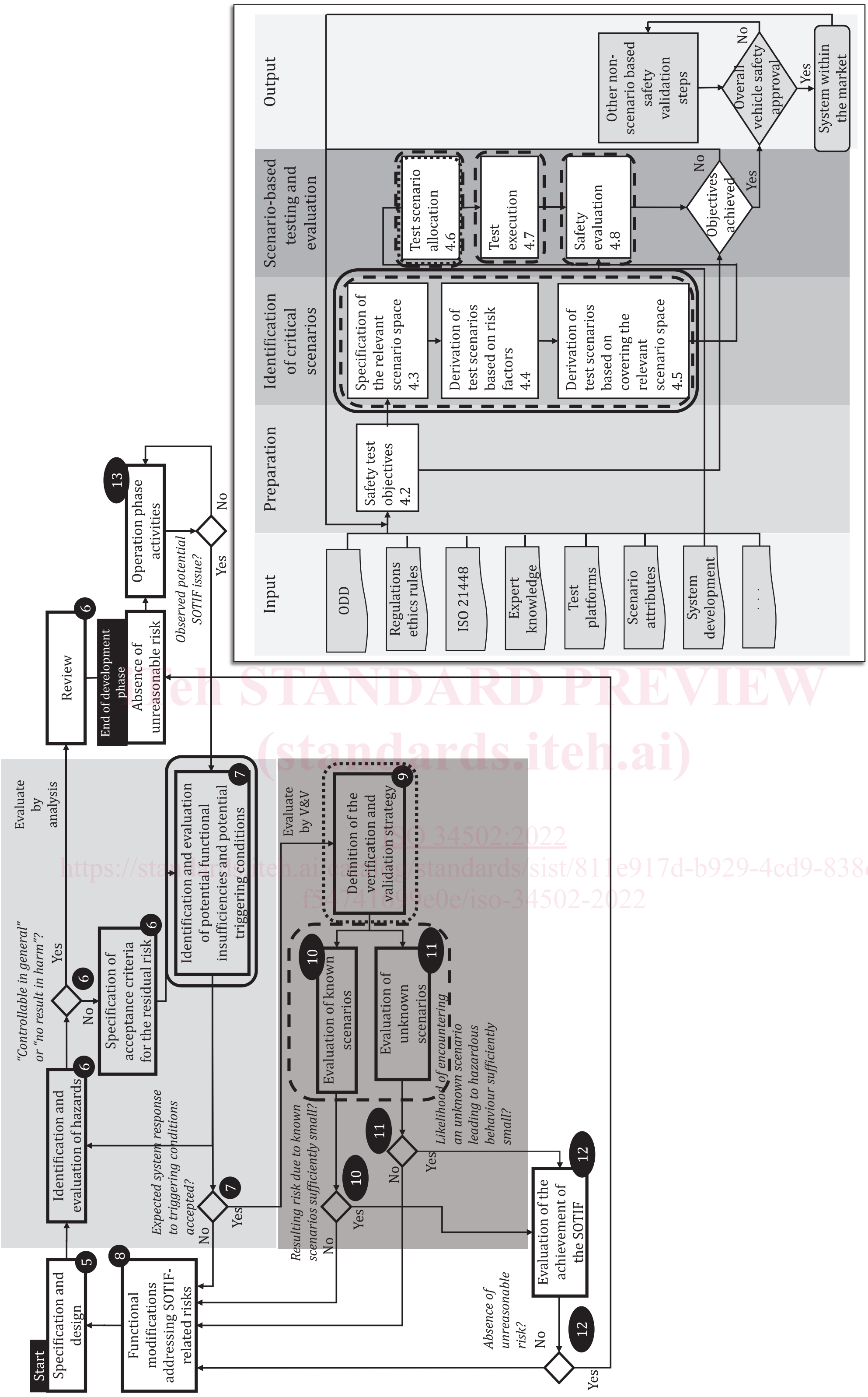


Figure 3 — Relationship between ISO 21448 (left) and ISO 34502 (right) flow charts

4.1.3 Requirements and recommendations

This document shall be applied in combination with:

— ISO 21448.

4.1.4 Requirements for conformity

When claiming conformance with this document, each requirement shall be met unless a rationale is provided, demonstrating that the non-conformity is deemed acceptable, i.e. the corresponding objectives are still achieved.

4.2 Safety test objectives

4.2.1 Objectives

The objective of 4.2 is to specify the relevant safety test objectives for the ADS safety evaluation.

4.2.2 General

The safety test objectives represent the safety properties of the ADS to be shown via a set of tests. The objectives are derived from general risk acceptance criteria like the principles of 'as low as reasonably practicable' (ALARP), of 'minimal endogenous mortality' (MEM), of 'positive risk balance' (PRB), and of applicable regulations. The safety test objectives are either derived from or provided by an external source like ISO 21448 or by a related regulation[11]. The safety test objectives are typically expressed by using, for example, one of the two following procedures.

a) Safety test objectives specified as a boundary value (upper, or depending on the formulation, lower boundary value) of the acceptable and demonstratable occurrence rate of a measurable safety-related behaviour of the ADS (or its elements) during operation within the operational domain.

   EXAMPLE 1 A hazardous behaviour of the system that is evaluated as critical, does not occur during x hours of test operation within the operational domain.

   EXAMPLE 2 The perception element forwards incorrectly perceived objects to the control element less than once per y hours during operation within the operational domain.

   EXAMPLE 3 The relative frequency of undesired behaviour in a given scenario is lower than x.

b) Safety test objectives specified as a performance reference model regarding the capability of the ADS to handle certain scenarios safely, based on minimum performance levels required for these scenarios.

   EXAMPLE 4 The ADS is capable of preventing any accident that would be preventable according to a reference performance model of a competent and careful human driver.

The safety test objectives are chosen in such a way that their fulfilment supports the overall safety argument of the ADS. They represent a measurable or observable property of the ADS.

NOTE Additional safety arguments (e.g. safety analysis) can be a necessary part the fulfilment of the safety test objectives to demonstrate that the overall safety argument is valid.

4.2.3 Input to this clause

4.2.3.1 Prerequisites

The following information shall be considered if available:

— industry standards (e.g. ISO 21448, the ISO 26262 series);

— operational design domain (ODD);

— design and functionality of the ADS, including the intended behaviour;

— other safety-relevant scenario catalogues (e.g. NCAP).

