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)

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 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:

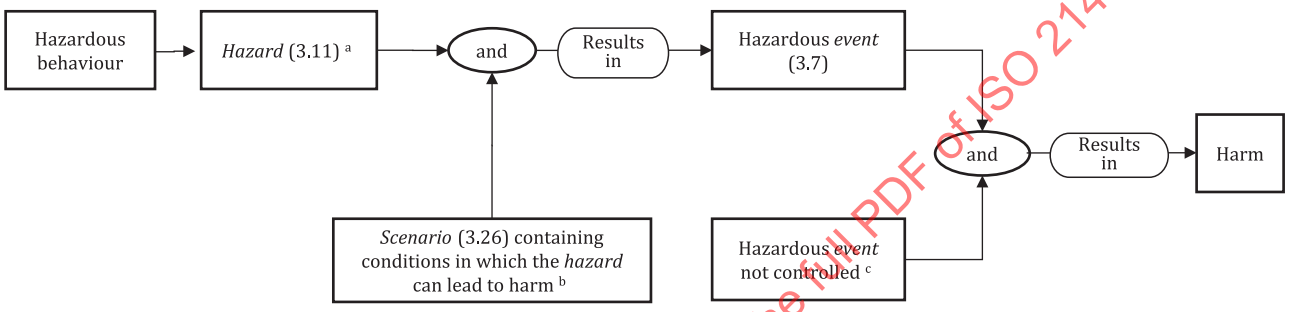
— presence of an indirect misuse by the driver: driver is inattentive and does not detect the hazardous behaviour of the system in time to be able to control it;

— 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

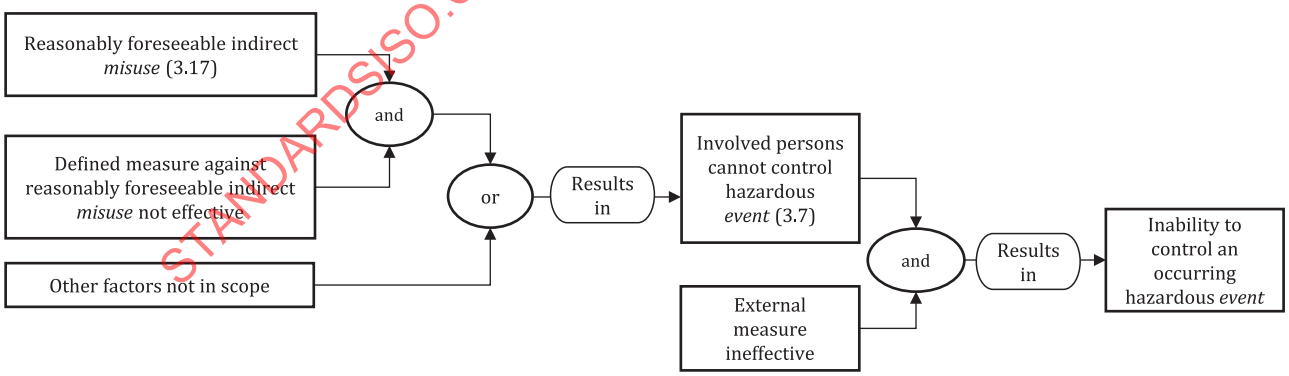
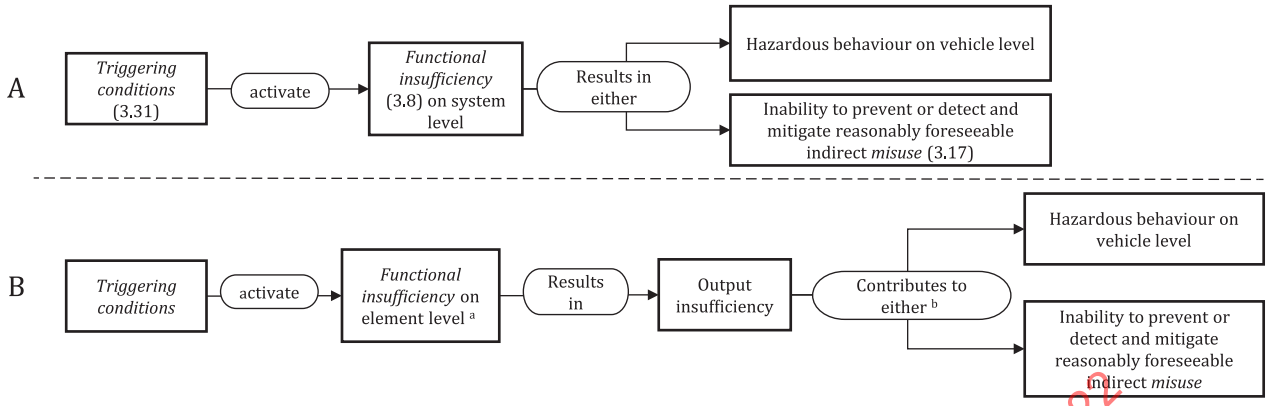


Figure 2 — Reasons for the hazardous event not being controlled



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.]

3.21
operational design domain
ODD
specific conditions under which a given driving automation system is designed to function

Note 1 to entry: Conditions can be spatial, temporal, intrinsic or environmental.

Note 2 to entry: The term "designed" is taken from the definition in SAE J3016[2]. In this document it means "specified".

Note 3 to entry: The conditions of automated driving system itself (e.g. the vehicle speed, computing capabilities, and perception sensing capabilities) are also in the scope of ODD.

Note 4 to entry: The concept was originally defined in SAE J3016[2].

3.22
performance insufficiency
limitation of the technical capability contributing to a hazardous behaviour or inability to prevent or detect and mitigate reasonably foreseeable indirect *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

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

Note 2 to entry: Performance insufficiencies are considered for E/E elements of the system and elements of other technologies considered relevant to the achievement of the *SOTIF* (3.25) (see Note 1 to entry of 3.8).

Note 3 to entry: The SOTIF activities include the identification of performance insufficiencies and the evaluation of their effects. The term "potential performance 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.

EXAMPLE Limitation of technical capabilities are limited calculation performance, limited perception range of a sensor, limited actuation, etc.

3.23
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 26262-1:2018, 3.128]

3.24
reaction
response to an *action* (3.2) by any actor in a *scene* (3.27)

3.25
safety of the intended functionality
SOTIF
absence of *unreasonable risk* (3.31) due to *hazards* (3.11) resulting from *functional insufficiencies* (3.8) of the *intended functionality* (3.14) or its implementation

Note 1 to entry: A hazardous behaviour of the system that could lead to a *hazard* (see Figure 1) is initiated by a *triggering condition* (3.30) of a *scenario* (3.26). Reasonably foreseeable direct *misuse* (3.17) is considered as a potential triggering condition.

Note 2 to entry: When identifying the hazardous *events* (3.7), intended use and reasonably foreseeable indirect misuse are also considered in combination with hazardous behaviour resulting from *insufficiencies of specification* (3.12) or *performance insufficiencies* (3.22).

3.26
scenario
description of the temporal relationship between several *scenes* (3.27) in a sequence of scenes, with goals and values within a specified situation, influenced by *actions* (3.2) and *events* (3.7)

Note 1 to entry: Every scenario starts with an initial scene. Actions and events, as well as goals and values, can be specified to characterise this temporal relationship within a scenario. In contrast to a scene, a scenario spans a certain amount of time.

Note 2 to entry: This definition is adapted from Reference [3].

Note 3 to entry: The referenced "goals and values" are conditional parameters of the *intended functionality* (3.14). A goal could be "staying between the lane markings". A value could be to "prioritize safety of pedestrians over avoiding monetary damage".

3.27
scene
snapshot of the environment including the scenery, dynamic elements, and all actors' and observers' self-representations, and the relationships among those entities

Note 1 to entry: A scene can include environmental elements (state, time, weather, lighting and other surrounding conditions), road infrastructure or internal elements (road or interior geometry, topology, quality, traffic signs, barriers, etc.) and objects/actors (static, dynamic, movable, interactions, manoeuvres if applicable).

Note 2 to entry: An all-encompassing scene (i.e. an objective scene or ground truth) incorporating all entities (e.g. scenery, dynamic elements, actors) can only be modelled in simulation. In the real-world, scenes are perceived by sensors. The scene perceived by the *ego vehicle* (3.6) or human driver is an incomplete, inaccurate, uncertain and potentially erroneous projection of ground truth.

Note 3 to entry: The scene can also include aspects of the ego vehicle and the system implementing the *intended functionality* (3.14), like tyre pressure, user occupation and the presence of failures of parts of the system.

Note 4 to entry: This definition is adapted from Reference [3].

3.28
single-point functional insufficiency
functional insufficiency (3.8) of an element leading directly to hazardous behaviour or the inability to prevent or detect and mitigate a reasonably foreseeable *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

3.29
situational awareness
understanding of the situation

3.30
triggering condition
specific condition of a *scenario* (3.26) that serves as an initiator for a subsequent system reaction contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17)

Note 1 to entry: The concept of "triggering" includes the possibility that there can be multiple conditions that can gradually happen, leading to hazardous behaviour or the inability to prevent or detect and mitigate a reasonably foreseeable misuse.

Note 2 to entry: A triggering condition of a *scenario* (3.26) activates a *functional insufficiency* (3.8), resulting in the subsequent system reaction. See Figures 1 to 3.

EXAMPLE While operating on a highway, a vehicle's automated emergency braking (AEB) system misidentifies a road sign as a lead vehicle, resulting in braking at X *g* for Y seconds. In this example, the triggering condition is the circumstance which leads to the misidentification of the road sign while operating on a highway, whereas AEB has the relevant *performance insufficiency* (3.22) (e.g. low accuracy of perception or misclassification by algorithm).

Note 3 to entry: The *SOTIF* (3.25) activities include the identification of triggering conditions and the evaluation of the response of the system. The term "potential triggering condition" can be used when the ability to initiate a corresponding reaction is not yet established.

Note 4 to entry: Reasonably foreseeable direct misuse, which could directly initiate a hazardous behaviour of the system, is considered as a potential triggering condition.

Note 5 to entry: Refer to Figures 1 to 3.

3.31
unreasonable risk
risk (3.23) judged to be unacceptable in a certain context according to valid societal moral concepts

[SOURCE: ISO 26262-1:2018, 3.176]

3.32
use case
description of a suite of related *scenarios* (3.26)

Note 1 to entry: A use case can include the following information about the system:

— one or several scenarios;

— the functional range (e.g. maximum allowed speed, maximum allowed deceleration);

— the desired behaviour;

— the system boundaries; and

— assumptions on the environment and human operation.

Note 2 to entry: The use case description typically does not include a detailed list of all relevant scenarios for this use case. Instead a more abstract description of these scenarios is used.

Note 3 to entry: This definition is adapted from Reference [3].

3.33
validation target
value to argue that the *acceptance criterion* (3.1) is met

Note 1 to entry: The definition of a validation target depends on target markets and operational scenarios.

Note 2 to entry: In the context of the *SOTIF* (3.25), validation is the assurance, based on examination and tests, that the acceptance criteria (of the identified hazards) will be achieved with a sufficient level of confidence.

EXAMPLE No hazardous behaviour of the functionality during a Y hour endurance run, or one hazardous behaviour with a certain severity during X times parking

Note 3 to entry: For the complete fulfilment of a given acceptance criterion, the fulfilment of more than one validation target can be necessary.

3.34
vehicle-level SOTIF strategy
VLSS
set of vehicle-level requirements for the *intended functionality* (3.14) used to support design, verification and validation activities to achieve the *SOTIF* (3.25)

Note 1 to entry: A VLSS can be defined for each SOTIF-related system.

4 Overview and organization of SOTIF activities

4.1 General

Clause 4 provides:

a) an overview of the SOTIF principles;

b) guidance on the workflow of SOTIF activities and use of this document; and

c) guidance on the management of SOTIF activities and supporting processes.

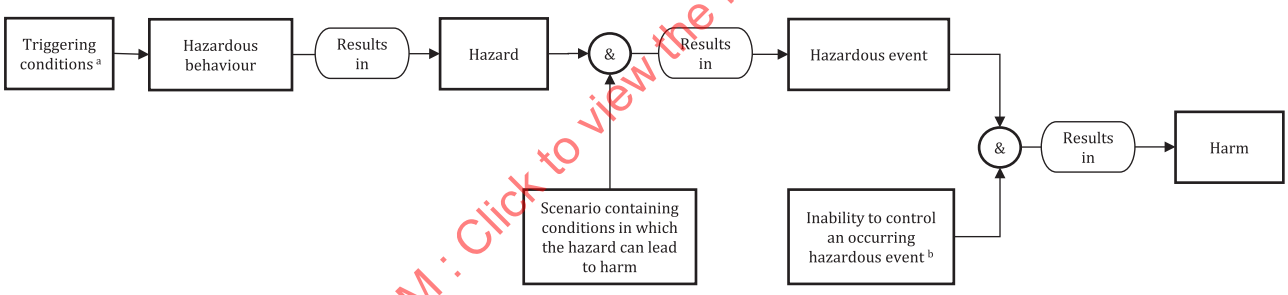
The activities specified in this document are applicable to the vehicle, system and component levels.

4.2 SOTIF principles

4.2.1 SOTIF-related hazardous event model

The main objective of this document is to describe the activities and rationale used to ensure that the risk level associated with all identified SOTIF-related hazardous events is sufficiently low.

The function, system specification and design include relevant use cases which, in turn, comprises several scenarios. These scenarios could contain triggering conditions that lead to harm (for a simplified version see Figure 4, for a more detailed version see Figures 1 to 3). In order to avoid the harm, proper situational awareness is necessary.



Key

a Triggering conditions include reasonably foreseeable direct misuse.

b The inability to control the hazardous event can also be the result of a reasonably foreseeable indirect misuse, e.g. the driver does not supervise the system as he/she is supposed to do.

Figure 4 — Visualisation of a SOTIF-related hazardous event model

EXAMPLE 1 When activated in an urban setting, a functionality intended for only highway use has limitations in recognizing and interpreting the motion of vulnerable road users.

EXAMPLE 2 Incorrect understanding of the system operating mode by the driver who assumes that the system is active even though it is deactivated. In such a situation, the potential insufficiencies of the system HMI to prevent this confusion or the absence of an appropriate system reaction (if the driver behaviour can be monitored) can also be considered as a hazardous behaviour of the system.

NOTE 1 Proper situational awareness relies on:

— Sufficiently comprehensive and accurate perception of the relevant environmental conditions, a correct understanding of the scene (e.g. detecting a relevant stop sign) and a forecast model regarding the state of each road actor (e.g. heading direction, speed). Situational awareness can be further supported by information such as localization, ego-motion, or communication with other vehicles or the environment;

— appropriate actions or reactions when driving (e.g. obey rules associated with stop signs).

Over the vehicle operational life, the following can vary:

— the environment (e.g. new type of traffic signs, road markings, vehicles);

— appropriate reactions (e.g. new driving action required by a new traffic sign; changes in driving scenarios, changes in driving laws).

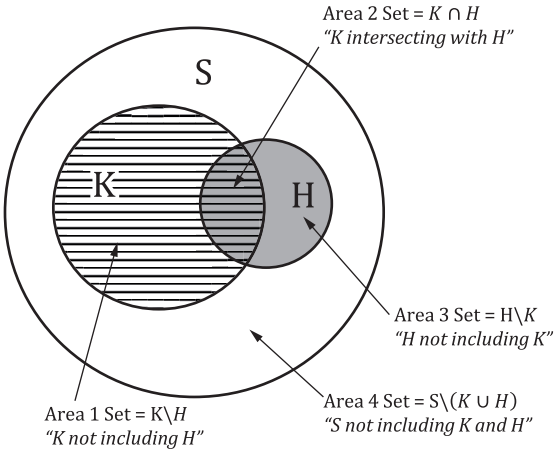
NOTE 2 The monitoring of such changes is addressed in Clause 13 of this document.

NOTE 3 This concern could be covered by requirements derived for the driving policy. An example of this is in D.1.

Such considerations are taken into account when specifying the operational design domain (ODD) and during system development (risk identification, definition of appropriate measures) to ensure the SOTIF during operation.

4.2.2 The four scenario areas

Within this document, the hazardous scenarios are scenarios causing hazardous behaviour. The scenarios which are part of the relevant use cases are classified into four areas (see Figures 5 and 6).



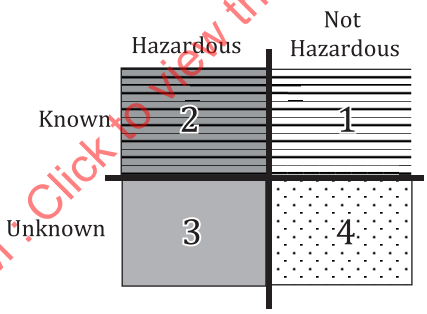
Key

represents the set of known scenarios K

represents the set of all possible scenarios S

represents the set of hazardous scenarios H

Figure 5 — Visualisation of scenario categories



Key

known, not hazardous scenarios (area 1)

known, hazardous scenarios (area 2)

unknown, hazardous scenarios (area 3)

unknown, not hazardous scenarios (area 4)

Figure 6 — Alternative visualisation of scenario categories

Areas 1, 2, 3 and 4 are defined to structure and guide the understanding of this document as follows:

— known not hazardous scenarios (area 1);

— known hazardous scenarios (area 2);

— unknown hazardous scenarios (area 3); and

— unknown not hazardous scenarios (area 4).

EXAMPLE Unknown areas are related to the scenarios when:

— the potential triggering conditions have been identified (e.g. extreme low temperature, special combination of driving scenarios), however, the behaviour of the system is unknown;

— there are unknown triggering conditions (e.g. “black swan” events); or

— known parameters of scenarios can combine into unknown potential triggering conditions (e.g. combination of weather and traffic conditions).

NOTE 1 Scenarios in area 4 that are unknown but not hazardous do not impose risk of harm. Once a scenario in area 4 is discovered (i.e. becomes known), it is moved to area 1.

This model is a conceptual abstraction representing a goal of the SOTIF activities, which is to:

— perform a risk acceptance evaluation of area 2 based on the analysis of the intended functionality;

— reduce the probability of known hazardous scenarios causing hazardous behaviour, in area 2, to an acceptable level through functional modification (see Clause 8);

— reduce the probability of the unknown scenarios causing potentially hazardous behaviour, in area 3, to an acceptable criterion through an adequate verification and validation strategy (see Clauses 9 and 11).

NOTE 2 This is just a conceptual approach of one aspect of the task since the sizes of the areas are not measurable.

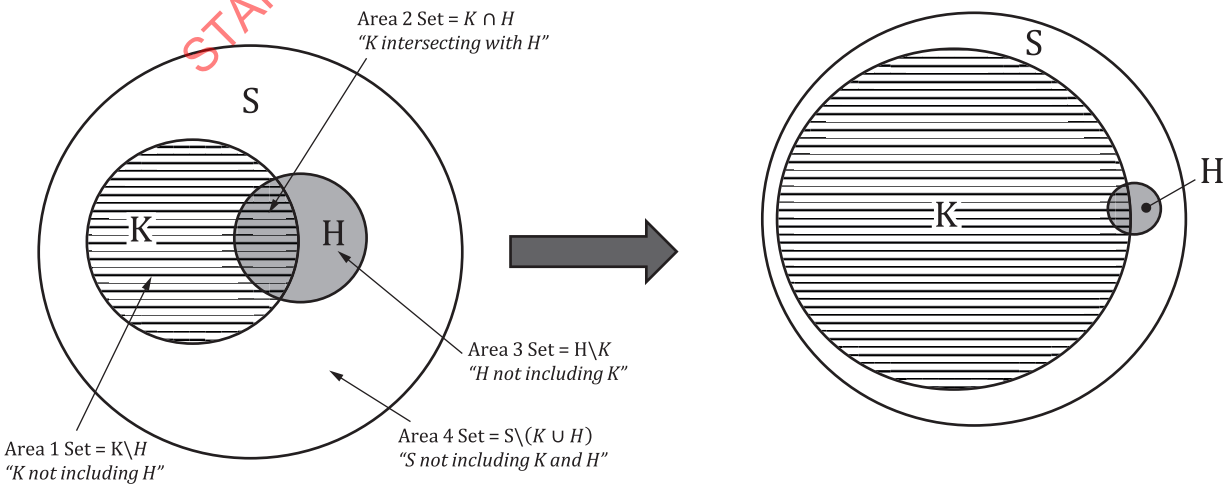
NOTE 3 The size of the areas represents the number of scenarios, not the risk due to these scenarios. However, this is just a conceptual approach of one aspect of the task since the sizes of the areas are not really measurable. The SOTIF task is to provide an argument for a sufficiently low risk of the intended functionality, for which the number of scenarios is one aspect, but not the only one. Severity of the resulting harm and likelihood of occurrence of a hazardous scenario contribute to the risk of the intended functionality but are not represented in the areas.

NOTE 4 If the usage of scenarios for certain SOTIF-related activities is not planned in the applied system development approach, this does not change the goal of SOTIF to avoid unreasonable risk.

A given use case can include known and unknown scenarios. Exploring scenarios of each use case can lead to the identification of previously unknown scenarios.

The ultimate goal of the SOTIF activities is to evaluate the potentially hazardous behaviour present in areas 2 and 3 and to provide an argument that the residual risk caused by these scenarios is sufficiently low, i.e. at or below the acceptance criteria. While the risk resulting from known scenarios in area 2 is explicitly evaluated, the risk resulting from unknown scenarios in area 3 is argued to be sufficiently small by statistics-based testing.

It is expected that the residual risk due to areas 2 and 3 will be reduced. The confidence in the achievement of the SOTIF will be increased by the growing scenario set in area 1 (see Figures 7 and 8).



Example of an initial starting point of development Goal for the SOTIF release

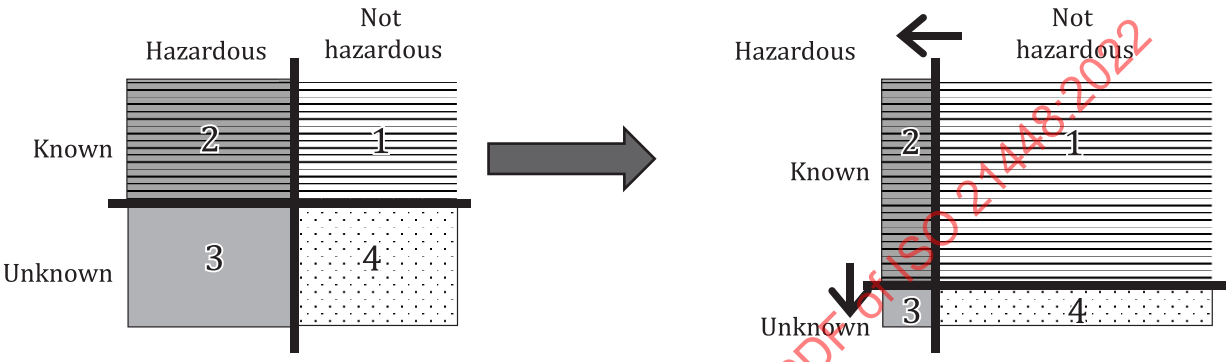
Key

represents the set of know scenarios K

represents the set of all possible scenarios S

represents the set of hazardous scenarios H

Figure 7 — Evolution of the scenario categories resulting from the ISO 21448 activities



Example of an initial starting point of development Goal for the SOTIF release

Key

known, not hazardous scenarios (area 1)

known, hazardous scenarios (area 2)

unknown, hazardous scenarios (area 3)

unknown, not hazardous scenarios (area 4)

Figure 8 — Alternative evolution of the scenario categories resulting from the ISO 21448 activities

4.2.3 Sense-Plan-Act model

Possible causes of hazardous behaviour considered in this document are closely related to the ability of the system to create a sufficiently accurate environmental model, make the right decisions and derive the correct control actions based on the environmental model and execute the control actions.

The key system elements and their interactions are represented by the "Sense-Plan-Act" model (see Figure 9). The element “Sense” executes the perception part (including localization), i.e. the creation of an environmental model based on the information received from sensing both the vehicle's external and internal environment as well as the vehicle and system states. The element “Plan” applies its goals and policies on the environmental model provided by the Sense element to derive the control actions. Finally, the element “Act” executes the control actions.

NOTE Decision algorithms are included in all elements of the Sense-Plan-Act model (e.g. classification, sensor data, fusion, situation analysis, action decision).

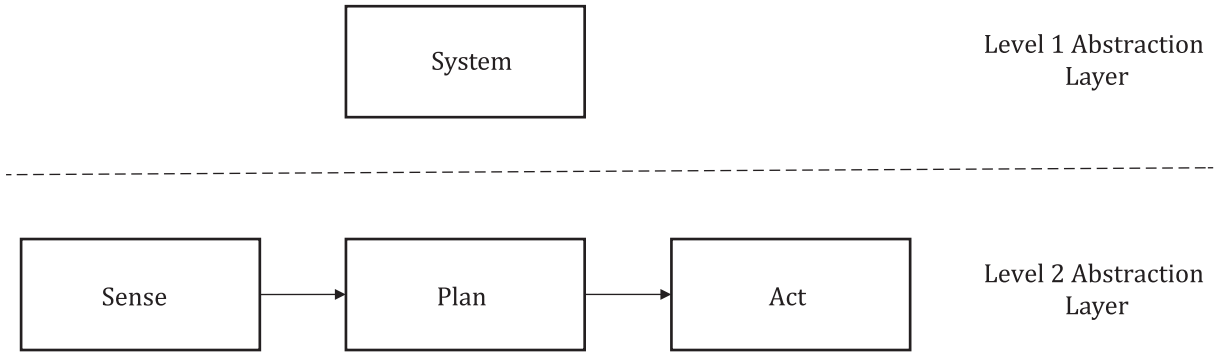


Figure 9 — Visualisation of the Sense-Plan-Act model

Based on the Sense-Plan-Act model, the selection of a capable, comprehensive system architecture can be an important consideration in achieving efficient SOTIF process so that the overall capability and corresponding activities can take place both at early stages and throughout the whole functional development lifecycle. Selecting a capable system architecture is crucial to ensure the SOTIF. Therefore, activities corresponding to the definition of the system architecture can be started at an early stage of the system development. Moreover, the system architecture is reviewed regularly along the system lifecycle and updated if necessary.

4.3 Use of this document

4.3.1 Flow chart and structure of this document

The SOTIF activities (see Figure 10) start with defining the specification and design (see Clause 5). The specification and design already include functional insufficiencies that are already known before the downstream SOTIF activities and cycles. Iterations of SOTIF activities can result in updates to the specification and design, and new previously uncovered functional insufficiencies. Each iteration starting from the specification and design relies on the specification and design being up to date.

The potentially hazardous behaviours of the intended functionality are subjected to a hazard identification and risk evaluation (see Clause 6). The identified hazardous events are evaluated regarding their risk and risk acceptance criteria are defined accordingly. If it is shown that the hazardous events do not lead to unreasonable risk, then no additional design measures are applied. Clause 6 does not consider the causes of hazardous behaviour of the intended functionality, but only their consequences for safety. Therefore, the focus is to evaluate hazardous events that could result from hazardous behaviour, and to define the acceptance criteria that are necessary to meet.

Clause 7 identifies the possible root causes for the hazardous behaviours of the intended functionality (see Figure 3) and evaluates if the risk resulting from the identified potential functional insufficiencies and triggering conditions is reasonable.

The functionality is modified (e.g. improvement of sensor capabilities, further restrictions of the ODD) to improve the SOTIF if deemed necessary as a result of the activities of Clauses 6, 7, 9, 10, 11, 12 and 13 (see Clause 8).

A verification and validation strategy is developed to provide evidence that the SOTIF-related vehicle-level residual risk is below an acceptable level and elements meet their functional requirements (see Clause 9) and the coverage over the operational design domain (ODD) is sufficient. To enable the collection of the required evidence, corresponding verification and validation test cases can be derived from this strategy and the test case coverage over the ODD is sufficiently high (see Clauses 10 and 11).

It is evaluated if the results of the SOTIF activities are sufficient to argue the achievement of the SOTIF (Clause 12).

A process to evaluate and resolve possible emerging field operation SOTIF issues is defined in the operation phase (see Clause 13).

Figure 10 describes the flow of the activities required in this document to ensure the safety of the intended functionality. The circled numbers denote the corresponding clauses within this document.

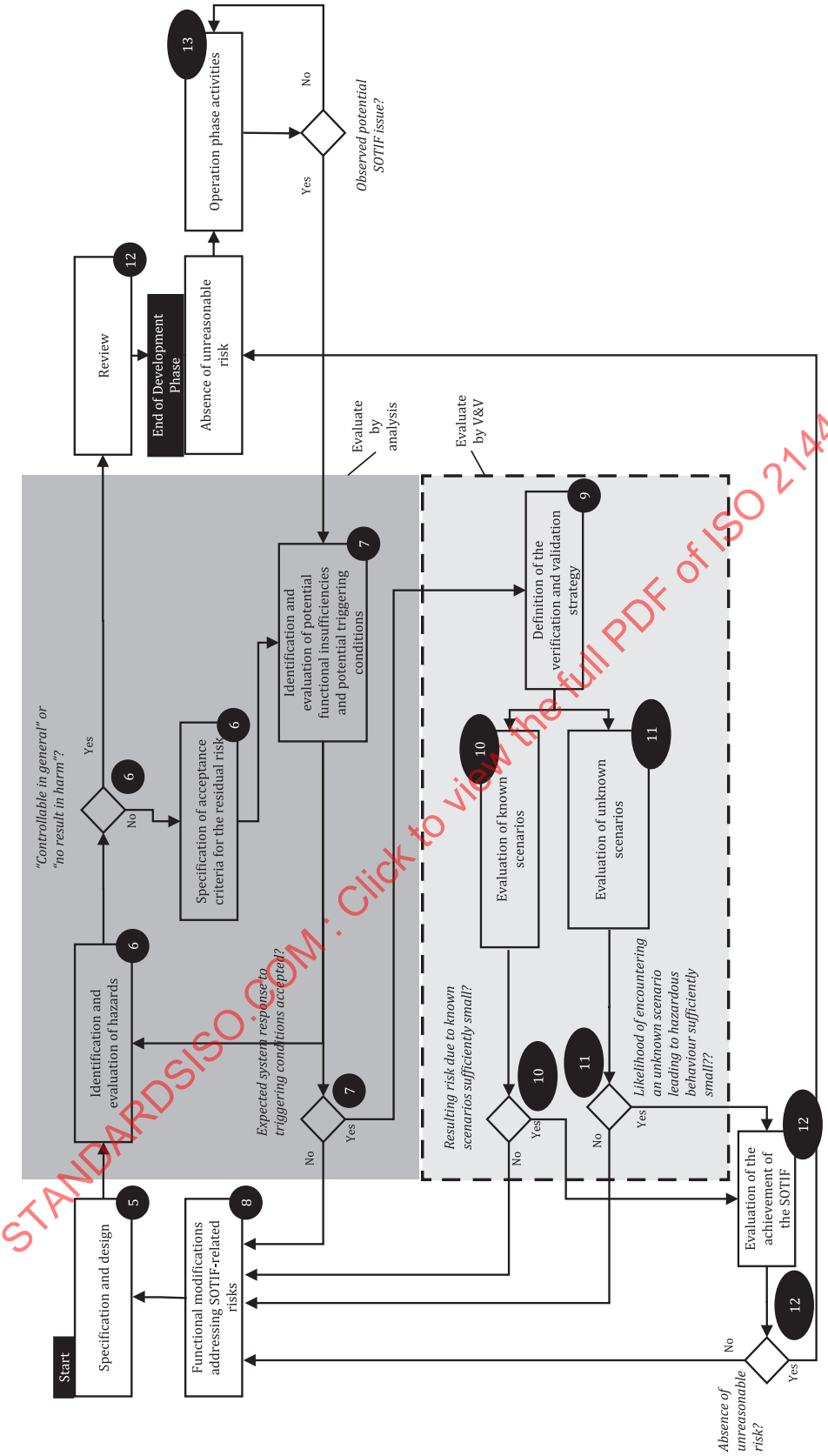


Figure 10 — Dependencies between the ISO 21448 activities

NOTE A.3 presents a simplified SOTIF application across levels of automation.

Annex A provides general guidance on the SOTIF.

Annex B provides guidance on scenario and system analysis.

Annex C provides guidance on SOTIF verification and validation.

Annex D provides guidance on specific aspects of SOTIF, like the specification of the driving policy, implication for machine learning, and considerations for maps and V2X.

4.3.2 Normative clauses

Compliance to this document is claimed by achieving the objectives listed at the beginning of the clauses and providing evidence of their achievement documented in the corresponding work products. The normative character of the objectives is expressed by the use of the key word "shall", which indicates a requirement.

NOTE A.1 gives examples of such arguments based on the Goal Structuring Notation (GSN).

4.3.3 Interpretation of tables

Some tables within this document list a collection of methods and measures in order to achieve a certain development target. The entries are meant to illustrate possible methods and measures and the table entries are not exhaustive. Other equivalent methods and measures can be applied. The intention of the tables is to support the development team in their selection of one or more appropriate measures and methods.

NOTE The choice of an appropriate set of methods can depend on various factors like complexity or exposure of the hazardous event.

4.4 Management of SOTIF activities and supporting processes

4.4.1 Quality management, systems engineering and functional safety

In order to develop a safe product, rigorous engineering and quality management processes are essential. These are already addressed in other standards, like IATF 16949, the ISO 26262 series and ISO/IEC/IEEE 15288. This document focuses only on the SOTIF-specific aspects of these processes.

NOTE 1 During product development, activities specified in this document and the ISO 26262 series can be carried out in parallel. Implemented measures in general can have an impact on SOTIF as well as functional safety and are evaluated by both disciplines. 6.1 provides practical guidance for implementing ISO 26262 and SOTIF in parallel.

For management activities and supporting processes ISO 26262-2, ISO 26262-7 and ISO 26262-8 can be extended to the SOTIF activities. Special attention for requirements cascading and traceability is further described in 5.3 and 10.2.

For SOTIF-related activities a set of methods and measures are selected as follows.

— The SOTIF process (see Figure 10) starts with defining the specification and design of the system and its architecture (see Clause 5).

— The potentially hazardous behaviours of the intended functionality are subjected to a hazard identification and risk evaluation (see Clause 6) that identifies hazards and their corresponding hazardous events. If it is shown that these hazardous events do not lead to unreasonable risk of harm, then no additional design measures are applied.

NOTE 2 Clause 6 does not consider the causes of hazardous behaviour of the intended functionality, but only their consequences for safety. Therefore, the focus is to evaluate hazardous events that could result from hazardous behaviour, and to define the acceptance criteria to meet.

— Clause 7 identifies the possible root causes for the hazardous behaviours of the intended functionality (see Figure 1) and estimates if the risk resulting from the identified potential functional insufficiencies and triggering conditions is reasonable.

— The functionality is modified (e.g. improvement of sensor capabilities, further restrictions of the ODD) to improve the SOTIF if deemed necessary as a result of the activities of Clauses 6, 7, 10, 11, 12 and 13 (see Clause 8).

— A verification and validation strategy is developed to provide evidence that the SOTIF-related vehicle-level residual risk is below an acceptable level and components meet their functional requirements (see Clause 9). Corresponding verification and validation test cases can be derived from this strategy in order to evaluate if the resulting risk is sufficiently small (see Clauses 10 and 11).

— The residual risk is evaluated (see Clause 12) considering the results from previous activities.

— A process to identify and resolve possible emerging field operation SOTIF issues is defined in the development phase and implemented during the operation phase (see Clause 13).

NOTE 3 Further explanations regarding the interactions between functional safety according to the ISO 26262:2018 series and this document can be found in A.2.

4.4.2 Distributed SOTIF development activities

In case of a distributed product development, a development interface agreement (DIA) is defined between all involved parties. The goal of the DIA is to confirm, in the early stages of a project, all responsibilities of the SOTIF activities and that adequate technical information will be exchanged between the development parties.

IATF 16949 provides a base process framework, that can also be considered within this context. This sub-clause focuses on how to extend a DIA to distributed SOTIF development and operation. The ISO 26262:2018 series provides the framework of a DIA and supply agreement regarding functional safety aspects. In order to apply this framework to SOTIF, tailoring can be applied by adding the responsibilities of each party related to SOTIF development and operation. The responsibilities of each party are considered and agreed upon to plan and perform the entire relevant SOTIF activities of Clauses 5 to 13. The information and work products that will be shared are specified. These activities can be done using processes that are described in ISO 26262-8:2018, 5.4.1, 5.4.2, 5.4.3, 5.4.4 and 5.4.6 and tailored for SOTIF activities. The documentation format is agreed at the beginning of the development project.

4.4.3 SOTIF-related element out of context

To achieve SOTIF it is essential that the interfaces between different systems [hardware (HW) and software (SW)] are described. In order to ensure that the integrated system is safe within the specified ODD, the boundaries of each system (e.g. a stand-alone sensing system) are carefully evaluated. Because environmental factors (e.g. ODD, scenario) are essential issues of SOTIF development, systems and their elements have different concerns depending on the hierarchical layers. As far as the development of these systems and elements are considered, they can be categorized in one of the following three types.

a) In-context development: the complete system is developed using all the SOTIF activities following a V model. For distributed parties who develop the system and its elements, requirements are determined including specification and design (see Clause 5) and other activities (see Clauses 6, 7, 8, 9, 10, 11, 12 and 13) depending on the role assignment. In ISO 26262 terms, this development would be considered as “in-context” development.

b) SOTIF-related element out of context: for these elements assumptions can be made regarding their use within the whole system and their contribution to the intended functionality. As such it is possible to make assumptions about the SOTIF-related output insufficiencies and their allowed target rate of occurrence. These assumptions are documented and used as inputs for the subsequent development of these elements. The SOTIF activities provide evidence that the corresponding target rates are met. For a SOTIF-related element out of context, the identified triggering conditions of the element and their resulting output insufficiencies are documented as well as their assumptions of use. When integrating this SOTIF-related element out of context, the

validity of the assumptions is established by SOTIF activities in the context of whole vehicle-level functionalities (see ISO 26262-10:2018, Clause 9).

c) Non-specific SOTIF-related development: the functionality of these elements can contribute in too many ways to the intended functionality so that it is practically not feasible to estimate the SOTIF-related requirements a priori without the context in which these elements will be used.

EXAMPLE The requirements allocated to graphical processing units (GPUs) will depend on the system context and the SW running on these GPUs.

5 Specification and design

5.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) the specification and design shall contain information sufficient to conduct the SOTIF-related activities; and

b) the specification and design shall be updated as required after each iteration of the SOTIF-related activities (see Figure 10).

5.2 Specification of the functionality and considerations for the design

The specification and design can include various aspects as listed in this subclause. Some aspects are relevant only for a specific automation level or a specific implementation. In addition, some aspects are relevant for the specification of the functionality on the vehicle level and some on the element level.

Aspects for consideration (where applicable) include, but are not limited to the following:

— the description of the intended functionality and the functionalities of the supporting subsystems and components including:
  — the ODD;
  — the level and details of the automated driving function control authority over vehicle dynamics;
  — the vehicle-level SOTIF strategy;
  — the use cases in which the function can be active or inactive, and the transitions between them; and
  — the description of decision-making logic (e.g. path planning, driving policy – see D.1);
— the design of the relevant system and its elements implementing the intended functionality;
— the performance targets of the installed sensors, controllers, actuators or other inputs and components (e.g. maps – see D.3) enabling the intended functionality;

  NOTE 1 Performance targets of an automated driving system, for example, include the detection and response to critical objects and events (e.g. pedestrians, vehicles, bicycles, motorcycles and traffic signs) within the ODD.

— the dependencies of the intended functionality on, and interactions or interfaces with:
  — the driver;
  — the driver interface (e.g. HMI), and how the interface is used to mitigate known reasonably foreseeable misuses;
  — the remote/back office operator;

  - the passengers, pedestrians, cyclists and other road users;
  - the relevant environmental conditions;
  - the road infrastructure and road furniture;
  - the data exchange to and from the cloud, inter-vehicle or other communication infrastructures (e.g. V2X/X2V – see D.4) and in-service telematics involving diagnostics and parameter updates;
  - the remote flashing of software updates; and
  - the other functions of the vehicle that might interfere with the intended functionality, including the exchange of information, and the corresponding assumptions of use;
- the reasonably foreseeable misuse (direct and indirect);
- the potential performance insufficiencies, identified triggering conditions and countermeasures of the system and its elements;

  NOTE 2 Some potential performance insufficiencies and risks identified during SOTIF activities can be accepted and have no "countermeasures". In such cases these can be documented as part of the specification and design.

- the system and vehicle architectures implementing the intended functionality;
- the warning and degradation concept:
  - the warning strategies;
  - the DDT fallback: takeover/fallback conditions and schemes for transitioning control from the automated driving system to the driver or another system within their respective use cases;
  - the minimal risk condition schemes (e.g. autonomously exit lane and park, stop in path, fallback-ready user); and
  - the driver monitoring system and its operational effect on the fallback strategy;
- the procedures supporting data collection and monitoring during and after development of the intended functionality:
  - the objectives and requirements for the data collection;
  - the architecture, implementation and mechanisms supporting the required data collection before SOTIF release; and
  - the requirements, design and mechanisms that support data collection during the operation phase for SOTIF analysis (see 13.5), including possible cloud based, "Over The Air", or RF communication technologies;
- the mechanism, design and requirements that support risk mitigation abilities during operation.

5.3 System design and architecture considerations

The specification and design provide an adequate understanding of the system, its elements, its functionality and the performance targets, so that the activities in subsequent phases can be performed. This includes an exhaustive list of known functional insufficiencies, related triggering conditions and, where applicable, their countermeasures. Some potential functional insufficiencies, triggering conditions and countermeasures are known and documented before the SOTIF-related process begins while others are revealed as a result of the SOTIF activities. The system is designed such that countermeasures are implemented to mitigate the effect of known functional insufficiencies on the overall system.

Each iteration of the SOTIF-related activity (see Figure 10) can result in engineering activities which can lead to updates in the specification and design at any relevant level. Each iteration relies on the specification and design being updated at any relevant level, such that it reflects all information discovered in previous iterations.

Cooperation among development parties (OEM, Tier 1, Tier N) is necessary to discover potential functional insufficiencies of the integrated system, component or element, and to develop countermeasures to these insufficiencies during the development phases (see 4.4). Relevant sections of design and specification are communicated to lower-level system and component developers. Assumptions of use, foreseeable misuse and potential performance insufficiencies are communicated from one tier to the next hierarchical levels, up to and including the OEM, after each development cycle/iteration.

As the SOTIF activities identify new functional insufficiencies and triggering conditions (see Clause 7), and measures to improve the SOTIF are defined (see Clause 8), the specification and design is updated as part of each development cycle as seen in Figure 10.

SOTIF work products are linked with the specification and design if they impact the specification and design (as defined in 5.2), including pre-existing relevant content. This ensures that all information from previous iterations is captured, and that the specification is ready for the next iteration cycle.

NOTE Traceability and completeness of the specification and design (work products 5.5) can be demonstrated by linking to SOTIF measures (work products 8.5) which can be further linked with:

— the relevant design document(s);

— the work products from:

  — Clause 6 - risk evaluation of hazardous behaviours (e.g. to achieve an S=0, C=0, or to obtain less constraining acceptance criteria);

  — Clause 7 - evaluation of the system's response to the identified triggering conditions (e.g. link to the analysis of a triggering condition showing unacceptable risk);

  — Clauses 9 and 10 - verification and validation results for known hazardous scenarios (e.g. link to a verification test report showing unacceptable performance with respect to the requirements);

  — Clauses 9 and 11 - validation results for unknown hazardous scenarios (e.g. link to a validation test report showing unacceptable performance with respect to a hazardous scenario or the validation targets);

  — Clause 12 - SOTIF release argument (e.g. link to report documenting reasons for rejecting release request); and

  — Clause 13 - field monitoring process (e.g. link to report documenting new hazardous scenario discovered during field monitoring);

The SOTIF technical assumptions related to risk evaluation in Clauses 6 (6.4) and 7 (7.4) are not necessarily associated with SOTIF measures in Clause 8 (8.3) but can still be traced to the specification and design. Design tools offering model-based design and supporting traceability between different model artefacts (requirements, components, interfaces, analysis, test cases and results) can support this process.

5.4 Performance insufficiencies and countermeasures considerations

The design includes considerations on potential performance insufficiencies that can result from an element output value which can potentially lead to hazardous behaviour at the vehicle level. A non-exhaustive list of examples of potential performance insufficiencies includes:

— insufficient classification,

— insufficient measurements,

— insufficient tracking,

— insufficient target selection,

— insufficient kinematic estimation,

— false positive detections (e.g. ghosts, phantom objects),

— false negative detections, and

— driving policy level limitations such as considering occluded areas.

Guidance on possible methods to identify functional insufficiencies and the corresponding vehicle-level hazardous behaviour can be found in B.3. Functional insufficiencies are most relevant when the system operates within its specified ODD. The way the system detects leaving its specified ODD, and how it operates during transitions, is relevant to support the complete analysis.

The system development is based on the assumptions made about the performance insufficiencies in the design. Measures are implemented to cope with these performance insufficiencies to ensure the SOTIF. The design and measures, integrated into the specification and design, decrease the residual risk and increase overall robustness (see Figures 5 and 6).

NOTE 1 Methods and measures to discover potential functional insufficiencies and their triggering conditions are detailed in Clause 7.

NOTE 2 Methods and measures to address functional insufficiencies such as (but not limited to) redundancy, diversity, complementary elements are described in Clause 8.

NOTE 3 The SOTIF content of the specification and design is verified as elaborated in Clause 10.

The following are examples of performance insufficiencies and possible countermeasures. This is content that is included in the specification and design document(s):

EXAMPLE 1 A highway lane boundary detection algorithm, for functions such as lane keeping, might incorrectly determine the lane due to debris on the roadway. However, lane excursions that result in a collision can be mitigated by other automated driving functionalities such as: using a high-definition map and localization to confirm the lane, rationalizing the vehicle trajectory with the trajectory of preceding vehicles, collision avoidance algorithms maintaining separation with other vehicles even if this implies leaving the perceived lane, etc.

EXAMPLE 2 An object-detection algorithm detects a person on a skateboard as a pedestrian but rejects the object due to its speed being implausible. A collision with the skateboarder can be mitigated, in this case, by a system with an abstraction between the object-detection algorithm and the sensing and processing algorithms and using other different plausibility checks.

EXAMPLE 3 A pedestrian crossing drawn as a three-dimensional optical illusion (see Figure 11) is used to alert drivers in some areas. The image is drawn on the road specifically to fool the human perception and can also fool a vision system into detecting a non-existent object. In this case, an optical flow-based analysis mechanism can prevent false braking. Optical flow analyses as well as radar-based environment recognition are alternative countermeasures for such cases that result from classification limitations.

Figure 11 — Example of optical illusion drawing that could fool a vision system

EXAMPLE 4 Using an automated parking system with an object protruding from the open trunk can lead to a hazardous event. A countermeasure in the system design might only permit automatic parking when the trunk is closed.

5.5 Work products

The work product is the specification and design, fulfilling objectives 5.1 a) and 5.1 b).

NOTE 1 The specification and design can be split into or linked to several documents such as: requirement specifications, functional specifications and design specifications of the SOTIF-related systems.

NOTE 2 The SOTIF specification of mitigation measures can be integrated into existing functional safety design documentation such as functional safety concept and/or technical safety concept.

6 Identification and evaluation of hazards

6.1 Objectives

The purpose of this clause is to achieve the following objectives.

a) The hazards arising from the intended functionality, defined at the vehicle level, shall be systematically identified.

b) The risk that arises from the hazardous behaviour of the intended functionality, and the corresponding scenarios in which the hazardous behaviour can lead to harm, shall be systematically identified and evaluated. The parameters that define the circumstances in which the behaviour of the intended functionality is considered hazardous shall be specified.

EXAMPLE Such parameters can be a speed deviation or the minimum distances to other objects.

c) The acceptance criteria for the residual risk shall be specified.

6.2 General

To achieve the objectives of this clause, the following information can be considered:

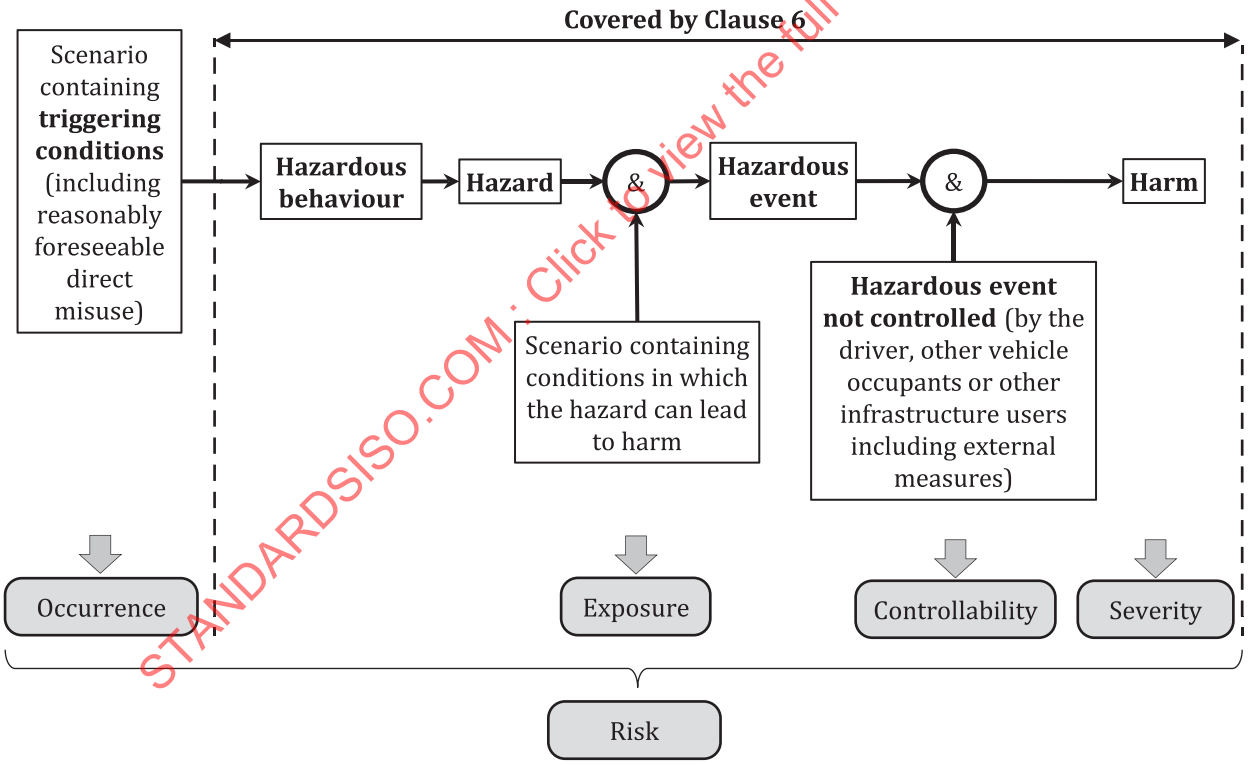
— specification and design in accordance with 5.5; and

— available data for the derivation of acceptance criteria.

6.3 Hazard identification

The hazards resulting from functional insufficiencies are determined systematically at the vehicle level. This systematic identification is primarily based on knowledge about the function and its possible deviations resulting from functional insufficiencies. This can be achieved by applying the methods specified in ISO 26262-3. An illustration of the common elements of the hazard analysis required by both the ISO 26262 series and by this subclause can be found in Figure 12. Figure 13 uses an AEB system as an example to show how the terms from Figure 12 are used. The example shows two hazards resulting from the same hazardous behaviour. The application of hazard analysis is further elaborated in A.2.5 using AEB as an example.

EXAMPLE 1 An AEB system can cause hazards originating from both hazardous behaviour of the intended functionality and malfunctioning behaviour. The hazard resulting from unintended braking, inside and outside the functional limits, can be analysed from a functional safety perspective in a hazard analysis and risk assessment. The same hazard related to unintended braking inside the functional limits is also subject to analysis of the SOTIF.



Key

→ result in

⇩ has characteristics of

Figure 12 — An illustration of common elements of hazard analysis in the ISO 26262 series and in this document

NOTE 1 Unlike in ISO 26262-3, when analysing a SOTIF-related hazard, no automotive safety integrity level (ASIL) is determined for a hazardous event. However, the parameters severity (S), exposure (E) and controllability (C) can be used to adjust the validation effort.

NOTE 2 The occurrence reflects the probability of encountering triggering conditions during the operating phase of the functionality.

There is an important difference between the occurrence of a triggering condition and the exposure to a scenario in which the hazard can lead to harm. In general, triggering conditions are not independent from scenarios. Therefore, in order to use the exposure to a scenario within an argument for risk reduction, the statistical dependence between the probability of being in a scenario and the probability of encountering a triggering condition is taken into account in the evaluation.

EXAMPLE 2 No statistical independence can be assumed for a triggering condition of a highway pilot where the scenario is driving on a highway.

In some specific cases, statistical independence can be assumed as it is shown in Figure 13.

The C parameter can be used to evaluate whether SOTIF-related hazards are controllable (see 10.6 and Table 10). Studies or assumptions about the reaction of road participants can be used to support controllability ratings.

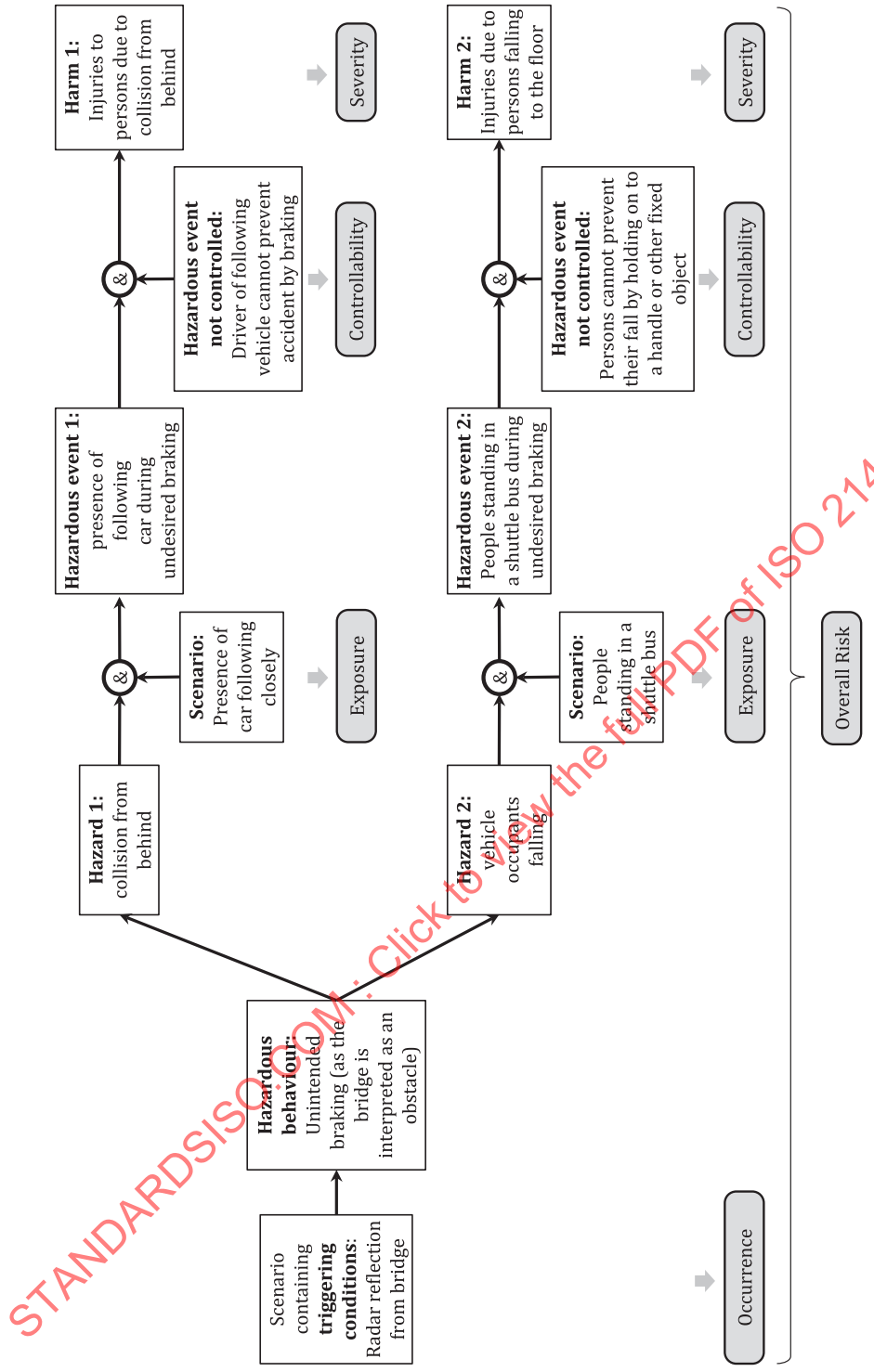


Figure 13 — An AEB example using terms from Figure 12

NOTE 3 The example in Figure 13 shows that the resulting risk can be assessed on two levels: first the risk relating to a specific hazard in a given scenario, and second the overall risk that is related to the hazardous behaviour and includes the evaluation of several hazards and the corresponding scenarios.

In addition to the systematic identification resulting from possible function deviations, further hazards can be identified by considering the interaction of the driver or user with the system including

reasonably foreseeable misuse. Reasonably foreseeable misuse is differentiated by its causal link with the hazard. A direct misuse of the intended functionality results in a triggering condition while an indirect misuse of the intended functionality causes a reduction in controllability or an increase in severity of a hazardous event resulting from a hazardous behaviour (e.g. an inattentive driver or a driver misunderstanding the limitations of a function).

The identification of reasonably foreseeable indirect misuse, and the analysis of its effects, are covered by Clause 7.

NOTE 4 7.3.4 and B.1 provide general guidance for the analysis of reasonably foreseeable misuse.

6.4 Risk evaluation

The risk evaluation aims to evaluate the risk due to hazardous behaviour in given scenarios; this helps to specify the acceptance criteria of a SOTIF-related risk.

NOTE 1 The hazardous behaviour resulting from a functional insufficiency on the vehicle level, if any, is part of this evaluation.

The severity of harm, and the controllability of hazardous events, can be estimated using the method described in ISO 26262-3:2018, Clause 6. Despite sharing the analysis method, the observed outcome and the estimated parameters for a specific hazard can be different for the SOTIF analysis.

NOTE 2 ISO 26262-3 introduces classes for controllability, severity, and exposure. In the context of Clause 6, it is only relevant whether a hazardous event is or is not controllable in general, or, does or does not result in harm. Exposure is not a determining parameter for risk evaluation in Clause 6. As the risk is evaluated in scenarios, their selection already implies that the exposure to them is SOTIF-related, otherwise they would not be considered for analysis.

NOTE 3 The exposure to specific scenarios can be considered for the specification of validation targets (see Clause 9).

EXAMPLE 1 The severity of a rear collision with the host vehicle, caused by automated emergency braking, can be reduced by limiting the brake intervention magnitude. The magnitude limit can be seen as a safety measure to increase controllability, or as a functional modification to the intended behaviour. When analysing the hazard, the limit is considered as part of the intended behaviour; in contrast, failures relating to the implementation of the limit would be the subject of other safety standards, such as the ISO 26262 series.

The severity and controllability of the hazardous event are considered to determine if the resulting risk is unreasonable in a given scenario. The severity and controllability evaluation considers the functional specification (according to the specification and design resulting from Clause 5). The absence of unreasonable risk is established if the controllability is rated as "controllable in general" (i.e. C=0) or the severity is rated as "no resulting harm" (i.e. S=0). In all other cases a hazardous event is considered SOTIF-related. The corresponding hazardous behaviour is described using measurable parameters like speed deviations and minimum distances to other objects. The controllability evaluation includes “no reaction”, or “delayed reaction” by the involved persons to control the hazard, e.g. resulting from reasonably foreseeable indirect misuse. This evaluation can also consider external measures.

EXAMPLE 2 An environmental condition that is not handled by an advanced driver assistance system (ADAS) in a safe manner and therefore, requires the driver to resume control can be considered for hazardous event classification.

A delayed or inappropriate reaction by the driver, including the time necessary for the driver to achieve sufficient situational awareness and recovery, can impact the controllability evaluation and is a topic of the SOTIF-related analysis.

If after a functional modification (see Figure 10) a hazardous event is judged as S=0 or C=0 then the hazard has been sufficiently addressed.

EXAMPLE 3 Table 3 gives an example of the evaluation of a potential consequence of a SOTIF-related hazardous event for an AEB system.

Table 3 — Example of a hazardous event

Hazardous behaviour	Potential consequence	Severity		Controllability		unreasonable risk?
		Rating	Note	Rating	Note	
Unintended AEB activation at x m/s^2 for y seconds while operating on a highway	Rear collision with following vehicle	S > 0	Effective impact speed: $v \geq x$ km/h	C > 0	The following vehicle might not be able to brake to avoid collision.	Yes

6.5 Specification of acceptance criteria for the residual risk

If the risk parameters are not evaluated as S=0 or C=0, then acceptance criteria are specified for the risks associated with the hazardous behaviour and the activities continue with Clause 7.

The argument for the S=0 or C=0 classification is reviewed as part of the SOTIF process and includes the review of the evidence for the classification (e.g. test or analysis results).

Acceptance criteria consider:

— applicable governmental and industry regulations;

— whether a function is new or already established in the market;

— whether the risk is unreasonable for the people who might be exposed to the risk (e.g. a vehicle owner, the operator, a pedestrian or a passenger in an automated public transport system);

— acceptance criteria of already established functions; and

— the performance of a driver who acts in an exemplary fashion.

EXAMPLE 1 Such acceptance criteria could be a maximum number of accidents per hour. An appropriate verification and validation strategy is defined in Clause 9 and is based on the specified acceptance criteria.

Approaches that can be considered when specifying acceptance criteria include:

— the available traffic data for the target market (e.g. accident statistics, traffic analyses) (see C.2.2.4); and

— pre-existing criteria from similar functions operating in the field.

EXAMPLE 2 Number of false positive events per x km produced by a similar collision warning system that is in series production (similar test distribution).

Appropriate quantitative acceptance criteria can be chosen provided that a valid rationale is given. The overall rationale can be based on one, or a combination of several, of the following individual rationales.

— A risk tolerability principle, such as the GAMAB (Globalement au moins aussi bon) or GAME (Globalement au moins équivalent); both French terms having the meaning "globally at least as good". Following this principle, the residual risk (with respect to safety) of any new system is not higher than that of existing systems having comparable functionality or hazards.

— A positive risk balance. The application of such a risk tolerability principle to the overall residual risk, that considers all hazards of the new system, allows relevant risk trade-offs to be made. A system can be released even though the residual risk for a given hazard has increased, provided that this is compensated for by counterbalancing reductions in one or more other residual risks.

— The ALARP principle. The ALARP risk management framework can provide a useful risk reduction principle, particularly regarding the development and introduction of novel technologies where "good practice" does not currently exist. By acknowledging that a state of zero risk is not possible, the ALARP principle aims to reduce risk to a level considered "reasonably practicable" by weighing the risk against the effort needed to further reduce it.

— The MEM (minimal endogenous mortality) principle. The MEM principle is based on the idea that the introduction of a technical system should not significantly increase the death rate in society. Quantitative acceptance criteria for the probability of death caused by a technological system are derived from the minimum probability of death from natural causes.

NOTE 1 A rationale in the context of this document can only include SOTIF-related risks and does not include risks from other safety domains (e.g. electrical safety).

NOTE 2 C.2 and C.6 give examples for defining and evaluating acceptance criteria and validation targets.

NOTE 3 A description of GAMAB, ALARP and MEM can be found in EN 50126-2:2017, A.1 (RAMS)[4].

NOTE 4 A valid rationale can be based on risk across a fleet or risk associated with an individual vehicle. Even if a fleet has a very low probability to encounter a triggering condition as part of a scenario, the response of the system can be unacceptable if the probability of facing such a scenario is high for a given individual vehicle.

6.6 Work products

6.6.1 Hazards at the vehicle level, fulfilling objective 6.1 a)

6.6.2 Risk evaluation of hazardous behaviours, fulfilling objective 6.1 b)

6.6.3 Acceptance criteria, fulfilling objective 6.1 c)

7 Identification and evaluation of potential functional insufficiencies and potential triggering conditions

7.1 Objectives

The purpose of this clause is to achieve the following objectives.

a) Potential insufficiencies of specification, potential performance insufficiencies and potential triggering conditions including reasonably foreseeable direct misuse shall be identified and those leading to a hazardous behaviour shall be determined.

b) The response of the system shall be evaluated for SOTIF acceptability.

NOTE 1 This includes the identification of functional insufficiencies and related triggering conditions relevant in the context of reasonably foreseeable direct and indirect misuses.

NOTE 2 This activity considers the potential insufficiencies of specification of the intended functionality at the vehicle level as well as the potential insufficiencies of specification or potential performance insufficiencies of E/E elements of the system.

7.2 General

To achieve the objectives of this clause, the following information can be considered:

— specification and design, in accordance with 5.5;

— hazards at the vehicle level, in accordance with 6.6.1;

— risk evaluation of hazardous behaviours including identified reasonably foreseeable indirect misuses, in accordance with 6.6.2;

— acceptance criteria, in accordance with 6.6.3; and

— known potential functional insufficiencies of the system and its elements and known potential triggering conditions (including reasonably foreseeable direct misuse) that could lead to a hazardous behaviour based on external information or lessons learnt (e.g. 13.5).

7.3 Analysis of potential functional insufficiencies and triggering conditions

7.3.1 General

The potential functional insufficiencies and triggering conditions are systematically analysed. This analysis can consider field experience and knowledge gained from similar projects or experts.

This analysis can be conducted in parallel, starting from both:

— the known potential insufficiencies of specification and performance insufficiencies to determine scenarios (containing triggering conditions) leading to identified hazardous behaviour, and

— the identified environmental conditions and reasonably foreseeable misuse to determine potential insufficiencies of the specification and performance insufficiencies.

NOTE 1 Further details on SOTIF analysis techniques are given in Annex B. Also, ISO 34502 [5] can be referred to.

NOTE 2 The analysis can be supported by inductive, deductive or exploratory methods.

NOTE 3 The analysis can be performed qualitatively, quantitatively, or both.

NOTE 4 Quantitative targets can be defined down to the element level, derived from acceptance criteria or validation targets at the vehicle level.

NOTE 5 Proper abstraction (e.g. generation and use of equivalence classes or subsets) of all relevant use case parameters can be helpful to cope with a large number of use case combinations.

NOTE 6 Traffic statistics can be used to focus on plausible use cases that could lead to potentially hazardous behaviour.

NOTE 7 This analysis can be supported by simulations, e.g. using Monte-Carlo methods.

An appropriate combination of methods to identify and to assess the potential insufficiencies of specification, performance insufficiencies, output insufficiencies and triggering conditions can be applied as listed by Table 4.

Table 4 — Analysis methods of potential functional insufficiencies and triggering conditions

Methods	
A	Analysis of requirements

[a] It includes analysis of the ODD boundaries.

[b] For example, STATS19 (UK)[6], GIDAS (Germany)[7], GES (US)[8], CARE[9], IGLAD[10].

[c] Several performance insufficiencies or insufficiencies of specification can be activated by a single triggering condition (e.g. heavy rain can impact the performance of different sensors such as radar and camera).

[d] This considers analysis of comparable systems in the market, predecessor systems and projects, and customer claims.

[e] This considers technological limitations (e.g. angular resolution due to camera imager, radar antenna design limitation or lack of environmental isolation such as water sealing and vibration) as well as technical limitations due to mounting (e.g. blind areas resulting from sensor not covering the entire 360° visual field around the vehicle).

[f] For example, a camera lens that becomes dull due to ageing effects within the specified limits.

[g] For example, vehicle-to-vehicle, vehicle-to-infrastructure, over-the-air maps.

[h] For example, based on analysis of records coming from Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR).

[i] The analysis methods are listed in Table 5.

Table 4 *(continued)*

Methods	
B	Analysis of the ODD, use cases and scenarios [a]
C	Analysis of accident statistics [b]
D	Analysis of boundary values
E	Analysis of equivalence classes
F	Analysis of functional dependencies
G	Analysis of common triggering conditions [c]
H	Analysis of potential triggering conditions from field experience and lessons learnt [d]
I	Analysis of system architecture (including redundancies)
J	Analysis of design of the sensors and potential technology limitations [e]
K	Analysis of algorithms and their output or decisions
L	Analysis of system ageing [f]
M	Analysis of possible environmental changes over vehicle operational lifetime (e.g. interference)
N	Analysis of external and internal interfaces [g]
O	Analysis of design of the actuators and potential limitations
P	Analysis of accident scenarios [h]
Q	Analysis of reasonably foreseeable misuse [i]

[a] It includes analysis of the ODD boundaries.

[b] For example, STATS19 (UK)[6], GIDAS (Germany)[7], GES (US)[8], CARE[9], IGLAD[10].

[c] Several performance insufficiencies or insufficiencies of specification can be activated by a single triggering condition (e.g. heavy rain can impact the performance of different sensors such as radar and camera).

[d] This considers analysis of comparable systems in the market, predecessor systems and projects, and customer claims.

[e] This considers technological limitations (e.g. angular resolution due to camera imager, radar antenna design limitation or lack of environmental isolation such as water sealing and vibration) as well as technical limitations due to mounting (e.g. blind areas resulting from sensor not covering the entire 360° visual field around the vehicle).

[f] For example, a camera lens that becomes dull due to ageing effects within the specified limits.

[g] For example, vehicle-to-vehicle, vehicle-to-infrastructure, over-the-air maps.

[h] For example, based on analysis of records coming from Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR).

[i] The analysis methods are listed in Table 5.

NOTE 8 Safety analysis methods can be adapted to identify and evaluate potential functional insufficiencies and triggering conditions and their influence on the hazards (e.g. Cause Tree Analysis, Event Tree Analysis (ETA), inductive SOTIF analysis or Hazard and Operability Analysis (HAZOP)). B.3 provides examples of adaptation of safety analysis methods.

Depending on the system architecture, potential functional insufficiencies of an element can be classified into:

— single-point functional insufficiencies; or

— multiple-point functional insufficiencies.

This classification can help determine the adequate functional modification to achieve the SOTIF (see Clause 8). It can be used to derive requirements to the element level necessary to achieve the SOTIF at the vehicle level (see Clause 5).

EXAMPLE 1 Given a SOTIF specified acceptance criteria to be achieved at the vehicle level, performance targets can be allocated to different contributing elements, for example as shown in Figure 14. Each sensor can be allocated less constrictive performance targets (e.g. false positive detection rate) compared to a single sensor system.

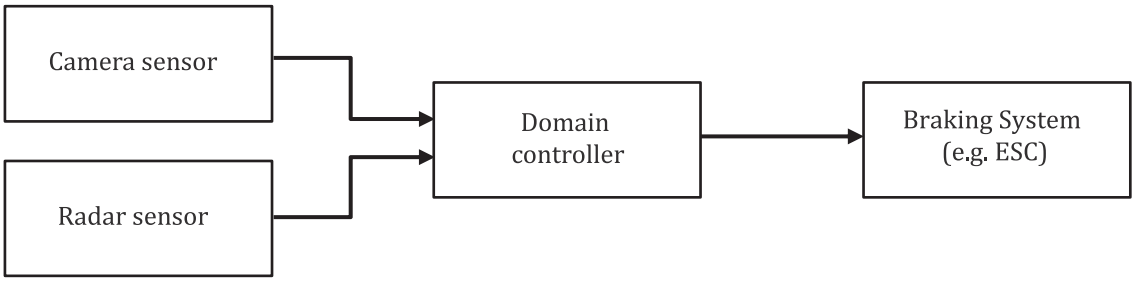
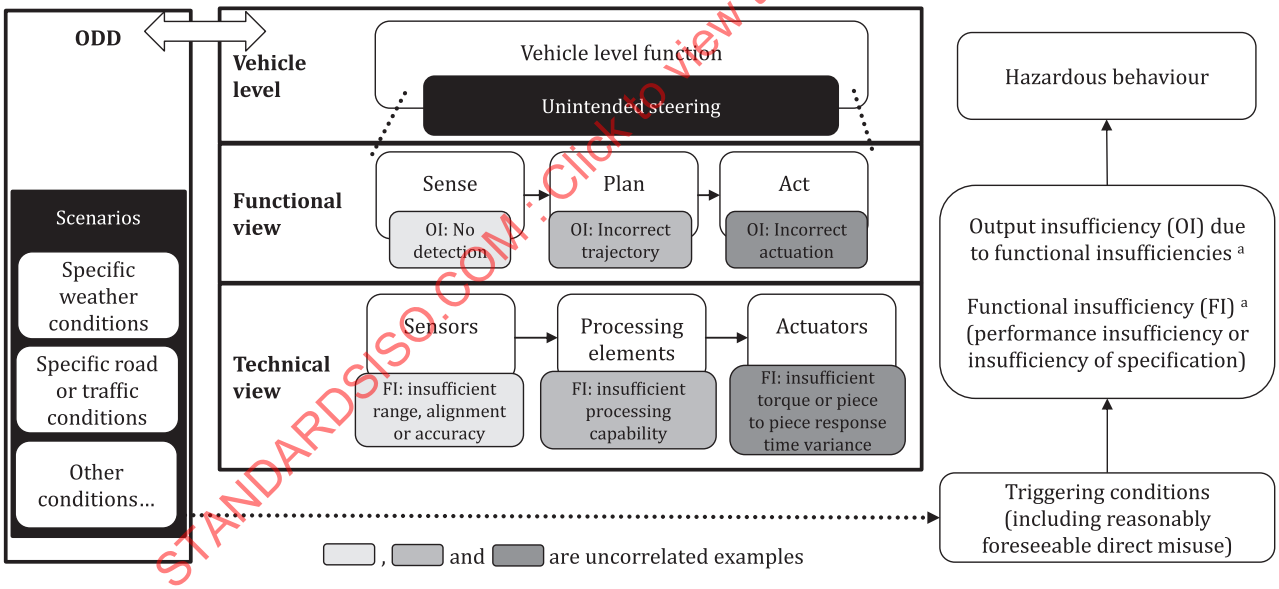


Figure 14 — Example of system architecture with the fusion of two diverse sensors

The classification can also be used during the definition of the validation strategy, where the validation targets for multiple-point functional insufficiencies can be reduced subject to independence considerations (see Clause 9 and C.6.3).

There can be multiple triggering conditions for a given performance insufficiency or insufficiency of the specification that lead to a hazardous behaviour. Additionally, known environmental conditions and reasonably foreseeable misuse can activate several vehicle or element level performance insufficiencies or insufficiencies of specification. Traceability is established and maintained between the hazardous behaviours, the triggering conditions and the potential performance insufficiencies or insufficiencies of specification on the vehicle or element level.

An illustration and an example of links between hazard, triggering conditions and the potential performance insufficiencies or insufficiencies of specification on the vehicle or element level can be found in Figure 15.



a Functional insufficiencies (as design properties) can exist within all viewpoints and on all abstraction layers.

Figure 15 — Illustration of links between potential functional insufficiencies and triggering conditions

In the following subclauses, planning algorithms, sensors and actuators are handled separately to allow a more structured presentation. If beneficial, the potential functional insufficiencies and triggering conditions in the sensors and actuators list can also be used for the planning algorithm analysis and vice versa.

7.3.2 Potential functional insufficiencies and triggering conditions related to planning algorithms

The analysis can consider the following categories, among others:

— environment and location;

— road infrastructure;

— urban or rural infrastructure;

— highway infrastructure;

— driver or user behaviour (including reasonably foreseeable misuse);

— potential behaviour of other drivers or road users;

— driving scenario (e.g. a construction site, an accident, a traffic jam with emergency corridor, vehicle driving in the wrong direction);

— known planning algorithm limitation (e.g. inability to handle possible scenarios, or non-deterministic behaviour);

— known insufficiencies of the specification of machine learning;

— known insufficiencies of the measurement data for machine learning; and

— known functional insufficiencies and functional improvements.

7.3.3 Potential functional insufficiencies and triggering conditions related to sensors and actuators

The analysis can consider the following categories, among others:

— the ODD;

— weather conditions;

— mechanical disturbance (e.g. noisy sensor output resulting from vibration due to location of sensor on the vehicle);

— dirt on sensors;

— electromagnetic interference (EMI);

— interference from other vehicles or other sources (e.g. radar or lidar);

— acoustic disturbance;

— glare;

— poor-quality reflection;

— accuracy;

— range;

— response time;

— performance impact due to durability, wear, ageing;

— authority capability (applicable to actuators, e.g. maximum applicable braking pressure for a hydraulic braking system by the intended functionality);

— multi-sensor data fusion; and

— alignment and installation of sensors.

EXAMPLE 1 Rain and snow can affect radar performance.

EXAMPLE 2 Rising sun in the front of the vehicle can affect the performance of a video camera.

EXAMPLE 3 A heavy woollen coat on a pedestrian can affect the performance of ultrasonic sensors.

EXAMPLE 4 Improper alignment can affect many sensor types.

NOTE 1 A potentially hazardous behaviour can result from a combination of known potential functional insufficiencies and triggering conditions.

NOTE 2 For specific analysis categories see Annex B. For each category, a list of detailed disturbances is determined based on knowledge and experience (including knowledge gained on similar projects and field experience).

NOTE 3 If sensor input provided by infrastructure elements is relevant for the automated driving (AD) or ADAS functionality, then this subclause is also applicable for this case in order to analyse the functional insufficiencies.

In addition, a systematic analysis of each environmental input, in the range of possible values (including potential and observed scenarios), can be conducted.

7.3.4 Analysis of reasonably foreseeable direct or indirect misuse

A reasonably foreseeable direct and indirect misuse of the intended functionality can contribute to an unreasonable level of risk.

On the one hand, the analysis of direct misuse is covered by Clause 7 as part of the potential triggering condition analysis. On the other hand, the potential functional insufficiencies that could lead to the ineffectiveness of a measure against indirect misuses are also within the scope of Clause 7.

Causes of reasonably foreseeable direct or indirect misuse can be:

— lack of understanding of the system by the users, e.g. the driver is misled by a similar system with different operating rules in the market;

— wrong user expectations of the system, e.g. insufficient, inappropriate or incorrect information presented to the driver;

— loss of concentration;

— overreliance on the system; and

— incorrect assumption of user interaction from the system design.

The analysis of reasonably foreseeable misuse can be supported using the methods described in Table 5. In addition, B.1 describes a method for deriving SOTIF misuse scenarios.

Table 5 — Methods for identification of reasonably foreseeable misuse

	Methods
A	Analysis of known misuse scenarios from field experience and other sources of lessons learnt [a]
B	Studies with test subjects
C	Analysis of use cases and scenarios
D	Analysis of users' interaction with the system [b]
E	Analysis of HMI
F	Analysis of known human patterns of lack of use, misuse and automation complacency
G	Analysis of human capability to perform or switch between certain tasks [c]
H	Application of relevant standards, regulations and guidelines [d]

[a] For example, user videos on the internet demonstrating how the system or other similar systems can be misused in a reasonably foreseeable way.

[b] For example, alertness of driver, system understanding, or operating mode confusion.

[c] For example, analysis of human capability to regain the situational awareness.

[d] For example, code of practice for the design and evaluation of ADAS[11], European statement of principles on human-machine interface[1].

NOTE 1 See detailed approach in B.1.

NOTE 2 The use of a vehicle by a driver incapable of ensuring the driving task in case of need is considered as abuse and it is outside of the scope of this document.

EXAMPLE 1 The driver is under the influence of controlled substances.

EXAMPLE 2 Driving at unreasonably high speed beyond the dynamic control capability of the vehicle on snow.

The need of additional measures dedicated to preventing or mitigating reasonably foreseeable misuse (indirect or direct), and the effectiveness of these measures, can be evaluated while estimating the acceptability of the system's response to the potential triggering conditions. The effectiveness of these measures can be demonstrated during the verification and validation phases.

7.4 Estimation of the acceptability of the system's response to the triggering conditions

The scenarios containing the identified triggering conditions are evaluated to determine whether the SOTIF is deemed to be achievable.

NOTE 1 These known scenarios are covered by the verification activities of Clause 10 to provide a final evaluation of their acceptability.

NOTE 2 Specifically, assumptions used for, or resulting from, this evaluation which are relevant for the achievement of the SOTIF are demonstrated in Clause 10.

NOTE 3 Assumptions that are considered during this evaluation can include expected behaviours of the system and its elements or assumed actions of the user.

The SOTIF is deemed as achievable without need of further functional modification (as described in Clause 8) if:

— the residual risk of the system causing a hazardous event is shown as being lower than the acceptance criteria specified in 6.5; and

NOTE 4 Evidence to be used for the risk evaluation will be generated during verification and validation activities (Clauses 9, 10 and 11).

— there is no known scenario that could lead to an unreasonable risk for specific road users.

NOTE 5 Even if a fleet has a very low probability of a triggering condition as part of a scenario, the response of the system can be unacceptable if the probability to encounter such a scenario is high for a given individual vehicle.

EXAMPLE A particular structure integrated into a roundabout or a bridge pier that systematically causes the AEB system to brake in a way that could lead to unacceptable occurrences of rear collision with the following vehicle.

A system's response to the triggering conditions that is not considered as acceptable according to the conditions above initiates further functional modification (as described in Clause 8).

7.5 Work products

7.5.1 Identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (including reasonably foreseeable direct misuse), fulfilling objective 7.1 a.

NOTE Reports of the analyses conducted to fulfil objective 7.1 a are included in 7.5.1.

7.5.2 Evaluation of the system's response to the identified triggering conditions for their acceptability with respect to the SOTIF, fulfilling objective 7.1 b.

8 Functional modifications addressing SOTIF-related risks

8.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) measures addressing SOTIF-related risks shall be specified and applied;

b) the input information to specification and design (5.5) shall be updated.

8.2 General

To achieve the objectives of this clause, the following information can be considered:

— specification and design (in accordance with 5.5);

— risk evaluation of hazardous behaviours (in accordance with 6.6.2);

— identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (in accordance with 7.5.1);

— verification and validation results for known scenarios (in accordance with 10.8), if any;

— validation results for unknown hazardous scenarios (in accordance with 11.4.1), if any; and

— SOTIF release argument in accordance with 12.5, if any.

8.3 Measures to improve the SOTIF

8.3.1 Introduction

The activities of Clause 8 to elaborate measures addressing SOTIF-related risks (hereinafter referred to as "SOTIF measures") can be performed when the following conditions are met:

— the intended functionality of the current specification and design (Clause 5) is identified as having a hazardous scenario that requires further analysis (evaluated as likely to cause harm in the risk evaluation of the hazardous event) (Clause 6); and

— the system's response to the identified triggering condition that causes the hazardous behaviour is evaluated as unacceptable (there is a known scenario where the residual risk of causing the hazardous event does not meet the acceptance criteria and leads to an unreasonable risk) (Clause 7).

The system is refined through the iteration of considering SOTIF measures in Clause 8, updating the specification and design (Clause 5) with these SOTIF measures, and risk evaluation of the intended functionality (Clause 6 and Clause 7) is conducted by using the updated specification and design.

This refined system (including the effectiveness of the SOTIF measures) is then evaluated in the V&V phase, and iterative activities for refinement of the system in the design phase might be performed via Clause 8 if any of the following conditions are met:

— the residual risk from a known hazardous scenario is determined to be unacceptable (Clause 10);

— an unknown and hazardous scenario where the residual risk is unacceptable is encountered (Clause 11); or

— the residual risk is deemed unacceptable (Clause 12).

In the above case, Clause 5 through Clause 8, are repeated to refine the system.

An appropriate combination of "avoidance" or "mitigation" SOTIF measures are selected to achieve the SOTIF-related risk reduction.

NOTE "Avoidance measures" represent inherently safe design measures where the first priority is eliminating the risks (aiming to achieve S=0 or C=0 in the Clause 6 risk evaluation), and functional modifications (especially new functions added) are a typical approach. However, it does not necessarily mean that S=0 or C=0 will be achieved.

"Mitigation measures" are considered to reduce the risk as much as possible when there is known difficulty in avoiding the risk or when it can be judged acceptable. They are also expected to improve the risk reduction effect when combined with avoidance measures or other mitigation measures.

For implementation of SOTIF measures, the following can be considered:

— there are no adverse effects on other elements; and

— there are no interactions with other hazardous scenarios.

In addition, SOTIF measures, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Therefore, conducting monitoring and review activities as described in Clause 13 is an essential part of the SOTIF measures implementation to assure that the SOTIF measures remain effective.

The subclauses 8.3.2 through 8.3.5 describe possible SOTIF measures.

8.3.2 System modification

Measures for system modification are aimed at maintaining the intended functionality as much as possible. These measures can include, but are not limited to:

1) increased sensor performance and/or accuracy by:

   — improved sensor technology;

     EXAMPLE 1 Increase the resolution of a sensor measurement.

     EXAMPLE 2 Change to new and improved sensor that addresses known limitations.

   — improved sensor disturbance detection that triggers an appropriate warning and degradation strategy;

   — diverse sensor types;

EXAMPLE 3 Add additional sensing devices to improve coverage with appropriate modality.

— improved sensor calibration and installation; or

EXAMPLE 4 Positioning the sensors for better coverage for certain corner cases that have potential for performance insufficiency.

EXAMPLE 5 Packaging the sensor(s) to avoid or minimize disturbances to an acceptable level.

EXAMPLE 6 Performing sensor coverage analysis and optimizing the selection of sensors (type, technology, quantity) and their relative positioning in the vehicle.

— sensor blockage detection and cleaning methods;

EXAMPLE 7 Detecting dirt on a camera using edge detection and cleaning it with fluid and wipers.

2) increased actuator performance and/or accuracy by improving the actuator technology (e.g. increase accuracy, extend or limit range of output, reduce response times, repeatability, arbitrate authority capability, utilize other functions to assist or add a new actuator to assist);

3) increased performance and/or accuracy of the recognition and decision algorithms by algorithmic modifications;

EXAMPLE 8 Improved sensor recognition algorithm [e.g. improve a feature descriptor for detecting objects in camera images, such as HOG (histograms of oriented gradients)].

EXAMPLE 9 Consider additional input information in the model.

EXAMPLE 10 Improve the algorithm to provide better robustness, better precision (e.g. switch from a linear to a non-linear model or use machine learning) (see D.2).

EXAMPLE 11 Speed up image processing with enhanced computing power (e.g. using a machine learning accelerator or operation-efficient hardware).

EXAMPLE 12 Recognition of exiting ODD[2] (e.g. approach to the exit ramp on a motorway).

EXAMPLE 13 Recognition of a known unsupported environmental condition (e.g. predict encounters with the sun glare based on geography, time of day, season, etc.).

NOTE Hardware performance improvement can be considered when implementing advanced algorithms.

4) increasing conspicuousness of the ego vehicle to enhance the controllability of other traffic participants in case of hazardous behaviour of the ego vehicle.

EXAMPLE 14 Installation of retro-reflectors, turning-on fog lights, turn indicators, active sounds, etc., as long as they are permitted by local regulations.

8.3.3 Functional restrictions

Measures for functional restriction are aimed at maintaining a partial functionality by degrading (or limiting) the intended functionality. These measures can include, but are not limited to:

1) restriction of the intended functionality for specific use cases;

EXAMPLE 1 Lane keeping assist functionality restricts the steering assist torque to avoid an undesired steering intervention when lane detection devices cannot clearly detect the lane.

EXAMPLE 2 Limitation of the ODD including environmental, geographical or time-of-day restrictions.

EXAMPLE 3 Restrict or constrain the driving policy (see D.1) to ensure safety of decision making.

EXAMPLE 4 Camera blinded by reflection of surrounding light caused by the afternoon sun; operation continues with restricted authority (e.g. reduced allowed maximum vehicle speed, limiting the maximal steering torque applied by a lane keep assist function) using radar and other sensors.

2) removal of authority for the intended functionality for specific use cases.

EXAMPLE 5 All perception sensors are blinded by a snowstorm; driver is requested to take over control.

EXAMPLE 6 Automated vehicle cannot handle toll booths or unmarked construction zones; driver is requested to take over control.

8.3.4 Handing over authority

Measures for handing over authority from a system to the driver are aimed at increasing controllability at lower levels of driving automation. These measures can include, but are not limited to:

1) modifying the Human-Machine Interface (HMI);

EXAMPLE 1 The HMI clearly communicates the handover request to the driver and provides the necessary information that supports the driver to achieve the appropriate situational awareness and to execute this task.

2) modifying the user notification and DDT fallback strategy.

EXAMPLE 2 When a system detects a sight restriction (e.g. reduced distance sensor range caused by mud), the speed is reduced, and the driver is requested by an appropriate HMI to take over the driving task. If the takeover is not executed within a specified timeframe the system will reduce the speed to zero.

NOTE 1 Depending on the levels of driving automation, the handover might not be possible.

NOTE 2 Improvement of the controllability can only be achieved if the transition itself is controllable and does not present additional risk to the driver.

NOTE 3 Guidance from HMI studies can be considered.

EXAMPLE 3 Code of practice for the design and evaluation of ADAS[11].

8.3.5 Addressing reasonably foreseeable misuse

Measures for addressing reasonably foreseeable misuse can include, but are not limited to:

1) customer education (information and training);

EXAMPLE 1 User manual, training courses, marketing, sales presentation.

2) improving the HMI;

EXAMPLE 2 Support the driver by providing information about the correct operation.

3) implementation of a driver monitoring and warning system; or

NOTE A system for detection and warning of driver distraction, etc. can be a useful method to prevent a reasonably foreseeable driver misuse of an automated vehicle system. Selection and implementation of an effective driver monitoring system depends on the target misuse.

EXAMPLE 3 Warn the driver when the steering wheel is released.

EXAMPLE 4 Ignore inputs/commands that can lead to hazardous behaviour and inform the driver about the reasons.

4) implementation of measures to prevent misuse.

EXAMPLE 5 If driver monitoring detects continued misuse despite driver warnings, then measures can be taken to discourage the hazardous behaviour; e.g. after multiple hands-off-warnings, lane keep assist function could be disengaged or degraded for the rest of the journey with appropriate warning information until the next key-on cycle.

EXAMPLE 6 The reasonably foreseeable misuse of activating a function, e.g. activating parking assist at too high a speed can be prevented by adding a speed restriction to the activation condition of the function.

8.3.6 Considerations to support the implementation of SOTIF measures

Following the implementation of the SOTIF measures, depending on the level of driving automation, the conducting of monitoring and review is important to ensure that the SOTIF measures remain effective and to support this some aspects can be considered when designing the system. These considerations can include, but are not limited to:

— testability for SOTIF-related system behaviour;

— diagnostic ability for SOTIF-related system behaviour; and

— data monitoring ability for SOTIF-related system behaviour.

8.4 Updating the input information for "Specification and design"

The input information for "Specification and design" is updated based on the specification of identified and applied SOTIF measures according to 8.3.

8.5 Work products

The work product is the specification of SOTIF measures fulfilling objectives 8.1 a) and b).

9 Definition of the verification and validation strategy

9.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) the verification and validation strategy for SOTIF, including validation targets, shall be defined and shall consider:

   1) the necessary evaluation of potentially hazardous scenarios;

   2) the sufficient coverage of the relevant scenario space;

   3) necessary evidence (e.g. analysis results, test reports, dedicated investigations); and

   4) procedures to generate the evidence;

b) the rationale for suitability of the selected verification and validation methods and validation targets shall be provided.

9.2 General

To achieve the objectives of this clause, the following information can be considered:

— the ability of sensors or external data sources (e.g. from infrastructure) to provide sufficiently accurate information on the environment to meet the performance requirements;

— the sufficiency of the dependability of the assumed external data sources (e.g. sudden outage of communication network or temporary absence of update possibility);

— the ability of the sensor processing algorithms to accurately model the environment;

— the ability of the decision algorithms to:

   — safely handle potential functional insufficiencies; and

  - make appropriate decisions according to the environmental model, the driving policy and the current goals (e.g. target destination);
- the robustness of the system or functionality, e.g.:
  - the robustness of the system against adverse environmental conditions;
  - the appropriateness of the automated system reaction on known triggering conditions; and
  - the sensitivity of the intended functionality and its monitoring to different scenario conditions;
- the absence of unreasonable risk due to hazardous behaviour of the intended functionality;
- the ability of the system (e.g. HMI) to prevent reasonably foreseeable misuse;
- the ability of the system to safely handle out of ODD use cases (e.g. system activation outside the ODD, transition out of ODD, etc.);
- the suitability of the OEDR, and the robustness of the execution of the driving policy (or behaviours) across the ODD;
- the suitability of the DDT fallback; the suitability of the MRC; and
- the compliance with the acceptance criteria at the vehicle level during the operation phase with a sufficient confidence.

To achieve the objectives of this clause, the following information can be considered:

- specification and design in accordance with 5.4;
- risk evaluation of hazardous behaviours in accordance with 6.6.2;
- acceptance criteria in accordance with 6.6.3;
- identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (including reasonably foreseeable direct misuse) in accordance with 7.5.1;
- specification of SOTIF measures in accordance with 8.5;
- system integration and testing plan (from external source);
- lessons learnt from field monitoring process in accordance with 13.5; and
- lessons learnt that were observed in the sensors' history, possibly in other domains (e.g. atmospheric storm events causing GNSS signal delays with the potential to cause a hazardous event).

The verification and validation strategy is focusing not only on performance evaluation and risk identification within the ODD, but also on the boundaries and outside of the ODD. One aspect of the strategy includes verifying that the system is not engageable from anywhere outside the ODD.

Another aspect is verifying that transitions from within the ODD to outside the ODD are accompanied by escalation to the driver or fallback system to achieve the minimal risk condition.

NOTE These aspects are important to argue the sufficient coverage of the relevant scenario space.

9.3 Specification of integration and testing

A verification and validation strategy is defined to provide an argument that the objectives are achieved and how the validation targets are met. The verification and validation strategy covers the whole intended functionality in the vehicle including both E/E elements and elements of other technologies considered relevant to the achievement of the SOTIF. The verification and validation strategy also supports the data monitoring of external sources relevant for the SOTIF.

The validation targets are defined to provide evidence that the acceptance criteria are met. The validation targets can be determined in many ways depending on the chosen validation methods.

For each of the selected methods from Tables 6, 7, 8, 9, 10, 11 or another source, an appropriate development effort (e.g. cumulative test length, depth of analysis) is defined. A rationale for each defined effort is provided. This can include the number or distribution of scenarios, number of experiments or simulation duration.

NOTE 1 Acceptance criteria address the risk resulting from known and unknown hazardous scenarios. This is considered in the derivation of the validation targets which can be different for area 2 and area 3.

NOTE 2 C.2 and C.6 give examples for defining and evaluating acceptance criteria and validation targets.

EXAMPLE 1 Consider a search for previously unknown triggering conditions that are relevant to the functionality. Validation targets are defined to support the hypothesis that remaining unknown triggering conditions do not impose unreasonable risk.

EXAMPLE 2 The validation target can be set using pre-defined false positive and false negative rates for a function being tested.

If only a subset of scenarios is relevant for a specific hazard, then the exposure to the subset can be considered when determining the target values and the validation duration.

NOTE 3 Table B.5 provides an example of how to generate a subset of scenarios.

NOTE 4 When evaluating the likelihood that a triggering condition will violate the quantitative target, the exposure, controllability and severity of the resulting behaviour can be considered. This can result in a reduction of the effort required to demonstrate the exposure to the triggering condition. See C.2.1 for a methodology to reduce the validation effort by taking into account exposure, controllability and severity.

EXAMPLE 3 Consider Figure 13 where unintended braking only results in a rear collision if a following vehicle is present. The exposure to a following vehicle can be considered when specifying a validation target.

NOTE 5 Variability of the triggering condition parameters is considered in the definition and elaboration of the verification and validation strategy.

NOTE 6 As functional modifications are made through the iteration of SOTIF activities (Figure 10), the system is analysed to determine if existing functions are impacted and these functions are retested with regression tests. This ensures that functional modifications do not cause potentially hazardous behaviour in existing functions. With a proper rationale, the regression testing scope can be tailored.

NOTE 7 To ensure that correct functional behaviour is maintained, complete V&V activities are documented for any release intended for production. This includes documentation of elements that have not been modified and documentation of retested elements impacted by changes.

NOTE 8 D.2.4 discusses verification and validation activities for off-line training such as used for machine learning.

The specification of the verification and validation strategy (e.g. integration test cases, analysis) can be derived using an appropriate combination of methods, considering the integration level, as illustrated by Table 6.

Table 6 — Methods for deriving verification and validation activities

Methods	
A	Analysis of requirements
B	Analysis of external and internal interfaces [a]
C	Generation and analysis of equivalence classes
D	Analysis of boundary values
E	Error guessing based on knowledge or experience
F	Analysis of functional dependencies
G	Analysis of common limit conditions and sequences
H	Analysis of environmental conditions and operational use cases [b]
I	Analysis of field experience and lessons learnt [c]
J	Analysis of system architecture (including redundancies)
K	Analysis of designs of sensors and their known potential limitations
L	Analysis of algorithms and their decision paths and their respective known limitations
M	Analysis of system and component ageing [d]
N	Analysis of triggering conditions
O	Analysis of performance targets [e]
P	Analysis of the measurable parameters from the hazard analysis
Q	Analysis of corner cases and edge cases from boundary values [f]
R	Analysis of SOTIF-related updates to existing systems
S	Use of databases with collected test cases and scenarios
T	Analysis of acceptance criteria
U	Analysis of accident scenario data
V	Analysis of the known potential limitations in the actuation

[a] This also includes V2X, maps, if available.

[b] This includes known sources of potentially hazardous behaviour of the system or its elements.

[c] This considers various driving conditions, driving styles, driving environments and end customer claims.

[d] Ageing effects of semiconductors which lead to failures are typically considered under the ISO 26262 series. SOTIF-related ageing effects of semiconductors, i.e. those impacting the nominal performance, are within the scope of this document.

[e] Performance targets can be specified on different levels of abstraction, e.g. on sensor level (range of radar, angle resolution of cameras) as well as on system level (e.g. a false positive rate of object detection).

[f] "A corner case is a scenario in which two or more parameter values are each within the capabilities of the system, but together constitute a rare condition that challenges its capabilities. An edge case is a scenario in which the extreme values or even the very presence of one or more parameters results in a condition that challenges the capabilities of the system"[12].

NOTE 9 See C.4 for further practices for verification and validation of automotive perception systems.

9.4 Work products

The work product is the definition of the verification and validation strategy fulfilling objectives 9.1 a) and b).

10 Evaluation of known scenarios

10.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) identified potentially hazardous scenarios shall be evaluated if they are hazardous or not;

b) the functionality of the system and its elements shall behave as specified for known hazardous scenarios and reasonably foreseeable misuse;

c) the potentially hazardous behaviour due to the specified behaviour at the vehicle level shall be evaluated concerning its acceptability;

d) known scenarios shall be sufficiently covered according to the verification and validation strategy; and

e) the verification results shall demonstrate that the validation targets are met.

NOTE This includes the evaluation of the appropriateness of the DDT fallback and the MRC.

10.2 General

To achieve the objectives of this clause, the following information can be considered:

— specification and design in accordance with 5.4;

— identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (including reasonably foreseeable direct misuse) in accordance with 7.5.1;

— measures addressing SOTIF-related risks in accordance with 8.5; and

— definition of the verification and validation strategy in accordance with 9.4.

NOTE For the traceability of identified pre-existing SOTIF-related content of the specification and design and of functional modifications resulting from iterations of the SOTIF activities, guidance is given in 5.3.

The structure of 10.3 to 10.5 follows the sense (10.3), plan (10.4), and act (10.5) pattern as introduced in 4.2.3. 10.6 addresses integration aspects.

10.3 Sensing verification

Methods to demonstrate the correct functional performance, timing, accuracy and robustness of the sensing part for their intended use and reasonably foreseeable misuse can be applied as illustrated by Table 7.

NOTE 1 Some issues can be assigned to different verification activities, e.g. object classification could be viewed as being part of the planning algorithm (see 10.4). In this case, verification methods from more than one subclause can be applied.

Table 7 — Sensing verification

Methods	
A	Verification of the sufficiency of the sensor specification (e.g. sufficiency of range, precision, resolution, timing constraints, bandwidth, signal-to-noise ratio, signal-to-interference ratio) [a]
B	Requirements-based test (e.g. classification, sensor data fusion)
C	Injection of inputs that trigger the functional insufficiency [b]
D	In the loop testing (e.g. SIL, HIL, MIL) on selected SOTIF-related use cases and scenarios considering identified triggering conditions [c]
E	Vehicle testing on selected SOTIF-related use cases and scenarios considering identified triggering conditions [c]
F	Sensor test under different environmental conditions within the specified ODD (e.g. cold, damp, light, visibility conditions, interference conditions)
G	Verification of sensor ageing effects (e.g. accelerated life testing etc.) [d]
H	Evaluation of experience from the field with this sensor or this type of sensor including field monitoring
I	Re-simulation of known hazardous scenarios to verify the effect of an implemented risk mitigation mechanism
J	Verification of the architectural properties including independence regarding triggering conditions, if applicable

[a] This includes also end-of-line testing during sensor assembly (e.g. the alignment between radar antenna and radar radome or the alignment of camera imager to camera lens).

[b] In some cases, it is possible to emulate a potential performance insufficiency of the sensor by means of error injection at the simulation level. A rationale why the error models can represent the tested phenomena is provided. Outcomes of those simulations can be combined with results of the analysis of triggering conditions.

[c] Use identified sensor model limitations to select the test environment (HIL/SIL/MIL or vehicle).

[d] In case of well-known ageing fault models for a specific sensor, verification of sensor ageing effects can be done partly in simulation.

NOTE 2 For test case derivation, the judicious use of the principles of combinatorial testing can be applied[13].

NOTE 3 C.4 provides examples for the verification of perception sensors.

10.4 Planning algorithm verification

According to 4.2.3 the planning algorithm derives the control actions based on the environmental model provided by the sensing part. Methods to verify the ability of the planning algorithm to react as required and its ability to avoid unwanted action can be applied as illustrated by Table 8.

Table 8 — Planning algorithm verification

Methods	
A	Verification of robustness against input data being subject to interference from other sources, e.g. white noise, audio frequencies, signal-to-noise ratio degradation (e.g. by noise injection testing)
B	Requirement-based test (e.g. situation analysis, function, variability of sensor data) [a]

[a] This also includes the verification that the vehicle selects and achieves the appropriate MRC.

[b] Driving policy guidance is introduced in D.1.

Table 8 *(continued)*

Methods	
C	Verification of the architectural properties including independence regarding triggering conditions, if applicable
D	In the loop testing (e.g. SIL, HIL, MIL) on selected SOTIF-related use cases and scenarios considering identified triggering conditions
E	Vehicle testing on selected SOTIF-related use cases and scenarios considering identified triggering conditions
F	Injection of inputs that trigger the potentially hazardous behaviour
G	Verification of proper compliance to the driving policy (e.g. achieving the MRC and operation upon exiting the ODD [a] [b]
H	Re-simulation of known hazardous scenarios to verify the effect of an implemented risk mitigation mechanism

[a] This also includes the verification that the vehicle selects and achieves the appropriate MRC.

[b] Driving policy guidance is introduced in D.1.

NOTE For test case derivation, the judicious use of the principles of combinatorial testing can be applied[13].

10.5 Actuation verification

Methods to verify the actuators for their intended use and reasonably foreseeable misuse can be applied as illustrated by Table 9.

Table 9 — Actuation verification

Methods	
A	Requirements-based test (e.g. accuracy, resolution, timing constraints, bandwidth)
B	Verification of actuator characteristics, when integrated within the vehicle environment or on a system test bench
C	Actuator test under different environmental conditions (e.g. cold conditions, damp conditions)
D	Actuator test between different load conditions (e.g. change from medium to maximum load)
E	Verification of actuator ageing effects (e.g. accelerated life testing)[a]
F	In the loop testing (e.g. SIL, HIL, MIL) on selected SOTIF-related use cases and scenarios considering identified triggering conditions
G	Vehicle testing on selected SOTIF-related use cases and scenarios considering identified triggering conditions
H	Verification of the architectural properties including independence regarding triggering conditions, if applicable
I	Re-simulation of known hazardous scenarios to verify the effect of an implemented risk mitigation mechanism

[a] In case of well-known ageing fault models for a specific actuator, verification of actuator ageing effects can be done partly in simulation.

NOTE If it can be argued that the actuation systems do not have any functional insufficiencies or triggering conditions then testing carried out solely according to the ISO 26262 series or other relevant domain specific standards can be sufficient.

10.6 Integrated system verification

Methods to verify the robustness and the controllability of the system integrated into the vehicle and the correct interaction of the system components within the vehicle can be applied as illustrated by Table 10.

Table 10 — Integrated system verification

	Methods
A	Verification of system robustness (e.g. by noise injection testing) [a]
B	Requirement-based test when integrated within the vehicle environment or on a system test bench (e.g. performance targets and behaviour characteristics, measurable parameters, range, precision, resolution, timing constraints, bandwidth)
C	In the loop testing (e.g. SIL, HIL, MIL) on selected SOTIF-related use cases and scenarios considering identified triggering conditions
D	System test under different environmental conditions (e.g. cold, damp, light, visibility conditions, interference conditions)
E	Verification of system ageing affects (e.g. accelerated life testing)
F	Directed randomized input test [b]
G	Vehicle-level testing on selected SOTIF-related use cases and scenarios considering identified triggering conditions
H	Controllability test (including reasonably foreseeable misuse)
I	Verification of internal and external interfaces
J	Verification of vehicle mounted sensing system characteristics [c]
K	Verification of the architectural properties including independence regarding triggering conditions, if applicable
L	Re-simulation of known hazardous scenarios to verify the effect of an implemented risk mitigation mechanism

[a] This also includes the verification of robust performance across the ODD and OEDR and the verification of robust execution of the MRC strategy including exiting ODD.

[b] Expected real world situations are often hard to reproduce, so randomized input tests can be used instead as a substitute, for example in the case of:

— image sensors adding flipped images or altered image patches;

— radar sensors adding ghost targets to simulate multi-path returns; or

— radar sensors adding ghost targets or missing detection targets due to multi-vehicle radar interference.

[c] This includes the operation of the different sensors under different operating conditions (e.g. where the capability of one sensor technology is insufficient, such as fog or windshield reflectivity affecting a camera or the shape and type of paint for a bumper/logo affecting a radar) and the tolerances of the sensor position.

NOTE 1 For verification of non-deterministic systems the evaluation of known hazardous scenarios can be performed using statistical methods or risk management techniques.

EXAMPLE Driving policy behaviours rely on assumptions of road participants, in particular in the presence of occlusions where following the known non-hazardous behaviour under certain circumstances might result in a collision.

NOTE 2 C.4 provides examples for the verification of integrated systems.

10.7 Evaluation of the residual risk due to known hazardous scenarios

The validation targets defined in Clause 9 provide the argument that the acceptance criteria are met during the operation phase with a sufficient confidence. Therefore, the verification results demonstrate that the validation targets for known hazardous scenarios are achieved and the residual risk from known hazardous scenarios is not unreasonable.

Known hazardous scenarios are not unreasonable, if:

— the probability of known scenarios causing hazardous behaviour complies with the validation targets; and

— there is no known scenario that could lead to an unreasonable risk for specific road users.

EXAMPLE Local geographic properties (e.g. a certain tunnel or bridge) cannot lead to an unreasonable increase of risk.

10.8 Work products

The work products are the verification and validation results to show that the intended functionality behaves as expected in the known scenarios fulfilling objective 10.1.

11 Evaluation of unknown scenarios

11.1 Objectives

The purpose of this clause is that the validation results shall demonstrate that the residual risk from unknown hazardous scenarios meets the acceptance criteria with sufficient confidence.

NOTE One aspect is a representative coverage of the possible scenario space by the whole set of V&V activities.

11.2 General

To achieve the objectives of this clause, the following information can be considered:

— specification and design in accordance with 5.4;

— identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (including reasonably foreseeable direct misuse) in accordance with 7.5.1;

— measures addressing SOTIF-related risks in accordance with 8.5;

— definition of the verification and validation strategy in accordance with 9.4; and

— verification and validation results to show that the intended functionality behaves as expected in the known scenarios in accordance with 10.8.

11.3 Evaluation of residual risk due to unknown hazardous scenarios

Unknown scenarios can be encountered in real-life situations. Methods to evaluate the residual risk arising from real-life situations, that could trigger a hazardous behaviour of the system when integrated in the vehicle, can be applied as illustrated by Table 11.

Table 11 — Evaluation of residual risk

Methods	
A	Validation of robustness to signal-to-noise ratio degradation (e.g. by noise injection testing)
B	Validation of effects and properties provided by the architecture including independence regarding triggering conditions, if applicable
C	In the loop testing on randomized test cases (derived from a technical analysis and by error guessing)
D	Randomized input test [a]
E	Vehicle-level testing on selected test cases (derived from a technical analysis and by error guessing) considering identified triggering conditions
F	Long term vehicle test
G	Fleet test
H	Test derived from field experience
I	Test of corner cases and edge cases [b]
J	Comparison with existing systems
K	Simulation based on random sequence of scenarios
L	Test of potential misuses with random usage and naïve users
M	Sensitivity analysis of the functionality concerning specific conditions of a scenario [c]
N	Analysis/simulation of relevant parameters [d]
O	Scenario exploration in real world [e]
P	Functional decomposition and probabilistic modelling (i.e. considering that the insufficiency condition of an element consists of multiple output insufficiencies of its sub-elements; see C.6.3.3)
Q	Validation against ground truth

[a] Expected real-world situations are often hard to reproduce, so randomized input tests can be used instead as a substitute, for example in the case of:

— image sensors adding flipped images or altered image patches; or

— radar sensors adding ghost targets to simulate multi-path returns; or

— radar sensors adding ghost targets or missing detection targets due to multi-vehicle radar interference.

[b] "A corner case is a scenario in which two or more parameter values are each within the capabilities of the system, but together constitute a rare condition that challenges its capabilities. An edge case is a scenario in which the extreme values or even the very presence of one or more parameters results in a condition that challenges the capabilities of the system."[12]

[c] A functionality is regarded as sensitive concerning a specific condition of the scenario if small changes of this condition can lead to significantly different behaviour at the vehicle level.

[d] See NOTEs 5, 6, and 7 of 7.3.1. The list of triggering conditions derived as described in 7.3 can be used to identify relevant use case parameters.

[e] Exploration means to search for unknown scenarios by covering a diverse set of the real-world scenarios. This can include systematically or randomly varying relevant parameters of the scenarios.

NOTE Parameter selection is argued by, for example, sensitivity analysis or statistical analysis to have evidence that the selected parameters are the relevant ones.

For tests in public areas, it is possible that additional safety measures are necessary to prevent or mitigate the potential risk to the public due to test vehicles (e.g. emergency stop mechanism).

NOTE 1 New unknown hazardous scenarios can arise each time when there are changes introduced such as algorithm changes, ODD changes, OEDR changes, the introduction of new vehicle types into the environment and driving policy changes. The methods in Table 11 can also be applied for the re-evaluation of the residual risk once these changes have been introduced.

The set of selected methods are adequate to identify potentially hazardous scenarios in area 3, e.g. by using inputs that are representative for the use case as well as by focusing on challenging or rare operational environments, specific use cases, scenes or scenarios. A rationale for the adequacy of the selected methods is provided.

Vehicle test length determination (e.g. for long-term tests, fleet tests) can consider knowledge from prior vehicle programmes, driver controllability or the criticality of selected test routes. When using randomised input tests with error injection, the number of scenarios simulated can be selected to match a required test length and content that is representative of the target geographic market.

When considering test methods such as test track, simulation, or open road, appropriate distribution of kilometres or hours of operation with respect to each test method is performed. A justification for this distribution can be provided.

NOTE 2 A continuous randomised simulation loop of the decision-making algorithms can simulate millions of kilometres of operation but might not be weighted the same as real-world exposure since simulations are always incomplete models of the real world.

NOTE 3 C.4 provides examples for the validation of SOTIF-related systems.

According to Clause 9 the validation targets are chosen in a way that their fulfilment entails that the acceptance criteria are fulfilled. Under these conditions the residual risk due to unknown hazardous scenarios is acceptable.

EXAMPLE A validation target can be a maximum number of encountered previously unknown hazardous scenarios for a set of test scenarios. If after the execution of these test scenarios the number of encountered previously unknown hazardous scenarios is smaller than the defined target value, then the validation target is met.

11.4 Work products

11.4.1 Validation results for unknown hazardous scenarios fulfilling objective 11.1

11.4.2 Evaluation of the residual risk fulfilling objective 11.1

12 Evaluation of the achievement of the SOTIF

12.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) the work products resulting from the SOTIF activities shall be reviewed for completeness, correctness and consistency;

b) an argument for the achievement of the SOTIF shall be provided, considering the fulfilment of the objectives of the clauses of this document and the corresponding work products; and

c) the argument for the achievement of the SOTIF shall be evaluated and a recommendation for approval or rejection of the SOTIF release shall be given.

12.2 General

To achieve the objectives of this clause, the following information can be considered:

— specification and design (in accordance with 5.5);

— hazards at the vehicle level (in accordance with 6.6.1);

— risk evaluation of hazardous behaviours (in accordance with 6.6.2);

— acceptance criteria (in accordance with 6.6.3);

— identified insufficiencies of specification, performance insufficiencies and triggering conditions (in accordance with 7.5.1);

— evaluation of the response of the system to triggering conditions (in accordance with 7.5.2);

— SOTIF measures specification (in accordance with 8.5);

— definition of the verification and validation strategy (in accordance with 9.4);

— verification and validation results to show that the intended functionality behaves as expected in the known hazardous scenarios (in accordance with 10.8);

— validation results for unknown hazardous scenarios (in accordance with 11.4.1);

— evaluation of residual risk (in accordance with 11.4.2); and

— field monitoring process (in accordance with 13.5).

12.3 Methods and criteria for evaluating the SOTIF

Each work product is examined for completeness, correctness and consistency.

An argument is developed to show the achievement of the SOTIF, based on the fulfilment of the objectives of Clauses 5 to 11 and of the field monitoring measures (e.g. process and necessary hardware resources) defined in Clause 13.

NOTE 1 For a possible argument structure example using the GSN, see A.1.

The evaluation of this argument can include, but is not limited to, the following aspects.

a) Are the hazards, potential functional insufficiencies, and triggering conditions analysed and any necessary design modifications to achieve the SOTIF implemented and evaluated, to ensure that these design modifications have sufficiently reduced the risk according to the acceptance criteria in all specified use cases?

b) Does the intended functionality achieve a minimal risk condition, when necessary, providing a state without unreasonable risk to the occupants or other road users, considering:

   1) the specified driver intervention;

   2) reasonably foreseeable misuse;

   3) the specified warning to the vehicle occupants and/or the other road users;

   4) the specified degradation of the functionality; and

5) the DDT fallback (to achieve the minimal risk condition)?

c) Does the verification and validation strategy provide coverage for all the known hazardous scenarios and does it provide an argument that the residual risk from unknown hazardous scenarios meets the acceptance criteria with sufficient confidence?

1) Do the test results cover identified triggering conditions, covering environmental conditions as well as direct and indirect misuse?

2) Are sufficient validation activities included in the verification and validation strategy to limit the risk due to known and unknown scenarios?

d) Is sufficient verification and validation completed and are the validation targets met, to have confidence that the residual risk is not unreasonable?

1) Has the intended functionality been exercised sufficiently to evaluate both nominal behaviour and potentially hazardous behaviour?

2) In case of a hazardous behaviour, was evidence provided to argue the absence of unreasonable risk?

3) Did testing provide sufficient coverage argument to support the robustness of the driving policy across all use cases and/or ODD, OEDR?

e) Are the necessary means for realising the operation phase activities (according to Clause 13) available?

NOTE 2 If operation phase activities described in Clause 13 have led to SOTIF measures, these measures are reviewed in Clause 12.

EXAMPLE See C.2.2.

NOTE 3 The examination of the results of the SOTIF activities can be considered jointly with the ISO 26262-2 functional safety assessment.

12.4 Recommendation for SOTIF release

Based on evidence of the methodology from 12.3, a recommendation of “acceptance”, “conditional acceptance” or “rejection” for release can be determined. In case of “conditional acceptance”, the conditions are documented and their fulfilment is verified before final release.

NOTE Conditional acceptance is an intermediate result. In this case, the conditions are documented and their fulfilment is verified before final release, i.e. the final release can be accepted when the conditions are satisfied.

EXAMPLE An intermediate target value for driven miles as part of a long-term endurance test can be set based on an acceptable rationale as specified in 6.5. If all conditions are met, this can justify acceptance. If the previous conditions are true except for completion of regression testing of a design improvement to resolve a SOTIF anomaly, then conditional acceptance is appropriate. Release can occur after the regression testing has successfully completed.

The evaluation of the achievement of the SOTIF is documented.

12.5 Work products

The work product is the SOTIF release argument fulfilling objective 12.1.

13 Operation phase activities

13.1 Objectives

The purpose of this clause is to achieve the following objectives:

1) a field monitoring process to ensure the SOTIF during operation shall be defined before release; and

2) the field monitoring process shall be executed to maintain the achievement of the SOTIF during the operation phase.

13.2 General

The SOTIF activities described in Clauses 5 through 12 aim at reducing the risk to an acceptable level at the time of SOTIF release. However, that risk evaluation might be reconsidered, for instance:

— if a previously unidentified hazard is uncovered in the field during operation of the functionality;

— if a previously unidentified functional insufficiency and/or triggering condition is uncovered in the field during operation of the functionality; and

— if assumptions such as environment conditions or traffic regulation change, compared with those defined during the development of the functionality.

To achieve the objectives of this clause, the following information can be considered:

— specification and design as defined in Clause 5;

— acceptance criteria as defined in Clause 6;

— identified potential insufficiencies of the specification, potential performance insufficiencies and triggering conditions (including reasonably foreseeable misuse) as defined in Clause 7;

— results of the verification activities as defined in Clause 10; and

— results of the validation activities and the residual risk evaluation as defined in Clause 11.

Figure 16 shows the scope of operation phase activities.

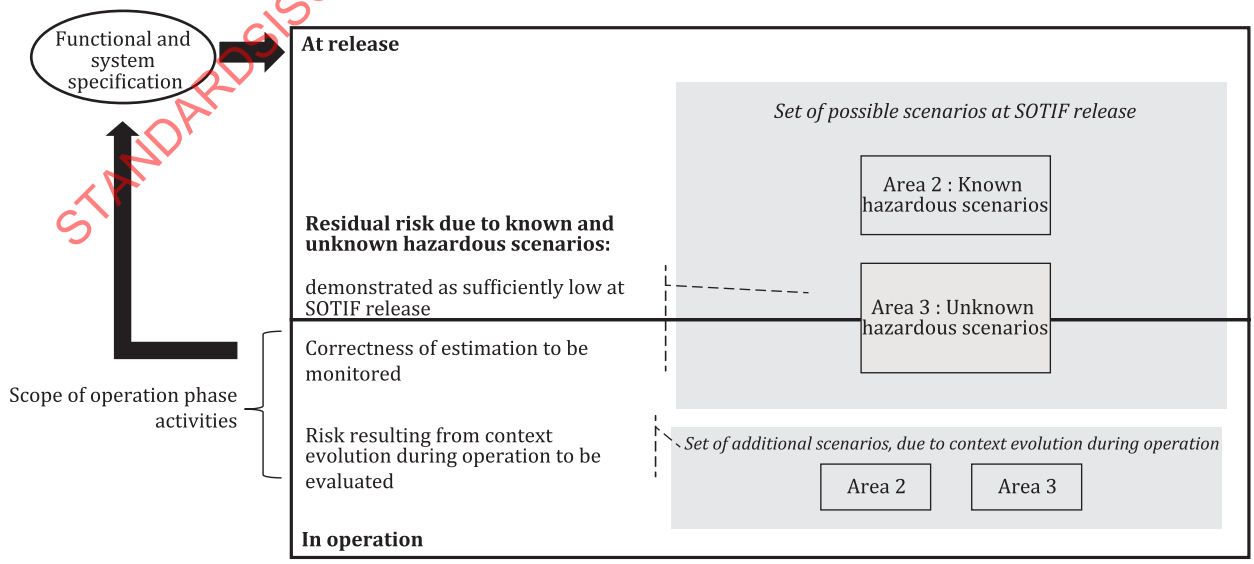


Figure 16 — Scope of operation phase activity

NOTE The activities that maintain compliance with specification and design necessary to achieve the SOTIF over the life cycle, including production, operation and services covered by ISO 26262-7, are not addressed in Clause 13.

13.3 Topics for observation

The expectations on the field monitoring process depend on the level of driving automation, the complexity of the intended functionality and the criticality of hazards. For lower levels of driving automation, the usual market observation can be sufficient. For higher levels of driving automation, additional means can be necessary, such as Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR).

The topics for observation can include, but are not limited to:

a) incidents where the functionality has caused or has had the potential to cause harm, or where the functionality has exceeded defined values which might lead to harm in a different situation,

EXAMPLE 1 These incidents can include:

— accident or incident reports;

— driver reports claiming problems;

— reasonably foreseeable misuse reports; and

— on-board mechanism signalling potential weaknesses, such as:

  — violating a minimum distance to an obstacle; and

  — scenarios where the system was close to triggering a specific system reaction.

NOTE 1 For higher levels of driving automation, it can be relevant to implement monitoring mechanisms, e.g. on-board monitoring. These can detect potential functional insufficiencies before accidents occur (such as functional insufficiencies leading to near-accidents, conditions that lead to an insufficient output at the element level). In this case, the requirements for SOTIF on-board monitoring mechanisms are specified during the development phase.

EXAMPLE 2 On-board monitoring mechanisms can:

— capture scenarios that triggered an emergency system reaction;

— capture scenarios where the driver unexpectedly took over; and

— capture scenarios leading to a minimal risk condition.

b) body of knowledge.

EXAMPLE 3 The body of knowledge can include:

— publicly available incidents on the market coming from public safety agencies (including other vehicle manufacturers) that can be relevant for the functionality,

— lessons learnt from other similar system designs or similar functionalities.

c) context evolution that could affect the SOTIF and might lead to the reconsideration of the SOTIF evaluation.

NOTE 2 Context evolution describes the changes in the scenarios that can be encountered including but not limited to the operational domain and user's system interaction.

EXAMPLE 4 The evolution can include:

— road and traffic evolutions;

— regulation modification;

— infrastructure modification;

— new types of usages and misuse;

— evolution of characteristics of road user; and

— modification of user habits in general, or resulting from the use of the system.

13.4 SOTIF issue evaluation and resolution process

Within the SOTIF issue evaluation and resolution process, the roles and responsibilities are defined:

— for forwarding the relevant data to the development;

— for evaluating the collected data to determine if the risk is still reasonable; and

— if necessary, for defining and rolling out measures to ensure the SOTIF.

Activities for operation phase include, but are not limited to the following:

1) Monitoring and analysis

The monitoring step continuously monitors the topics of observation defined according to 13.3. The monitoring can be reactive [see 13.3 a)] and proactive [see 13.3 b) and 13.3 c)]. Furthermore, monitoring can uncover potentially hazardous scenarios that were not identified during the development phase.

If any SOTIF relevant observation is made, the impact on the SOTIF argument is analysed and the validity of the SOTIF argument is re-evaluated.

NOTE 1 Monitoring targets can be defined in the development phase.

NOTE 2 SOTIF relevant observations can be used to update or enrich the databases used to support SOTIF analysis for further development (lessons learnt).

NOTE 3 See Annex A for examples of SOTIF argument.

NOTE 4 If necessary, the SOTIF argument can be updated.

2) Risk evaluation and hazard mitigation

If the SOTIF argument is no longer valid, the risk is evaluated. Depending on the risk associated to the SOTIF relevant observation, a decision is taken on the risk mitigation means. An immediate reaction might be necessary to mitigate an unreasonable risk. This might result in measures that do not require any additional SOTIF activities [e.g. partial or complete inhibition of the functionality over the air (OTA)] before the final fix is available, for which the corresponding SOTIF activities are executed. A long-term action might be necessary to add new SOTIF measures and to update the system, requiring additional SOTIF activities to be performed leading to a new SOTIF release. System and function modifications deemed necessary after SOTIF release are addressed considering Clauses 5 through 12.

NOTE 5 OTA updates can provide a flexible and convenient method to implement modification to address the identified functional insufficiencies in a timely manner during the operation phase.

13.5 Work products

The work product is the field monitoring process fulfilling objective 13.1.

Annex A
(informative)

General guidance on SOTIF

A.1 Examples of structuring the SOTIF argument with GSN

A.1.1 General

A.1 gives two examples of how the SOTIF argument can be expressed using the goal structuring notation (GSN)[14]. Tables A.1 and A.2 describe the elements used in the GSN examples. The argument can be structured in different ways. Possible, but not exclusive structures can be found in A.1.2 and A.1.3.

GSN is a method widely used in the safety community. The purpose of GSN is to document the rationale for the top goal that the absence of unreasonable risk has been achieved. This is done by showing how goals are broken down into sub-goals, and eventually supported by evidence (solutions) whilst making clear the strategies adopted and the context in which goals are stated.

NOTE GSN can be used to address goals and objectives also derived from other standards such as the ISO 26262 series.

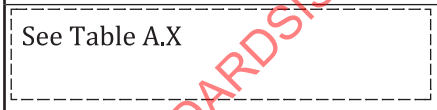
Table A.1 — Description of used GSN elements

Symbol	Name	Description
{Goal identifier} < Goal statement >	Goal	A goal, rendered as a rectangle, presents a claim forming part of the argument.
{Strategy identifier} <Strategy statement>	Strategy	A strategy, rendered as a parallelogram, describes the nature of the inference that exists between a goal and its supporting goal(s).
{Solution identifier} <Solution statement>	Solution or Evidence	A solution or evidence, rendered as a circle, presents a reference to an evidence item.
{Context identifier} <Context statement>	Context	A context, rendered as shown left, presents a contextual artefact. This can be a reference to contextual information, or a statement. Sometimes used for defining terms within goals or strategies.
{Assumption identifier} <Assumption statement> A	Assumption	An assumption, rendered as an oval with the letter 'A' at the bottom-right, presents an intentionally unsubstantiated statement.

Table A.1 *(continued)*

Symbol	Name	Description
	Supported by	Supported by, rendered as a line with a solid arrowhead, allows inferential or evidential relationships to be documented.
	In context of	In context of, rendered as a line with a hollow arrowhead, declares a contextual relationship.
	Multiplicity	This is a means of indicating that there may be multiple instances of the corresponding relationship, upon instantiation. A solid ball is the symbol for many (meaning zero or more). The label next to the ball indicates the cardinality of the relationship.

Table A.2 — Description of used notational elements not present in the official GSN standard

Symbol	Name	Description
	Assurance claim point	This is a means of referencing an argument pertaining to the relationship between two elements. NOTE A safety argument includes references to information that — provide context; — state assumptions; and — represent evidence. The sufficiency and appropriateness of these references can be questioned. The answer to such a question will be an argument supporting a claim that the information is sufficient and appropriate. The use of an assurance claim point (ACP) is a convenient syntactic means of indicating that a supporting confidence argument is present, or required, without cluttering up the main argument diagram. The argument behind the ACP is then provided in a separate diagram.
	Figure reference	This is a reference to Figure A.X in which the argument is continued.
	Table reference	Reference to Table A.X

A.1.2 GSN example 1

The example 1 GSN argument (Figures A.1 to A.7) is based on the absence of unreasonable risks due to known (i.e. area 2) and unknown (i.e. area 3) potentially hazardous scenarios.

NOTE In the GSN example AD is used as an acronym for “automated driving”, DA is used as an acronym for “driver assistance”.

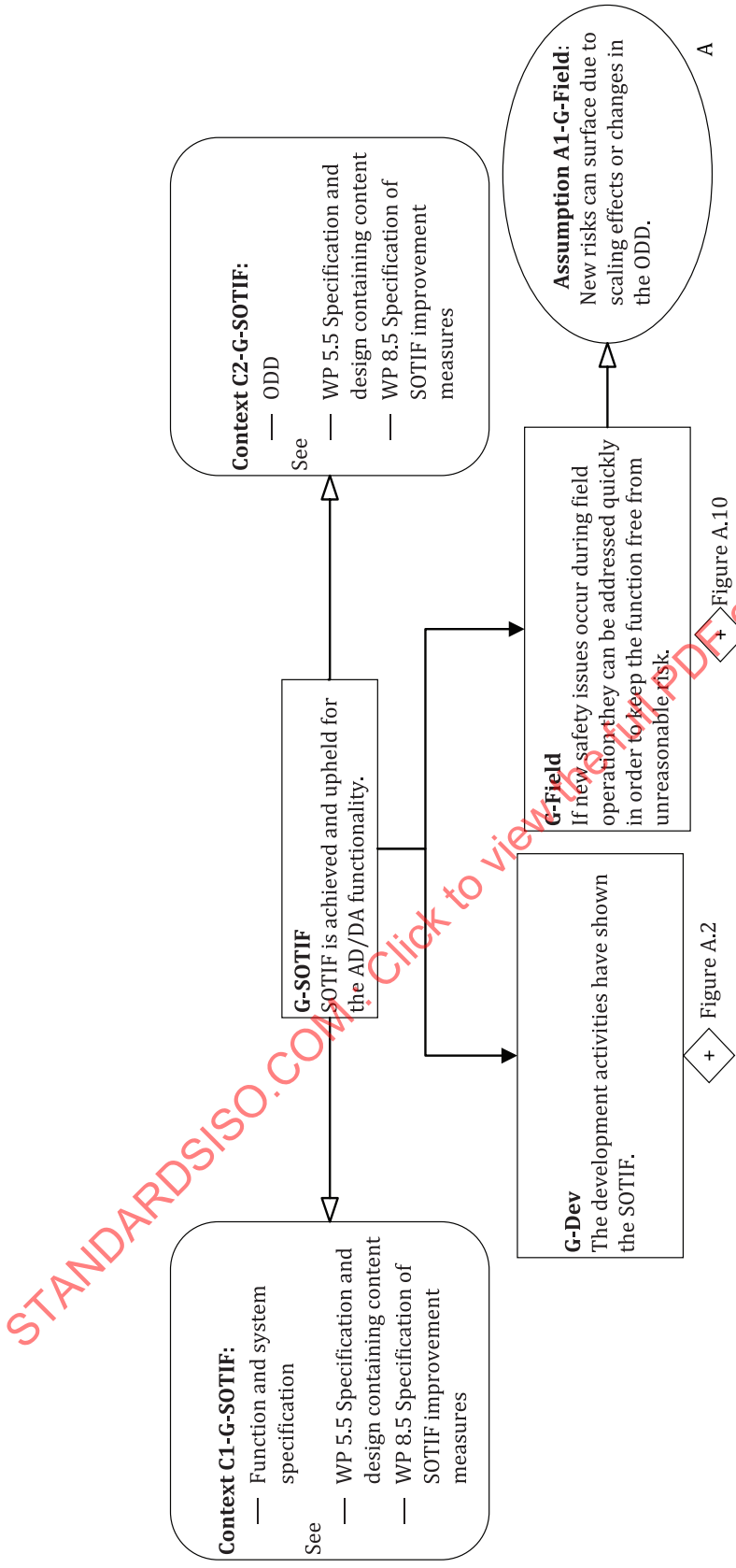


Figure A.1 — G-SOTIF: SOTIF is achieved and upheld for the AD/DA functionality

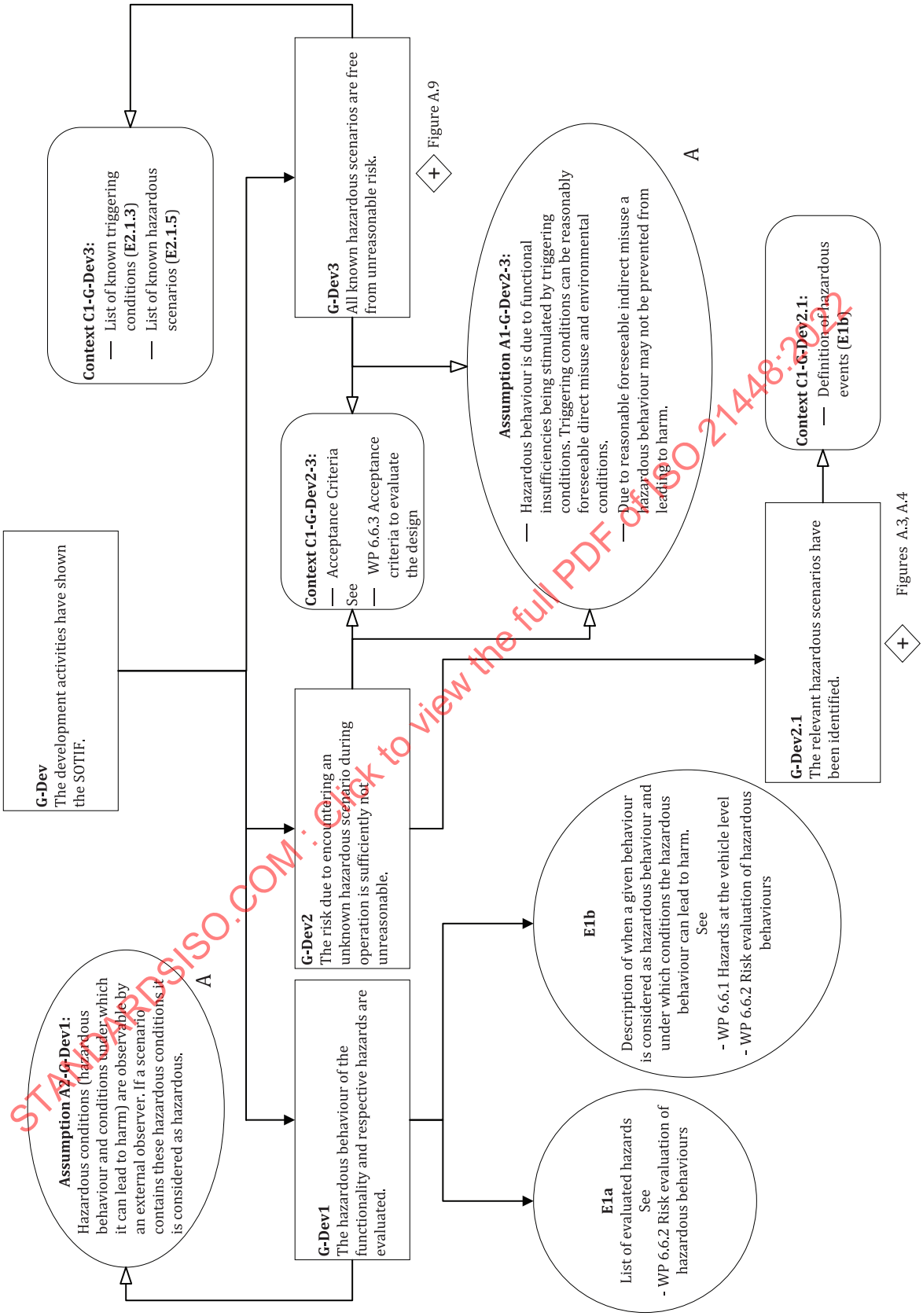


Figure A.2 — G-Dev: development activities have shown the SOTIF

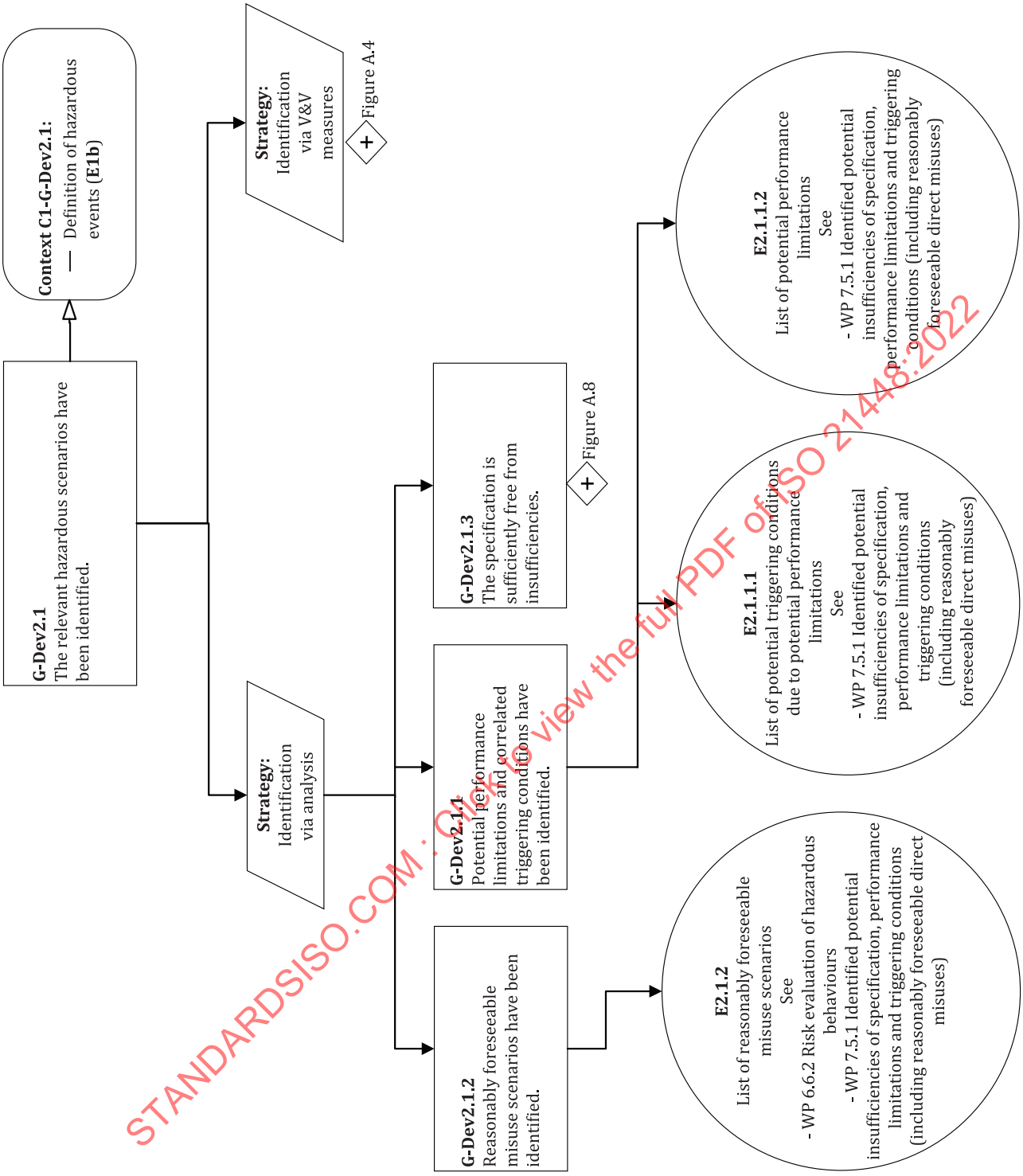


Figure A.3 — G-Dev2.1: relevant potentially hazardous scenarios have been identified – part 1

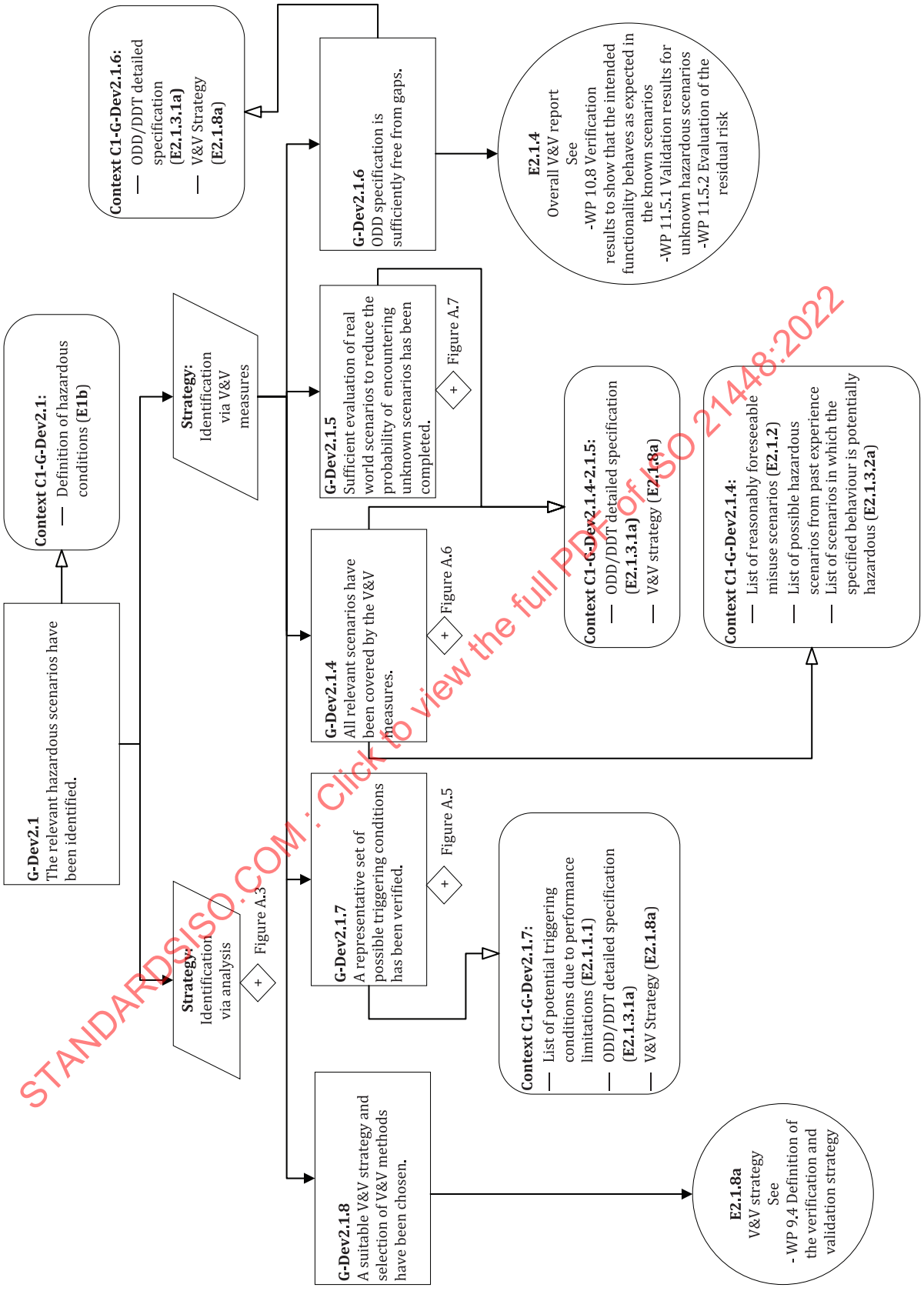


Figure A.4 — G-Dev2.1: relevant hazardous scenarios have been identified – part 2

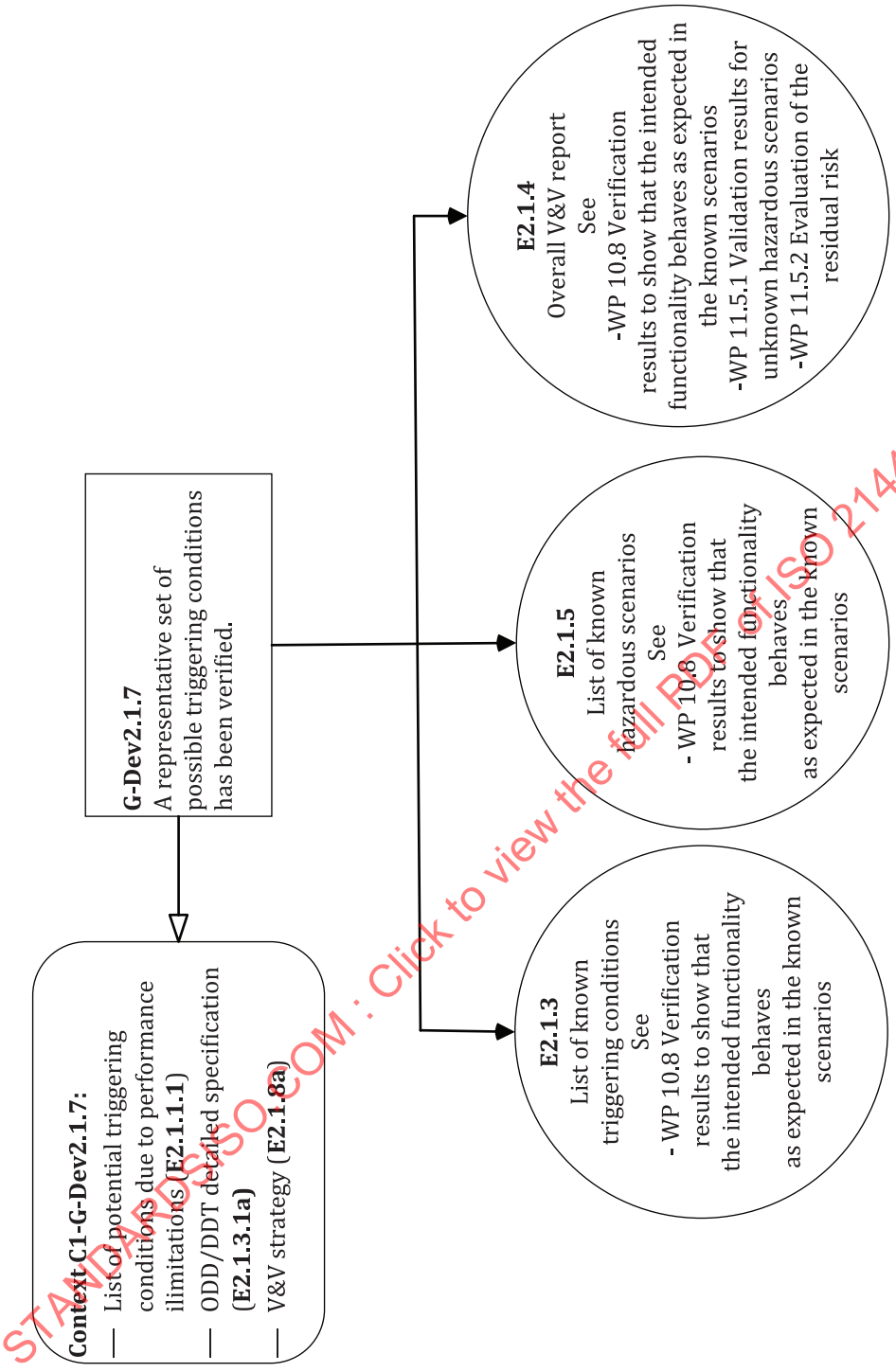


Figure A.5 — G-Dev2.1.7

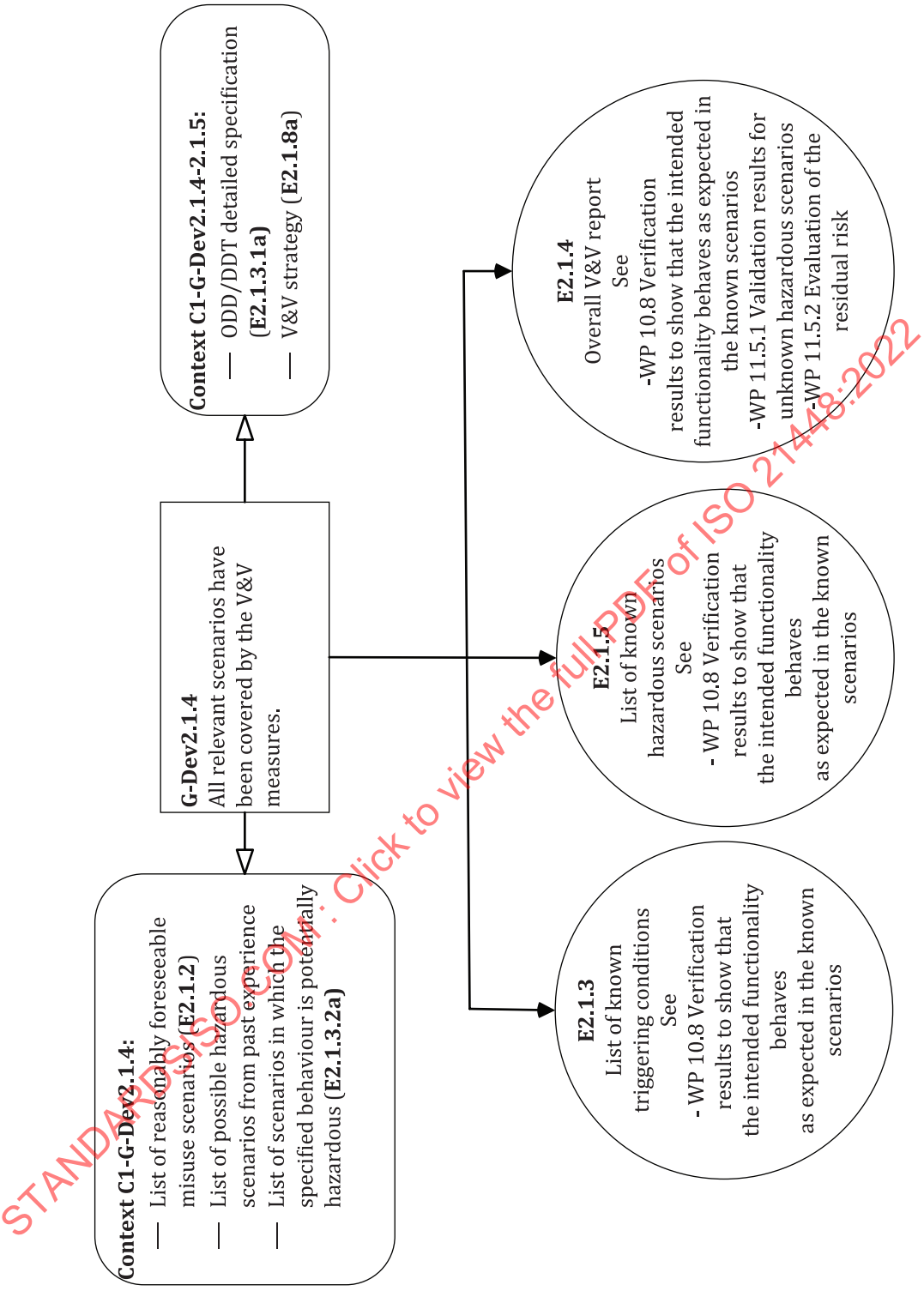


Figure A.6 — G-Dev2.1.4

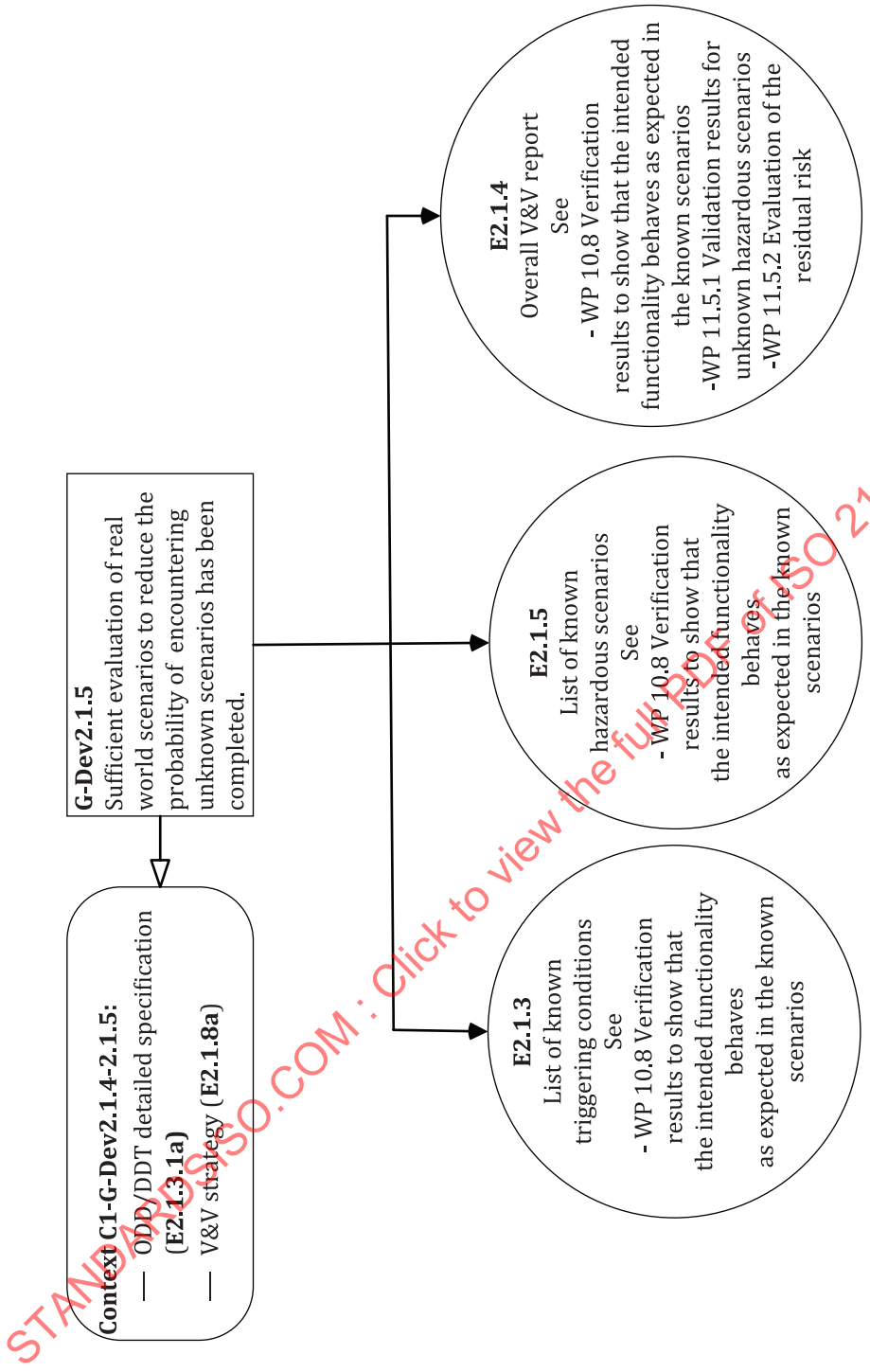


Figure A.7 — G-Dev2.1.5

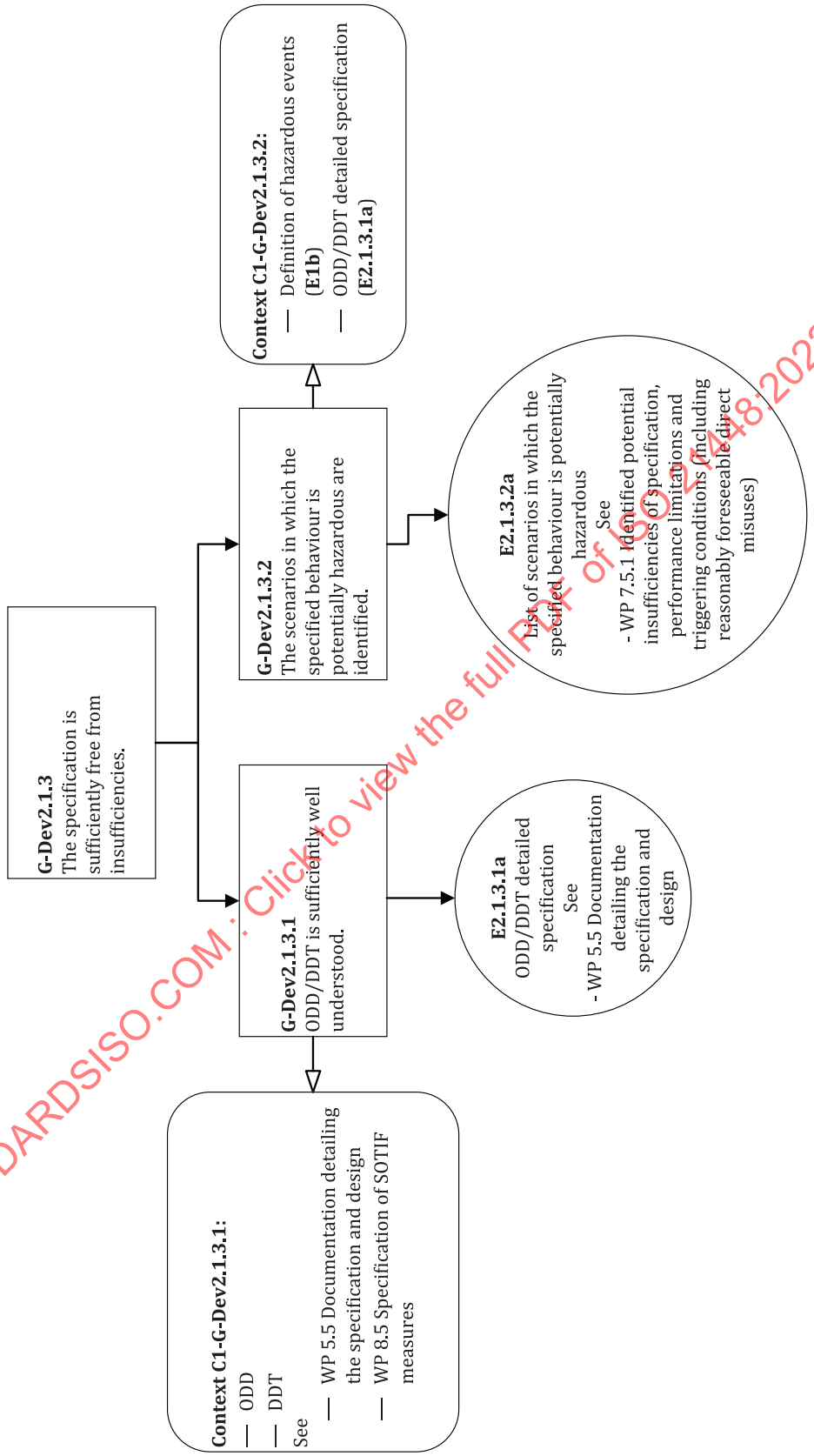


Figure A.8 — G-Dev2.1.3: specification is sufficiently free from insufficiencies

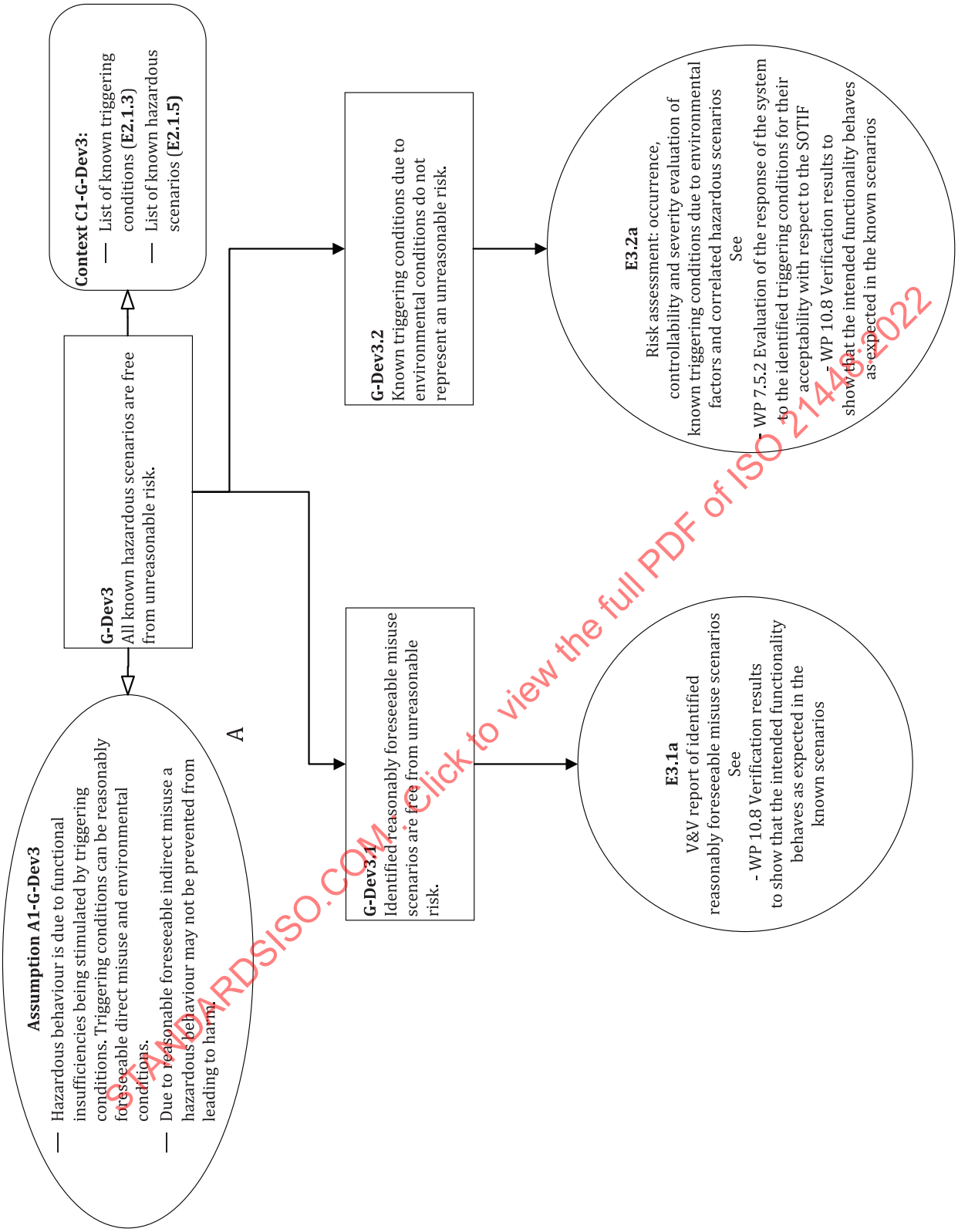


Figure A.9 — G-Dev3: all known potentially hazardous scenarios are free from unreasonable risk

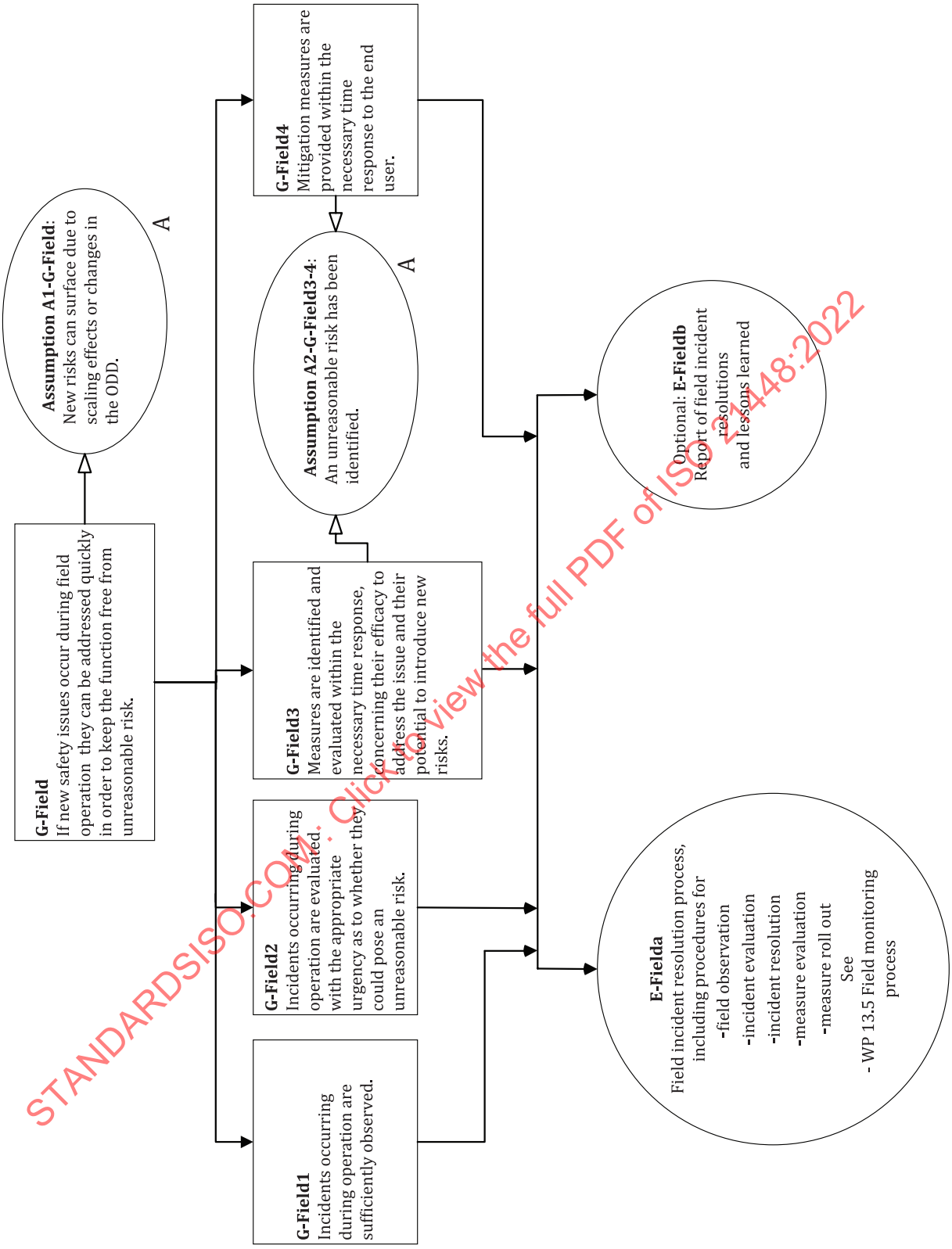


Figure A.10 — G-Field: if new safety issues occur during field operation they can be addressed quickly in order to keep the function free from unreasonable risk

A.1.3 GSN example 2

The example GSN (Figures A.11 to A.16) shows an argument structure to support the top goal: "the absence of unreasonable risk due to hazards associated with the intended functionality of the system or its reasonably foreseeable misuse has been achieved".

The argument structure presented is generic and applicable for all systems. It is developed down to the subgoal where further development becomes system specific. At this point, reference is made to topics mentioned in the standard that could be used to further develop each subgoal and provide the necessary evidence.

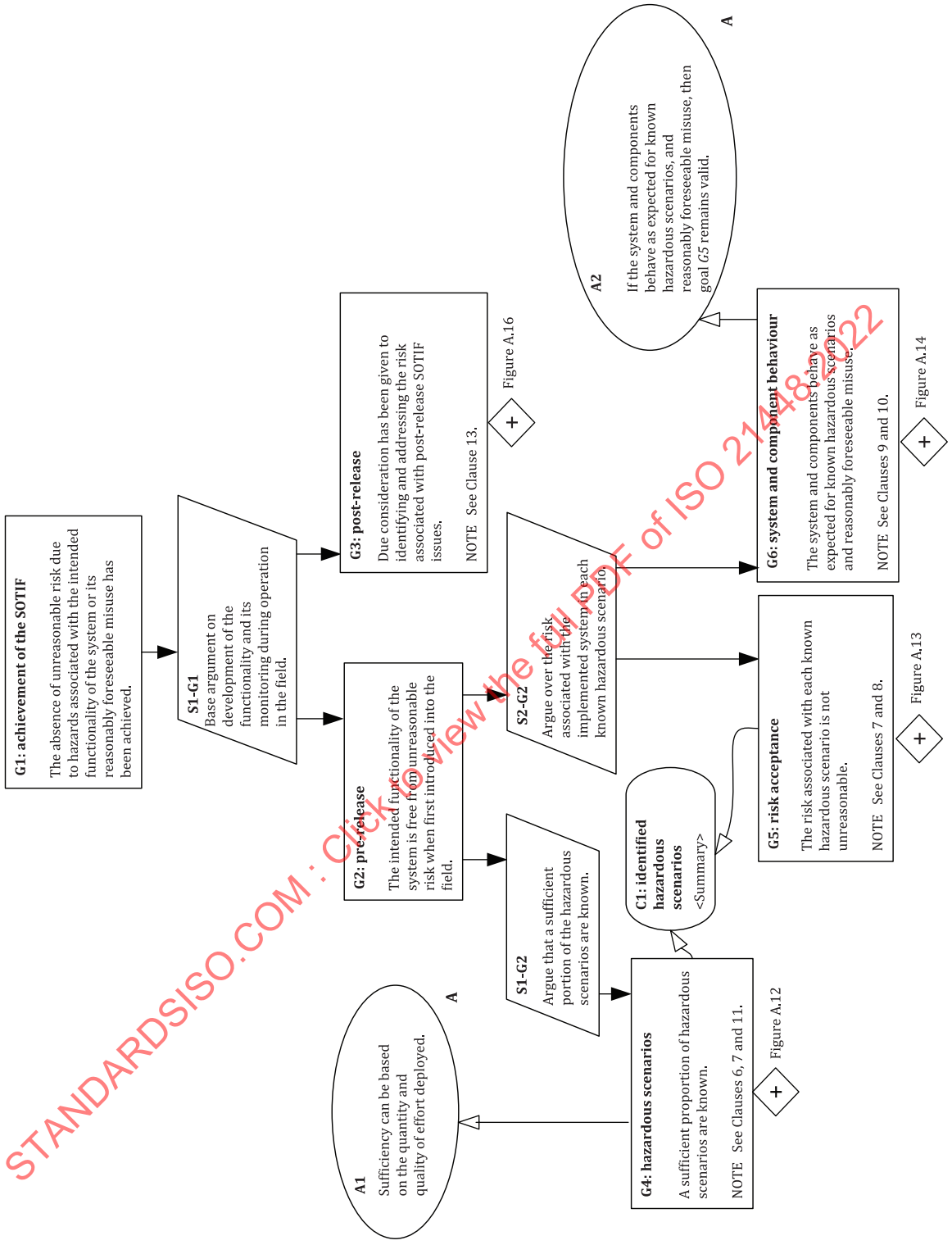


Figure A.11 — Absence of unreasonable risk due to hazards associated with the intended functionality of the system or its reasonably foreseeable misuse has been achieved

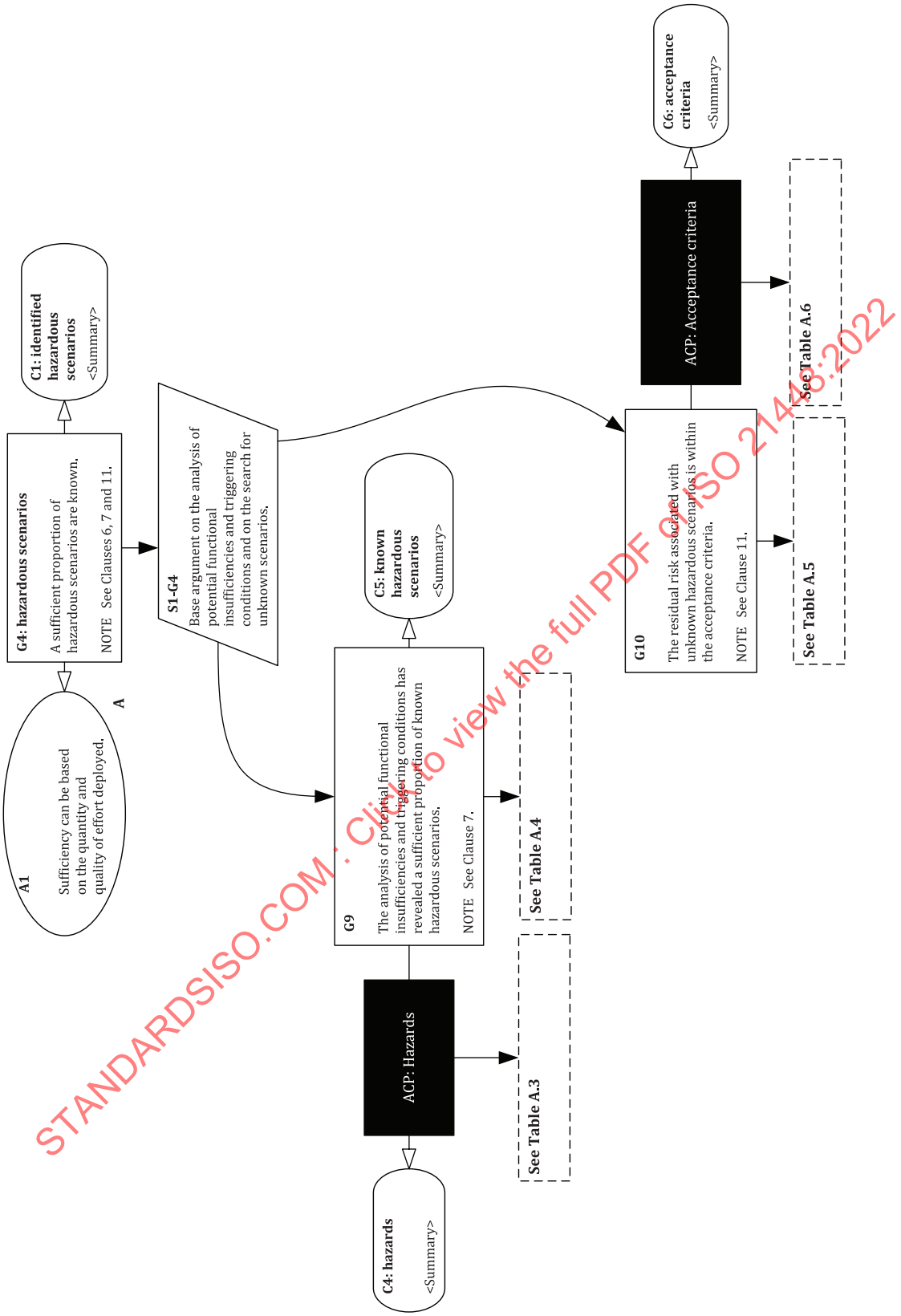


Figure A.12 — G4: potentially hazardous scenarios

Table A.3 — Topics relevant to the ACP: hazard claim (all hazards have been correctly identified)

Sufficiency of method(s) used to identify all the hazards resulting from functional insufficiencies
The definition of the method
The resource expended in deploying the method
The completeness and correctness of the risk evaluation
The capability of the review (according to Clause 12) of the evidence generated by the SOTIF activities to detect potential issues with the achievement of the SOTIF

Table A.4 — Topics relevant to the development of G9 (The analysis of potential functional insufficiencies and potential triggering conditions has revealed a sufficient proportion of known potentially hazardous scenarios)

Knowledge gained from similar projects
Knowledge gained from field experience
Known potential insufficiencies of specification and performance insufficiency
Previously identified environment conditions and reasonably foreseeable misuse
Sufficiency of methods, used in combination, to identify all potential functional insufficiencies and potential triggering conditions (Table 4)
The ability of each method to identify particular potential functional insufficiencies and potential triggering conditions (Table 4)
The definition of the method (Table 4)
The resource expended in deploying the method (Table 4)
Identification of potential functional insufficiencies and triggering conditions related to algorithms
Identification of potential functional insufficiencies and triggering conditions related to sensors and actuators
Analysis of reasonably foreseeable misuse (Table 5)
The capability of the review (according to Clause 12) of the evidences generated by the SOTIF activities to detect potential issues with the achievement of the SOTIF

Table A.5 — Topics relevant to the development of G10 (the residual risk associated with unknown hazardous scenarios is within the acceptance criteria)

Vehicle design (e.g. mounting position)
Sufficiency of the methods used to reveal hitherto unknown scenarios (Table 11)
The ability of each method to identify particular potential functional insufficiencies and triggering conditions (Table 11)
The definition of the method (Table 11)
The addressing of newly identified scenarios

Table A.6 — Topics relevant to the ACP: hazard claim (the acceptance criteria have been correctly defined)

Compliance with the defined acceptance criteria
The effort considered sufficient
The applicable governmental and industry regulations
The definition of the confidence to be demonstrated for the SOTIF
The use of available traffic data for the target market (C.2.2.4)
The use of pre-existing criteria from similar functions operating in the field
The rationale for chosen target, e.g. GAMAB, ALARP, MEM

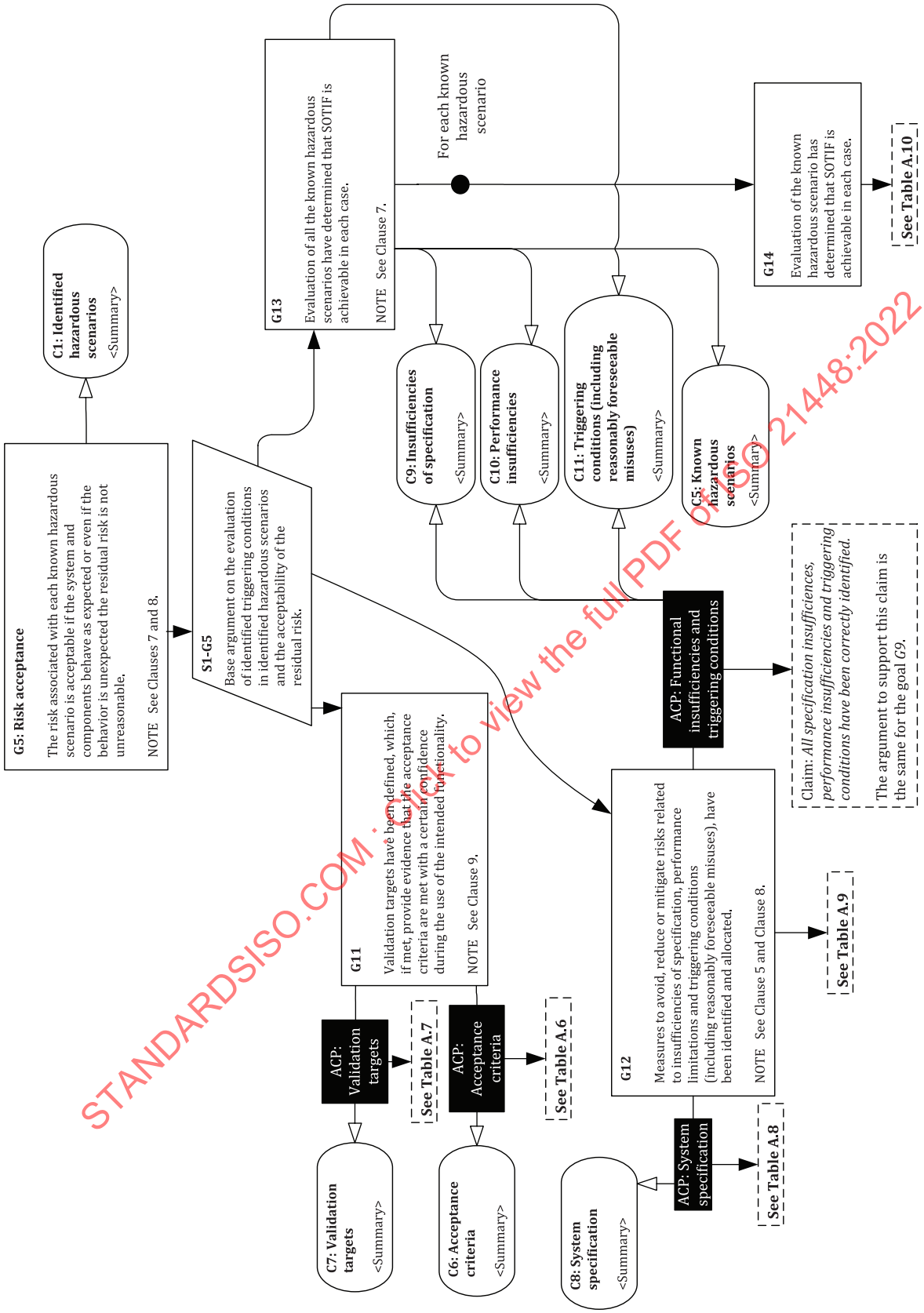


Figure A.13 — G5: risk acceptance

Table A.7 — Topics relevant to the ACP: validation targets claim (the validation targets have been correctly set)

Exposure to a subset of scenarios
Use of exposure, controllability and severity when evaluating a triggering condition

Table A.8 — Topics relevant to the ACP: system specification claim (the system specification has been defined completely and correctly)

The completeness and correctness of the ODD definition
The completeness and correctness of the description of intermediate level decision-making logic
The completeness and correctness of the description of the vehicle, and elements that can include system, sub-system, components, etc. implementing the intended functionality
The completeness and correctness of the description details of the authority and levels of driving automation of the function over vehicle dynamics
The appropriateness of the performance targets
The completeness and correctness of the description of the reasonably foreseeable misuse scenarios
The completeness and correctness of the description of the interfaces and interactions
The completeness and validity of the assumptions
The completeness and correctness of the description of the limitations of the system and subsystems and their countermeasures
The completeness and correctness of the description of the system architecture supporting the countermeasures
The completeness and correctness of the description of the warning and degradation concept
The completeness and correctness of the description of the data collection information supporting the intended functionality
The completeness and correctness of the description of the performance targets
The completeness and correctness of the description of the known potential performance insufficiencies and their countermeasures
The completeness and correctness of the description of the effectiveness of the iteration process in keeping the specification up to date
The completeness and correctness of the description of the effectiveness of the process for managing a distributed development
The completeness and correctness of the description of the system limitations
The completeness and correctness of the description of the robustness provided by the final system architecture
The capability of the review (according to Clause 12) of the evidences generated by the SOTIF activities to detect potential issues with the achievement of the SOTIF

Table A.9 — Topics relevant to the development of G12

Use of "avoidance" measures
Use of "reduction" measures
Use of "mitigation" measures
Use of system modifications to avoid or reduce the SOTIF-related risks
Use of measures to restrict the intended functionality
Use of measures for handing over authority from a system to the driver
Use of measures to reduce or mitigate the effects of reasonably foreseeable misuse
Adequacy of the process for updating the system specification with the modification

Table A.10 — Topics relevant to the development of G14

The use of expert judgement
The comparison of the residual risk to the acceptance criteria specified in 6.5

Table A.10 *(continued)*

The absence of known scenarios that could lead to an unreasonable risk for a specific vehicle

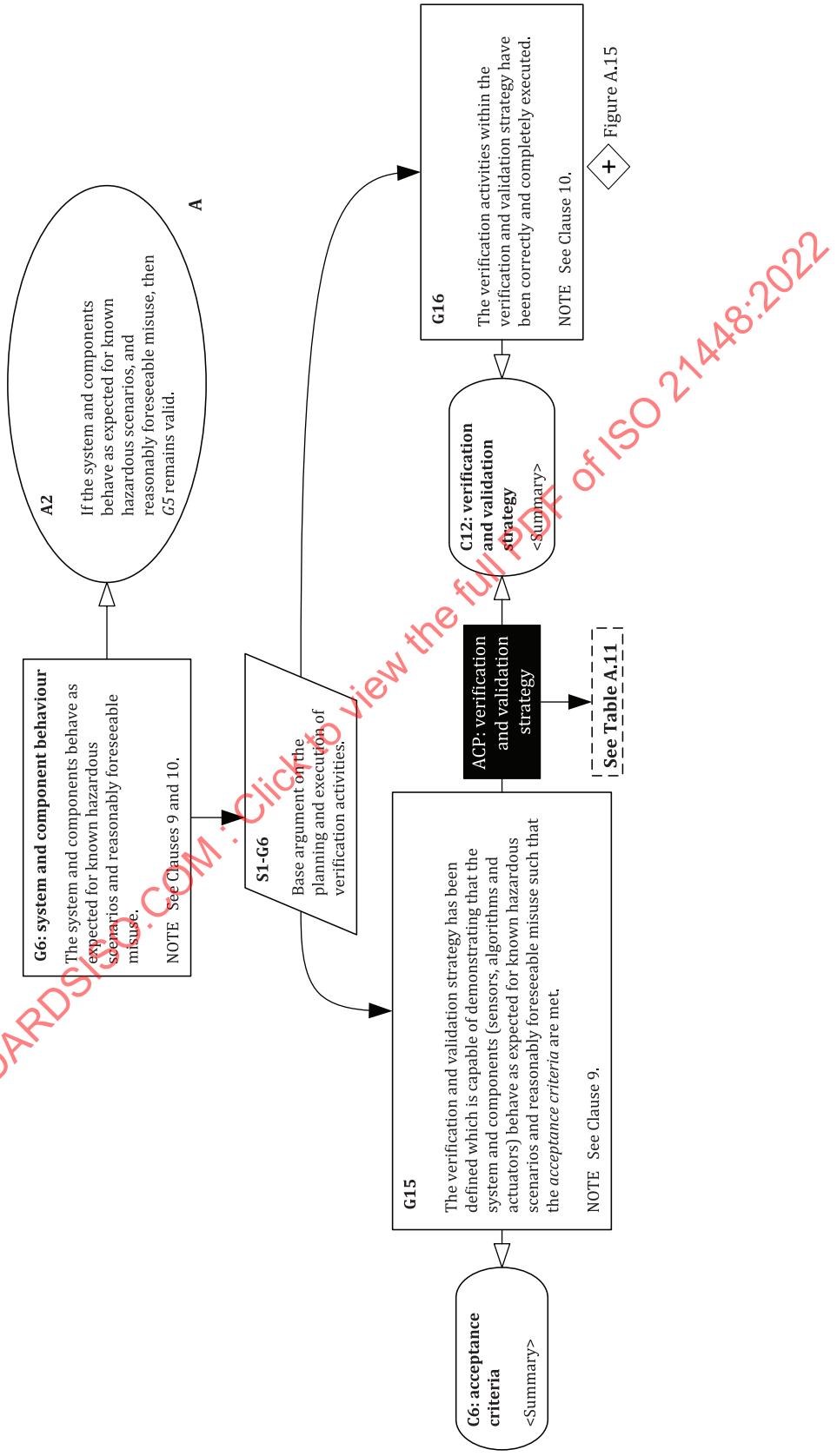


Figure A.14 — G6: system and component behaviour

Table A.11 — Topics relevant to the ACP: verification and validation strategy (the verification and validation strategy has been correctly defined)

The coverage of the known scenarios
Exposure to a subset of scenarios
Use of exposure, controllability and severity when evaluating a scenario with the hazardous behaviour
The rationale for the methods used to specify verification and validation activities (Table 6)
The capability of the strategy to verify the ability of sensors to provide accurate information on the environment
The capability of the strategy to verify the ability of the sensor processing algorithms to accurately model the environment
The capability of the strategy to verify the ability of the decision algorithms to safely handle the limitations of the technical capabilities of the elements
The capability of the strategy to verify the ability of the decision algorithms to make appropriate decisions according to the environment model and the system architecture
The capability of the strategy to verify the robustness of the system or function
The capability of the strategy to verify the absence of unreasonable risk due to the hazardous behaviour of the intended functionality
The capability of the strategy to verify the ability of the HMI to prevent reasonably foreseeable misuse
The capability of the strategy to verify the effectiveness of the fallback handover scenario
Rationale for the methods chosen (Table 7, Table 8, Table 9, Table 10)
Adequacy of the methods chosen (Table 7, Table 8, Table 9, Table 10)
The capability of the review (according to Clause 12) of the evidences generated by the SOTIF activities to detect potential issues with the achievement of the SOTIF

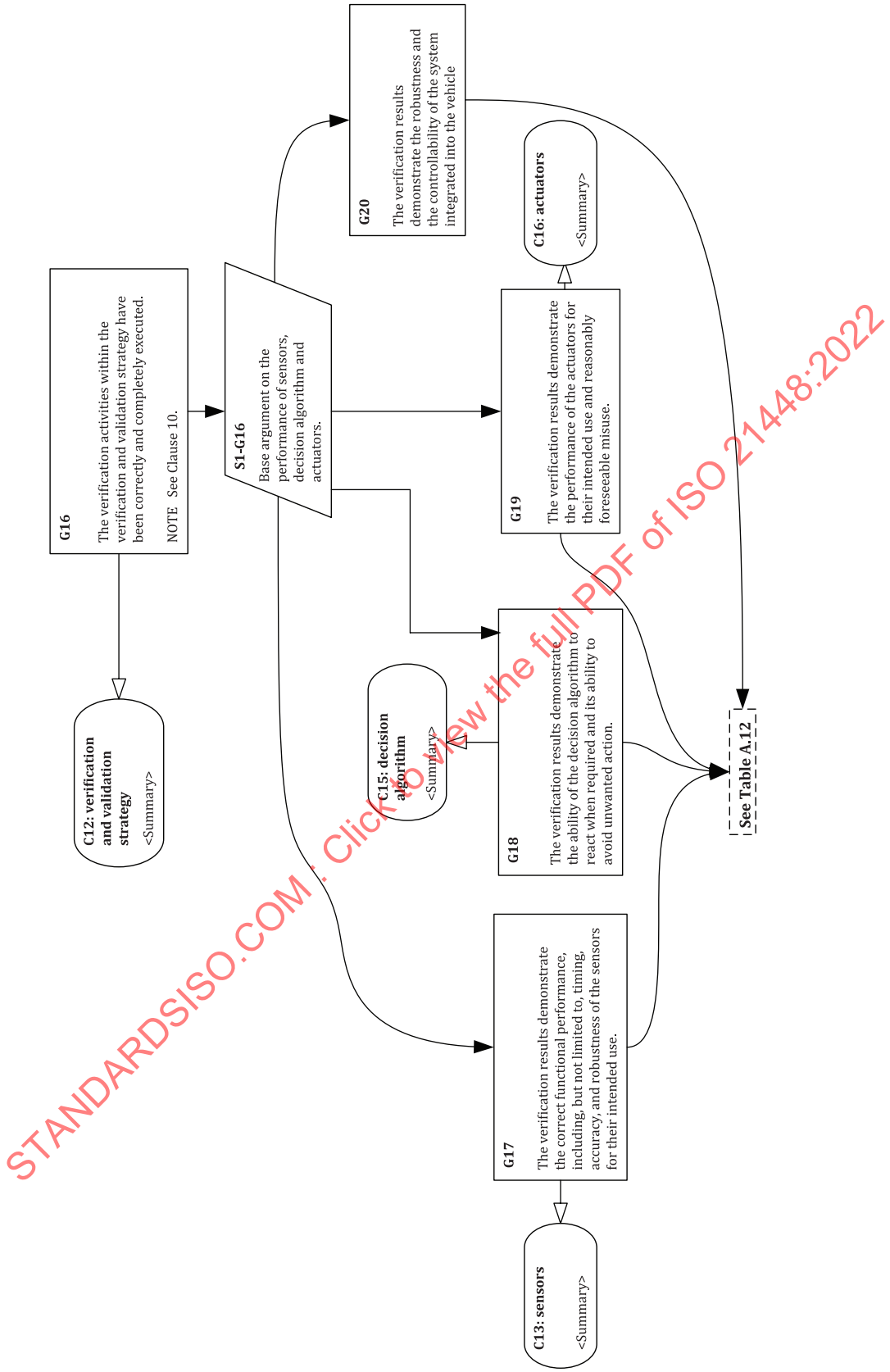


Figure A.15 — G16

Table A.12 — Topics relevant to the development of G17, G18, G19, G20

Vehicle design (e.g. mounting position)
Coverage of known scenarios
Compliance with Acceptance Criteria
Coverage of triggering conditions
Rationale for the methods chosen (Table 7, Table 8, Table 9, Table 10)
Adequacy of the methods chosen (Table 7, Table 8, Table 9, Table 10)
The definition of the method (Table 7, Table 8, Table 9, Table 10)
The resource expended in deploying the method (Table 7, Table 8, Table 9, Table 10)
The capability of the review (according to Clause 12) of the evidences generated by the SOTIF activities to detect potential issues with the achievement of the SOTIF

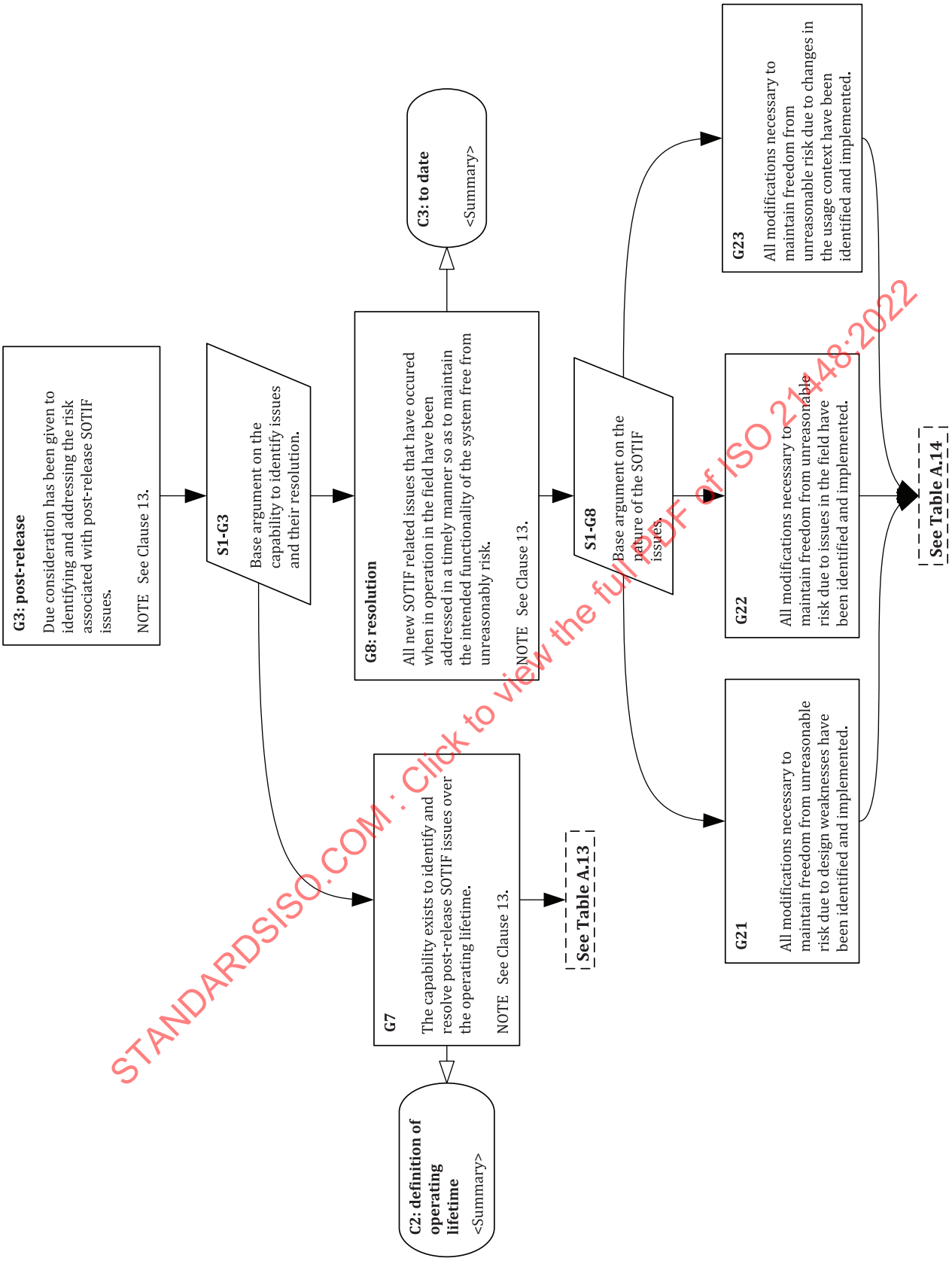


Figure A.16 — G3: post release

Table A.13 — Topics relevant to the development of G7

The adequacy of the on-board and off-board infrastructure for monitoring functional insufficiencies in use
The capability to identify, and respond to, potential weaknesses of the system
The capability to identify and correct design weaknesses
The capability to identify, and respond to, operational changes
The capability to collect field data
The capability to monitor SOTIF-related issues, including misuse of the system
The capability to use field data to identify issues
The capability to monitor the state of knowledge
The capability to monitor changes to the usage context
The capability to analyse and evaluate the identified risks
The capability to mitigate identified risks

Table A.14 — Topics relevant to the development of G21, G22, G23

The identification of, and response to, potential weaknesses of the system
The identification and correction of design weaknesses
The identification, and response to, operational changes
The use of field-monitoring data collection to enhance the databases used for SOTIF activities
The monitoring of SOTIF-related issues, including misuse of the system
The use of field monitoring to identify potential weaknesses
The monitoring of the state of knowledge to identify potential weaknesses
The monitoring of changes to the usage context to identify potential weaknesses
The analysis and evaluation of the identified risks
The mitigation of risks

A.2 Explanations regarding the interaction between functional safety according to the ISO 26262 series and this document

A.2.1 General

This subclause explains and provides examples of interaction between functional safety according to the ISO 26262 series and this document to show the potential for synergies.

For sake of simplicity, not all aspects of the discussed activities or work products are completely addressed. Therefore, there is no claim for completeness.

A.2.2 Scope of the ISO 26262 series versus the scope of this document

A.2.2.1 General

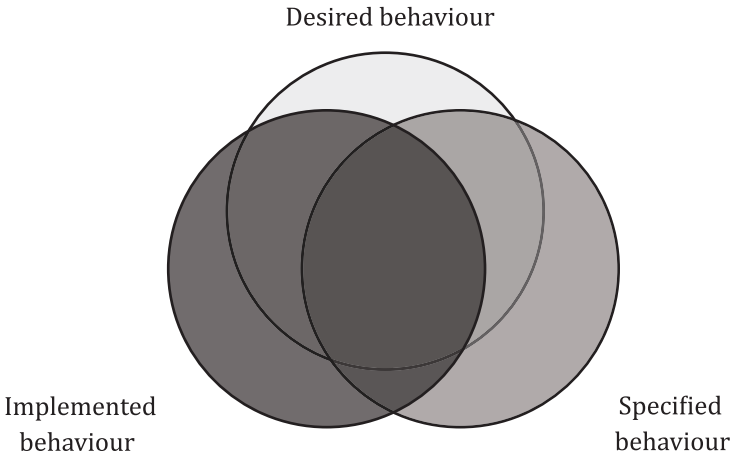
The differences and commonalities of both standards are further explained with the help of two different approaches:

— the three-circle behavioural model,

— the causality classification view of safety issues.

A.2.2.2 The three-circle behavioural model

The differences and the overlap of the scopes of the ISO 26262 series and this document are elaborated using the three-circle behavioural model described in Figure A.13 in Reference [15].



NOTE 1 The significant lack of overlap among the three circles is done for illustrational purposes only and does not imply the real situation.

Figure A.17 — Three circle behavioural model

In Figure A.17 each circle represents a different aspect of the behaviour.

— The desired behaviour is the ideal (and at times aspirational) behaviour from a safety point of view that does not consider any technical constraints. It reflects the user's and society's expectation of the system behaviour.

EXAMPLE 1 An automated driving function that never has an accident or causes an accident.

EXAMPLE 2 The desired behaviour of an AEB would be 100 % true positive and 0 % false positive braking.

NOTE 2 The desired behaviours are not necessarily always documented with all its possible aspects.

— The specified behaviour is a representation of the desired behaviour taking constraints into consideration (e.g. legal, technical, commercial, customer acceptance).

NOTE 3 According to Clause 3 the intended functionality is defined as the specified functionality. Hence the intended behaviour, defined as the behaviour of the intended functionality, is a synonym for the specified behaviour.

— The implemented behaviour is the real-world system behaviour.

Comparing the scopes of the ISO 26262 series and this document we can arrive at the following conclusions.

— The ISO 26262 series explicitly excludes the safety aspect of the nominal behaviour of the item in its scope, whereas this document explicitly includes the safety of the specified behaviour at the vehicle level, which corresponds to the nominal behaviour.

— The ISO 26262 series explicitly addresses the issue of E/E random hardware faults. This is not explicitly addressed by this document. However, the reaction to the random hardware fault, i.e. the emergency operation can have SOTIF aspects.

— To ensure that the implemented behaviour is as specified is a task of the ISO 26262 series and for certain complex systems (e.g. ADAS, AD systems) is a task of this document. For these systems the ISO 26262 series does not give enough guidance on how to ensure this. The issue is related to the open-context problem, i.e. the real world can never be 100 % accurately described or its correct perception cannot be 100 % validated. The systems that use complex algorithms and sensors like video, radar or lidar to perceive and classify their environment and derive their control action from this information are in the scope of this document.

EXAMPLE 3 A camera-based system has a function to detect humans. The algorithm can have issues incorrectly classifying humans when they wear clothing with a certain colour pattern. It is impossible to specify and test all possible colour patterns that clothing could have. This document is designed to describe additional requirements to the ISO 26262 series. The E/E elements relevant for SOTIF are considered as safety related elements of the ISO 26262 series.

EXAMPLE 4 If the software implemented algorithm for object detection can contribute to a safety goal violation or its achievement then it is considered to be a safety-related element in ISO 26262-1 terms.

A.2.2.3 The causality classification view of safety issues

In the causality classification view of the safety issues the differences and the overlap of the scopes of the ISO 26262 series and this document are shown in Figure A.18.

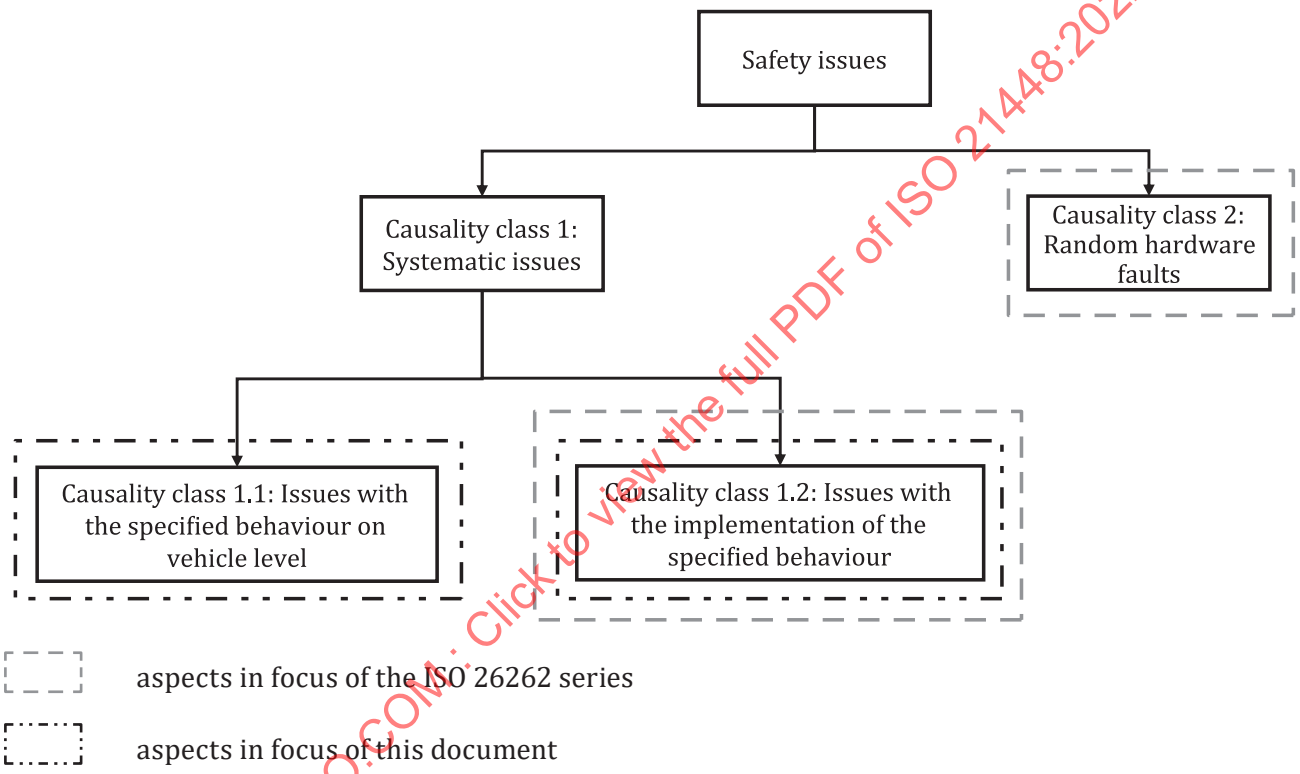


Figure A.18 — Safety issues causality classification scheme

NOTE 1 This classification scheme focuses only on safety issues caused by E/E systems addressed by the ISO 26262 series and this document. Other safety issues (e.g. due to electrical hazards) have been omitted for the sake of simplicity.

The scheme contains following classifications:

Causality class 1: systematic issues

This class contains safety aspects that potentially relate to systematic issues. This class can further be divided into:

— causality class 1.1: issues with the specified behaviour at the vehicle level;

— causality class 1.2: issues with the implementation of the specified behaviour.

Causality class 2: random hardware faults

This class contains safety issues caused by random hardware faults that are addressed by the ISO 26262 series.

Causality class 1.1: issues with the specified behaviour at the vehicle level

This class contains safety issues caused by the specified behaviour at the vehicle level. This document addresses the risk resulting from the specified behaviour at the vehicle level of the functionalities, for which proper situational awareness is essential to safety. The situational awareness is derived from complex sensors and processing algorithms (e.g. object detection via camera, lidar or radar). The causes in this class are referenced in this document as insufficiency of the specification at the vehicle level.

NOTE 2 The ISO 26262 series explicitly excludes the safety aspects of the nominal behaviour from its scope.

Causality class 1.2: issues with the implementation of the specified behaviour

The issues of this class are caused by performance insufficiencies, insufficiencies of specification on element level and other miscellaneous design and implementation issues.

These three types of systematic issues of causality class 1.2 are in scope of the ISO 26262 series since they are related to potential systematic failures of the E/E systems, subsystems, components or other elements, including those coming from SOTIF-related requirements.

On element level only performance insufficiencies and insufficiencies of specification are within the scope of this document, which are related to the intended functionality where proper situational awareness is essential to safety. Functions in scope at element level include:

— sense: perception of the environment (e.g. detection of surrounding static and dynamic objects, detection of the street layout and ego vehicle location using vehicle internal and vehicle external (e.g. V2X) data);

— plan: decision algorithms (i.e. the control algorithms that derive control actions based on the before mentioned perception); and

— act: actuation (i.e. the execution of the control requests derived by the before mentioned decision algorithms)

NOTE 3 If a certain safety issue cannot clearly be classified as a SOTIF or a functional safety issue then both standards can be applied to address the issue.

A.2.3 Alignment of this document with the ISO 26262 series activities

The alignment between this document and the ISO 26262 series product development activities is shown in Figure A.19. As the two standards handle different aspects of safety, both processes are considered for a solid safety argument of a product. The alignment of the activities between the standards is important to be able to implement possible modifications to the design of to the vehicle, and elements that can include system, subsystem, components, etc. at a sufficiently early stage.

At the beginning of the development process, the specification and design (according to Clause 5) can be aligned with the item definition of ISO 26262-3 (see A.2.4).

NOTE Clause 5 contains the functional and design specification across all levels of abstraction. This is not the case for the item definition which specifies the functionality on top level.

The identification and evaluation of hazards caused by the intended functionality is aligned with hazard analysis and risk assessment (HARA) of ISO 26262-3 (see A.2.5). Identification and evaluation of performance insufficiencies and potential triggering conditions consider system limitations and evaluate their acceptability with respect to the SOTIF (see A.2.7). This phase can be aligned with the definition of functional safety concept and technical safety concept of the ISO 26262 series (see A.2.6 and A.2.7).

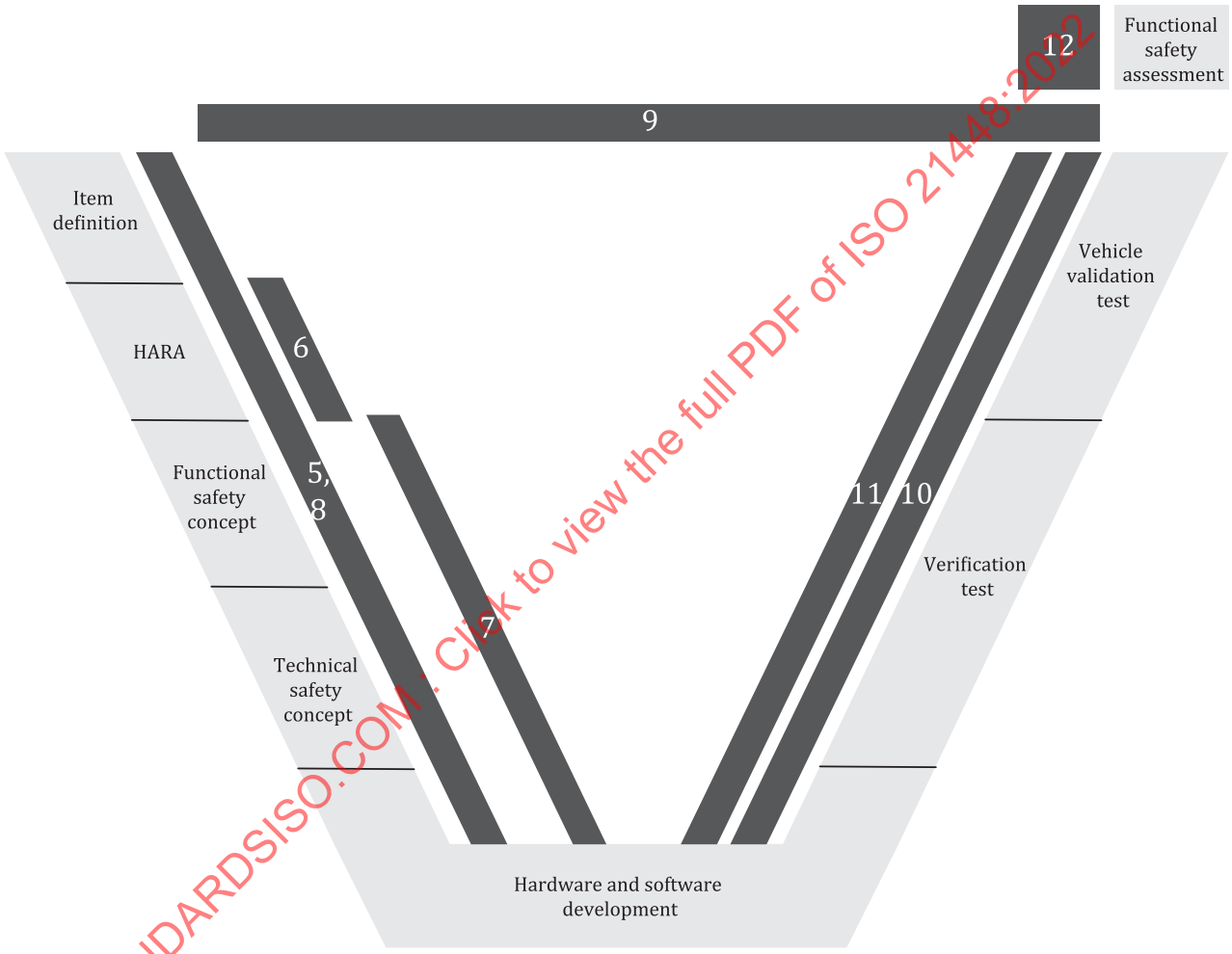
Functional modifications to reduce SOTIF risks (according to Clause 8) can be aligned with the left side of the ISO 26262 V-model.

When evaluating performance insufficiencies and potential triggering conditions at hardware (HW) and software (SW) component level, the activity can be aligned with HW and SW development activities

of the ISO 26262 series. The guidance for distributed SOTIF development and safety element out of context (SEooC) procedures is given in 4.4.2. The topic of the supporting processes of ISO 26262-8 is explained in A.2.9.

Verification and validation of the SOTIF can be aligned with the corresponding activities of the ISO 26262 series on the right side of the V-model (see A.2.10). Definition of the SOTIF V&V strategy is compiled from information produced on previous stages of the SOTIF development.

Evaluation of the achievement of the SOTIF and functional safety assessment conclude the development activities and are used for the overall system release. The monitoring of field operation is aligned with the ISO 26262-7 required field monitoring process.



Key

process step ISO 26262 series

X ISO 21448 process step, the number X references the corresponding clause

Figure A.19 — Possible interactions of product development activities between this document and the ISO 26262 series

A.2.4 Item definition and specification of the functionality at the vehicle level

The starting point for this document is the specification of the functionality at the vehicle level. For the ISO 26262 series, it is the item definition.

NOTE 1 An item is a system or a combination of systems implementing a vehicle function or part of a vehicle function. It is possible that a given vehicle function is implemented by multiple items. In this case, there will be a difference between the vehicle function and the function of the single items themselves.

NOTE 2 An item can contribute to the implementation of more than one vehicle function, resulting in the specification of more than one vehicle function (or a subset of these) as part of the item definition.

NOTE 3 The functionality specified at the vehicle level used for this document is the same as the vehicle function implemented by one or more items in the sense of the ISO 26262 series.

EXAMPLE 1 The vehicle function "autonomous emergency braking (AEB)" in this example is implemented by a radar sensor, a domain controller and a braking system [e.g. electronic stability control (ESC)] (Figure A.20).

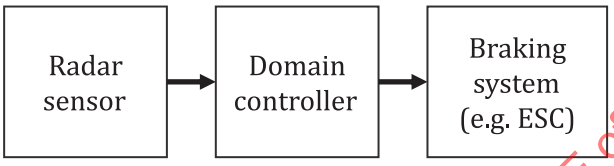


Figure A.20 — Example system architecture

The ISO 26262 series allows different ways to define the items. As an example, the vehicle function could be implemented by two items (radar sensor and domain controller being one item, the ESC being the other) or the vehicle function could be implemented by one item (radar sensor, domain controller and ESC).

In A.2.4 through A.2.10, the item is defined in such a way that it implements the whole vehicle function, i.e. the item function is equal to the vehicle function.

NOTE 4 Other functions implemented by the item are neglected in this example for sake of simplicity.

EXAMPLE 2 AEB specification of the functionality at the vehicle level: AEB function triggers maximum braking force:

— once an obstacle is detected and collision is unavoidable (this means that the collision cannot be prevented, but the severity of the impact can be reduced;

— with a maximum speed reduction of x km/h.

NOTE 5 Changes to improve the SOTIF (e.g. functional modifications, introduction of new elements) can also have an impact on the item definition.

A.2.5 HARA and identification and evaluation of hazards caused by the intended functionality

A.2.5.1 General

The ISO 26262 series focuses on E/E functions and in the HARA the malfunctioning behaviour is analysed based on the resulting hazards at the vehicle level. At the vehicle level, the behaviour leading to a hazard is the same whether it was caused by an E/E failure or an unsafe intended functionality (or even a security issue). However, there can be differences in the magnitude of these hazards, since in the case of a hazardous behaviour of the intended functionality authority limitations (e.g. limiting the maximal deceleration of an AEB) can be considered. Hazards and malfunctioning behaviours that are identified in a HARA can therefore be the same or similar as the ones considered for the SOTIF.

A.2.5.2 ISO 26262-3 Hazard analysis and risk assessment (HARA)

The HARA identifies the malfunctioning behaviours of the item and assesses the resulting risk.

EXAMPLE 1 Malfunctioning behaviour of the AEB item:

— UNDESIRED autonomous braking:

  — within specified speed reduction limits: ASIL *X* as a result of the E, C and S evaluation of the hazardous events;

  — outside specified speed reduction limits: ASIL *Y* as a result of the E, C and S evaluation of the hazardous events (with $Y \geq X$);

— TOO LATE or MISSED autonomous braking:

  — due to the high controllability (braking is a regular task of the driver) and the low exposure (emergency braking is a rare event), the hazardous events can be rated as QM.

NOTE (In relation to EXAMPLE 1 above) in other systems with higher levels of driving automation levels, the system can take over the responsibility for the driving task of braking in general, not only for emergency operations. In this case, the above statement might not be valid anymore.

The parameters of the HARA can be impacted by functional modifications motivated by SOTIF.

EXAMPLE 2 AEB function limits the maximum speed reduction while braking autonomously, this increases the controllability of the following vehicles to avoid a rear collision and reduces the severity of a collision.

A.2.5.3 Identification and evaluation of hazards caused by the intended functionality

This activity evaluates the vehicle function according to the following aspects:

— is the specified behaviour of the vehicle function safe?

— what are the undesired behaviours of the vehicle function and are they a source of credible harm?

— what are the risks due to reasonably foreseeable misuse?

EXAMPLE Risk identification and evaluation for AEB:

— Is the specified behaviour at the vehicle level safe in the specified use cases?

  If the specified behaviour can be the cause of an accident, evaluate if there is a more appropriate behaviour in the given context.

  According to the specification of the AEB system, it only intervenes when the collision is unavoidable. In such a scenario, the driver can brake with maximum force. If the driver does not do this, the AEB system takes over this task. This is the best possible behaviour, unless the driver wants to prevent the accident by lateral evasion. In the latter case, braking might even be counter productive, reducing the available lateral acceleration force. Due to this the specified behaviour at the vehicle level is modified: the AEB intervention is suppressed or aborted in case of y Nm steering torque. With this modification the specified behaviour at the vehicle level is considered safe.

  For the sake of simplicity further evaluation of this new add on is omitted in this example.

— What are the undesired behaviours of the vehicle function? Are they a source of credible harm?

  — False positive: undesired braking within specified speed reduction limits.

    — The following traffic could not react in time, leading to a rear collision. Here the system introduces a new risk. This undesired behaviour is a source of credible harm and with that, is SOTIF-related.

  — False negative: not braking in case of an imminent collision.

    — The system behaves as a pure assistant, i.e. it does not relieve the driver from the braking task nor will it give the impression of releasing the driver from this task since the driver will never experience the system to brake unless an accident is already unavoidable. From a SOTIF point of view, no new risks are introduced by the system by this undesired behaviour and it is not considered as a source of credible harm. Therefore, this undesired behaviour is not SOTIF-related.

      In other systems it could be possible that the system takes over the responsibility for the driving task of braking. In this case the above statement is no longer valid and this undesired behaviour becomes SOTIF-related.

  — Braking outside specified speed reduction limits

    — The capability to brake within the specified speed reduction limits depends on the accuracy of the vehicle speed measurement and the execution of the actuators.

    — Environmental potential triggering conditions which could lead to a braking outside of the speed reduction limits are conceivable (e.g. wind gust from front, quick increase in upward gradient) but it is assumed that the item's control loop would adapt to them quickly keeping over-braking within irrelevant limits

    — The performance insufficiencies of vehicle speed measurements, the braking control loop and braking actuation are well addressed by established systems. They do not require the SOTIF procedure described in this document. This undesired behaviour is not relevant for this document.

— What are the risks due to reasonably foreseeable misuse?

  — Misuse scenario: driver will transfer “braking on object” task to the AEB system.

    — In the user manual, it is clearly mentioned that the system is only assisting the driver and does not prevent the collision, it just reduces the effect.

    — The system brakes in a very uncomfortable manner.

    Therefore, the risk that the driver will transfer the driving task of braking completely to the system is not unreasonable.

    In general, the driver is informed about the limitations of the system (e.g. via the user manual), in order to reduce the likelihood of misuse.

    Care is taken that sales material including advertising and product naming does not lead to incorrect expectations of the user.

A.2.5.4 Conclusion

Care is taken so that the results of the identification and evaluation of hazards caused by the intended functionality and the HARA are consistent. In the example used in A.2.5, this is the case for the malfunctioning behaviour / undesired behaviour “undesired braking” and “Not braking in case of an imminent collision”. Undesired behaviour identified within the identification and evaluation of hazards caused by the intended functionality and malfunctioning behaviour identified within the HARA can lead to the same hazards.

Identification and evaluation of hazards caused by the intended functionality and the HARA do not necessarily always cover the same topics. Evaluating the specified behaviour concerning its safety is a typically SOTIF topic.

Only reasonably foreseeable indirect misuse is considered in ISO 26262 HARA as possible causes of reduced controllability or increased severity when evaluating a hazardous event caused by a malfunctioning behaviour of the item.

Reasonably foreseeable indirect misuse is similarly considered in this document when evaluating a hazardous event caused by a hazardous behaviour of the system. However, this document also considers reasonably foreseeable direct misuse, that is considered as a possible triggering condition.

Some aspects of these activities, for example, the controllability evaluation, can be viewed both as a SOTIF as well as a functional safety topic.

A.2.6 Functional safety concept and SOTIF functional specification

The functional safety concept specifies the fault reaction (e.g. emergency operation, transition into the safe state, etc.). For ADAS and automated driving systems, this fault reaction can also be a SOTIF issue. For these systems, SOTIF determines the necessary functionality in order to execute the specified fault reaction in a safe manner. The task of functional safety is to ensure the availability of the defined necessary functionality in case of a fault (e.g. via fault tolerance) or to ensure that the probability of the fault occurring is sufficiently small (e.g. via fault prevention).

Defining a safe fault reaction itself can be viewed as a SOTIF task as well as a functional safety task.

EXAMPLE In case of an automated driving function: the fault reaction can be for example:

— safe stop in the current lane,

— drive to the next parking lot.

NOTE The consistency of the functional modifications of Clause 8 with the requirements derived from the ISO 26262 series in the functional safety concept can be achieved by proper information exchange and/or reviews.

A.2.7 Technical safety concept and SOTIF

As a result of SOTIF activities the system design might change (e.g. by introducing new sensors), which can have an impact on the technical safety concept.

Also, as a result of functional safety activities, the system design might change (e.g. by introducing new sensors) which can have an impact on the SOTIF.

A.2.8 Safety analysis

The analysis activities to ensure the functional safety and the SOTIF focus on the functional chain and use the same design as a starting point, but have different viewpoints. The analysis for functional safety addresses systematic issues with the implementation of the specified behaviour and random hardware faults of the E/E elements.

The analysis for SOTIF (Clause 7) focuses on functional insufficiencies, their potential triggering conditions and their impact on the vehicle behaviour. In addition, reasonably foreseeable indirect misuse is also considered in this context (Clause 6, Clause 7).

The safety analysis for the ISO 26262 series can be used as an input for the SOTIF analysis and vice versa.

The aspects of the safety of the specified behaviour at the vehicle level and the risk resulting from reasonably foreseeable misuse are unique for the analysis for SOTIF.

A.2.9 Supporting processes

This document does not explicitly formulate requirements concerning the development process itself. The suitability of the development process is important to achieve safety and is addressed by existing standards such as IATF 16949 and the ISO 26262 series. For instance, the supporting processes of ISO 26262-8 are assumed to be adapted, if necessary, and applied to support the achievement of the SOTIF, for example:

— the Development Interface Agreement (DIA) according to ISO 26262-8:2018, Clause 5 is elaborated to also address the SOTIF aspects (see 4.4.2);

— confidence in the use of software tools according to ISO 26262-8:2018, Clause 11 can be applied to the tools relevant to achieve the SOTIF with a few adaptations.

NOTE 1 In addition to explicit tool errors, the capability of a simulation tool to represent the real world within certain tolerances can be of particular relevance in the SOTIF context.

NOTE 2 The accuracy of the real-world data measurement itself can be of particular relevance in the SOTIF context.

A.2.10 Verification and validation

Verification and validation strategy (see Clause 9) as well as the specified test cases (see Clauses 10 and 11) addressing SOTIF-related requirements can also take functional safety requirements into consideration.

As some test cases can address SOTIF as well as functional safety issues, some test cases address aspects of functional safety (e.g. the capability of a safety mechanism to detect and signal a random hardware fault) or SOTIF (e.g. tests to evaluate the sufficiency of the specified behaviour at the vehicle level) alone.

A.3 Simplified SOTIF application examples

Table A.15 provides a comparison of simplified examples of domain relevant SOTIF hazards and mitigations as a function of increasing vehicle autonomy for the reason of comparison of different kinds of functionalities.

Table A.15 — Simplified examples of domain relevant SOTIF hazards and mitigations

	Driver assistance (L1- per Clause 3 Table 2)	Partial driving automation (L2- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	High driving automation (L4 per Clause 3 Table 2)
System example	**Adaptive cruise control**	**Adaptive cruise control combined with lane keeping**	**Automation for traffic jam convenience**	**Highway co-pilot**	**Robo-taxi**
System description	This function enhances standard automotive cruise control using a sensor to detect a lead vehicle. If the lead vehicle is getting too close the feature will take action by slowing the vehicle to match the speed of the lead vehicle.	This function uses sensors to maintain vehicle position in the centre of the lane and detect a lead vehicle to adjust vehicle speed to maintain a pre-set headway.	This function uses sensors to maintain a safe longitudinal distance from the lead vehicle when in a traffic jam on the highway. It includes steering so as to stay in the lane of travel.	This function uses multiple and diverse sensors to autonomously navigate in traffic, executing all necessary manoeuvres for highway driving.	This function uses multiple and diverse sensors to autonomously navigate in traffic from point A to point B within a defined geo-fenced area.
DDT- lateral and longitudinal vehicle motion control	Driver and system	System	System	System	System
DDT- OEDR	Driver	Driver	System	System	System
DDT- fallback	Driver	Driver	Fallback-ready user [a]	Fallback-ready user [a]	System
Operational use case(s)	1) Maintain headway to lead vehicle up to set speed 2) When there is no lead vehicle in front of the ego vehicle, maintaining desired speed	1) Following a lead vehicle in lane up to set speed and headway 2) When there is no lead vehicle in front of the ego vehicle, maintaining desired speed and following lane	1) Following a lead vehicle that is operating at or below x km/h at a distance no greater than y m 2) If lead vehicle changes lanes, maintain following the next immediate lead vehicle, or if no lead vehicle present then driver is requested to take back control of the vehicle	All highway related use cases (following, lane keeping, merging, passing, etc.)	All urban and highway related use cases (following, passing, merging, stopping for traffic controls, etc.)

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

Table A.15 *(continued)*

	Driver assistance (L1- per Clause 3 Table 2)	Partial driving automation (L2- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	High driving automation (L4 per Clause 3 Table 2)
Operational design domain	The system is operational when vehicle is operating at or above x km/h.	The system is operational when vehicle is in a detected lane and is operating at or above x km/h.	The system is operational when the vehicle is within the geo-fence (mapped area), in a valid lane, and operating below x km/h in most environmental conditions (the feature is assumed to disengage in case of adverse environmental conditions such as thick fog, heavy rain, etc.).	The system is operational on mapped highways in most environmental conditions (feature is assumed to disengage in case of adverse environmental conditions such as thick fog, heavy rain, etc.).	The system is operational in a geo-fenced mixed highway and urban area in all environmental conditions except extreme weather (as defined in the specification).
Example of an intended behaviour/functionality	Maintain a safe headway with the lead vehicle. If the lead vehicle is getting too close, the feature will apply an appropriate brake force to maintain a safe headway. If it detects that the lead vehicle is far off, the feature will apply an acceleration until the user's pre-set speed is reached.	Maintain lane boundaries and maintain a safe headway with the lead vehicle. If the lead vehicle is getting too close, the feature will apply an appropriate brake force to maintain a safe headway. If it detects that the lead vehicle is far off, the feature will apply an acceleration until the user's pre-set speed is reached. Lateral control is applied to stay in lane.	The system requests that the user takes control in case of adverse environmental conditions like thick fog (user expected to take control before exiting the ODD).	Execute a zipper merge making lateral manoeuvres while leaving appropriate time and space for others.	Exhibit caution in occluded areas.

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

Table A.15 *(continued)*

	Driver assistance (L1- per Clause 3 Table 2)	Partial driving automation (L2- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	High driving automation (L4 per Clause 3 Table 2)
An example of SOTIF hazard requiring mitigation	System brakes when approaching a bridge perceiving it incorrectly as a static metal object in the roadway.	Ego vehicle and lead vehicle are operating in a merge lane. The lead vehicle merges into the intended lane and the ego vehicle now no longer detects a lead vehicle so it begins to accelerate to the previously pre-set cruise control speed. The ego vehicle driver is unable to merge into the intended lane before the merge lane ends and goes off the road.	The fallback-ready user does not take control when requested because the user did not observe the visual alert and the system enters a heavy fog area where it cannot perceive objects with acceptable precision.	Vehicle failed to merge successfully due to the inability to detect a vehicle with lighting and colouring that spoofed the automated system into misclassifying the vehicle as nominal skyline.	A large vehicle in the adjacent lane occludes a traffic light, the robo-taxi does not perceive the traffic light and proceeds into the intersection when the light is red.
An example of SOTIF mitigation	Software algorithm is enhanced to differentiate between vehicles and road infrastructure (i.e. steel bridge, steel covering).	The feature has limited acceleration authority.	The vehicle is designed to be able to detect the impeding heavy fog condition and provide a visual alert to the fallback-ready user. If the fallback-ready user does not take control, the system uses other methods to notify the driver by stimulating other driver senses such as audio, touch, kinematic (such as short brake pulses).	An orthogonal and independent collision mitigation algorithm that is separately evaluating the raw sensor data verifies that the generated path is collision free before it is accepted by the lower level controllers.	The vehicle rationalizes map data with perception data to look for a traffic light state before proceeding into an intersection and understands that the presence of the large vehicle is creating an occlusion of the traffic light. An appropriate behaviour is chosen.

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

With respect to verification and validation there are many commonalities regardless of level of driving automation.

Evaluation of the SOTIF mitigation measure regarding the known potentially hazardous scenarios:

1) analytical efforts to expose new potential triggering conditions;

2) exercising the feature in the context of the known scenario where the mitigation is demonstrated.

This can be achieved using a combination of sub-system and system level testing on a closed course, simulation, or open road.

Evaluation of the SOTIF mitigation measure regarding the unknown potentially hazardous scenarios:

a) analytical efforts to influence the V&V strategy to expose undiscovered potential triggering conditions;

b.) exposure across the ODD in closed course, simulation, and open road continues to achieve the validation target in order to show that the residual risk of unknown potentially hazardous scenarios is acceptable.

When expanding an ODD (such as exporting feature to other cities or countries) the changes within the ODD and OEDR are identified and evaluated. This can lead to the necessity to repeat test and simulation activities.

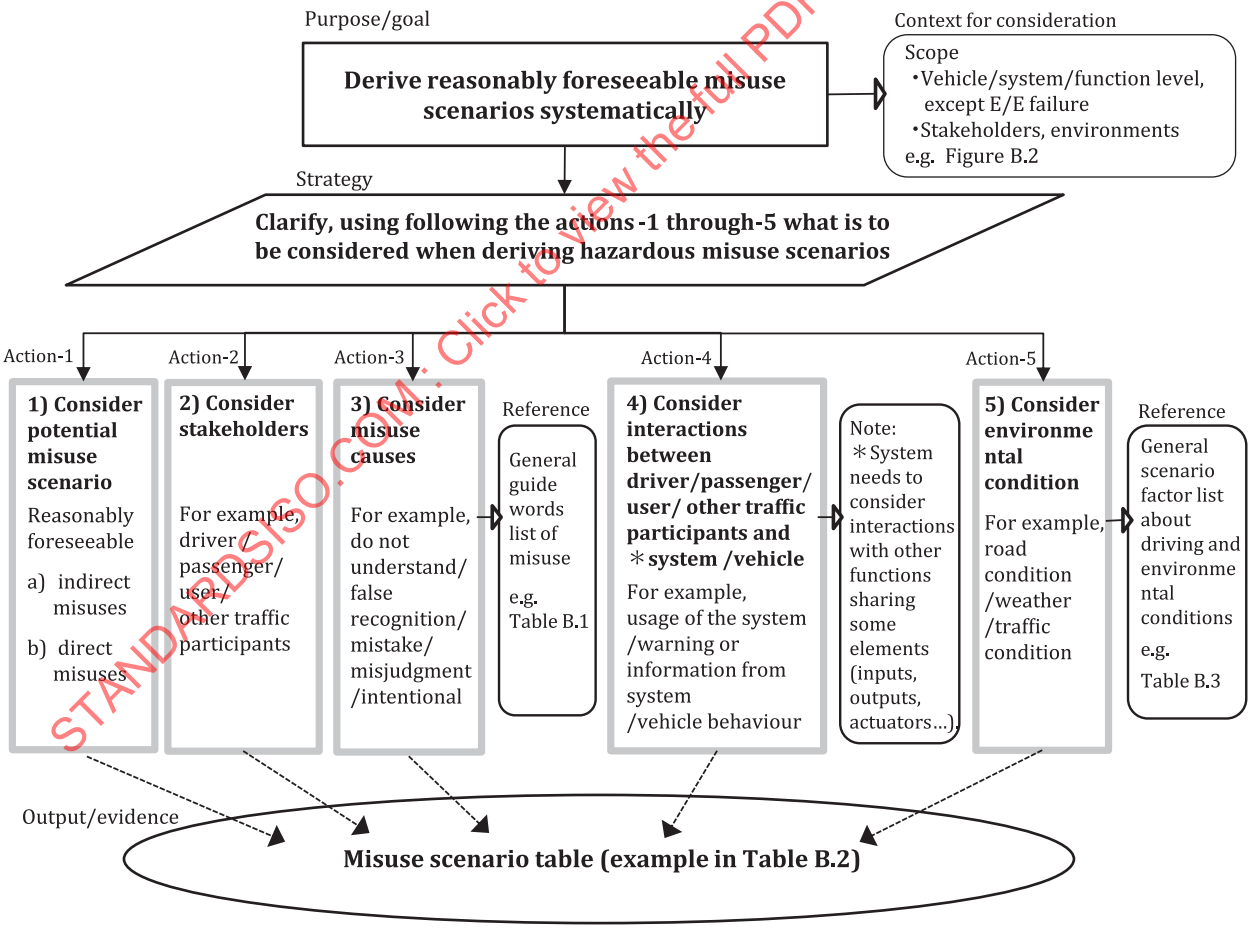
Annex B
(informative)

Guidance on scenario and system analyses

B.1 Method for deriving SOTIF misuse scenarios

B.1.1 Overview

For systems that are SOTIF-related, it is important to consider potential reasonably foreseeable misuse when performing the safety analysis. Scenarios containing SOTIF-related misuse can be derived from various sources, such as: lessons learnt, expert knowledge, brainstorming by designers, etc. B.1 gives an example methodology for systematically deriving SOTIF-related misuse to support the SOTIF safety analysis. The concept overview of this example methodology is given in Figure B.1 and an example of a SOTIF-related misuse is outlined. The approach to the human factors analysis is described in Reference [16].



NOTE For the meaning of the symbol shape of each element in Figure B.1 refer to Table A.1.

Figure B.1 — Systematic derivation of SOTIF-related misuse scenarios (example)

Points to consider and an example scenario factor table for scenarios containing SOTIF-related misuses are described in B.1.2.

B.1.2 Flow of safety analysis method for misuse

The points that can be considered when deriving the SOTIF-related misuses are described below.

1) Potential misuse scenario

   Consider the two types of misuse cases:

   — "reasonably foreseeable indirect misuses", are considered in combination with potentially hazardous system behaviour when identifying hazardous events; and

   — "reasonably foreseeable direct misuses", which could directly initiate a hazardous behaviour, as a potential triggering condition.

2) Stakeholders

   Consider who initiates the SOTIF-related misuse that leads to the hazard (e.g. driver, passenger, user, other traffic participants).

3) Misuse causes

   When considering the SOTIF-related misuse causes, general guide words derived from the typical human misuse process (recognition, judgment and action) can be useful.

   Examples of possible guide words are described in Table B.1.

Table B.1 — Guide words for human error

Process	Guide word	Example
Recognition	1. Does not understand	Cannot operate correctly due to complicated usage or insufficient information.
	2. False recognition	Cannot recognise correctly due to being overloaded with information.
Judgment	3. Judgment error/misjudgement	Misjudgement due to wrong impression or misunderstanding (e.g. changing the environment of a GNSS antenna by mounting a bike rack).
Action	4. Slip/mistake	Mistake due to loss of concentration (distraction, drowsiness, automation complacency, etc.).
	5. Intentional	Violation of social rules, commonly accepted human behaviour, correct operation (according to user manual).
	6. Unable	Difficult to operate

4) Interactions between the driver/user, system and vehicle

   A possible cause of misuse might be miscommunication or a time constraint on the interaction between the driver/user and the system/vehicle interfaces (see Figure B.2).

   For example, the following interface subjects can be derived:

   — system operation by the driver (usage): interface from driver to system/vehicle;

     EXAMPLE 1 The system, which is expected to be activated by the voice instruction of the driver, might also be activated unexpectedly due to the key words being spoken in the conversation between occupants.

   — warning notification from the system: interface from system/vehicle to driver; and

   — system/vehicle behaviour: interface from system/vehicle to driver.

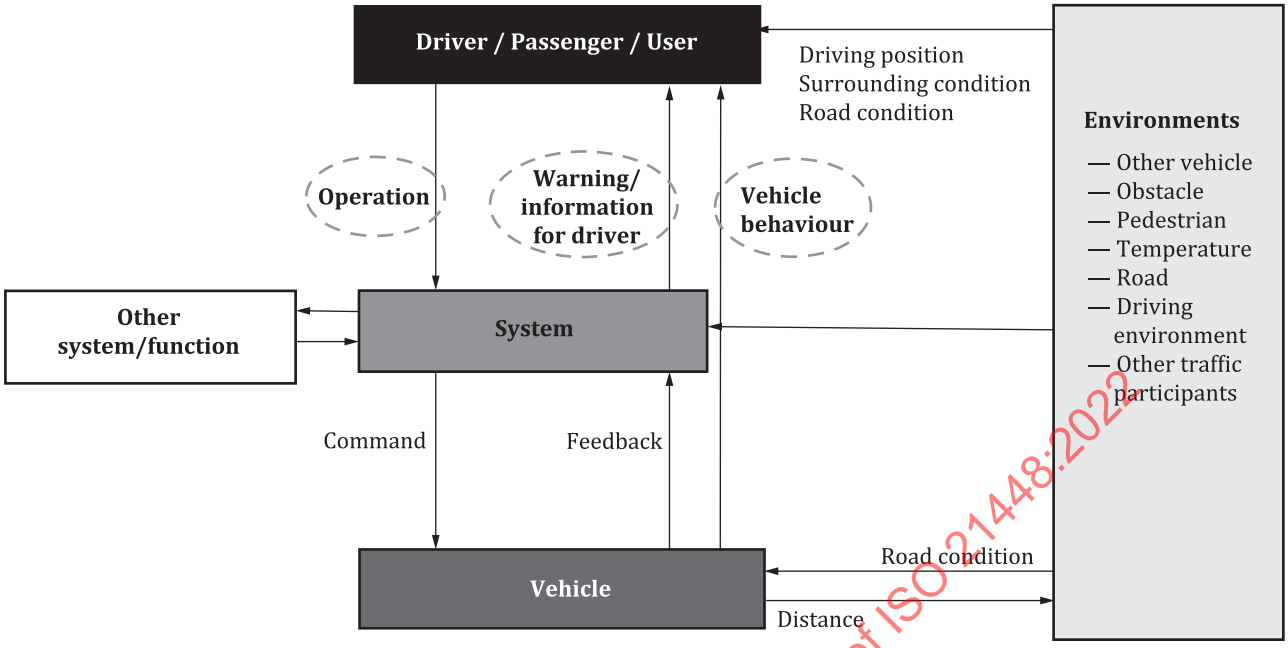


Figure B.2 — Example of interactions between the driver/user, system and vehicle

NOTE 1 The boxes and arrows in Figure B.2 have the following meaning:

— boxes: possible external factors interacting with the system;

— arrow: possible interaction.

5) Consideration of the environmental conditions in use case and scenarios

The impact of the environment, including road conditions, can be considered when deriving the SOTIF-related misuse.

EXAMPLE 2 Some environmental conditions for consideration in use cases scenarios are described in Table B.3 or Table B.4.

NOTE 2 Table B.3 or Table B.4 can be used both for the functional insufficiency scenario analysis and for analysis of scenarios containing SOTIF-related factors. As alternative, misuse cases can be linked to the hazard identification activity (see clause 6) and the driving situation catalogue used there.

The scenarios containing SOTIF-related misuse are derived considering points 1) to 5), in that case a scenario table, such as Table B.2, can be used.

NOTE 3 Methods such as HAZOP and STPA (System-Theoretic Process Analysis, an application example of which is shown in B.4) can be useful in deriving SOTIF-related misuse scenarios.

NOTE 4 The Figure B.1 method is not intended to be a comprehensive analysis of all combinations. The methods outlined in Figure B.1 are intended as an example that can be used to initiate the derivation of the analyses required for a specific SOTIF development. Only factors that influence hazardous events are selected for the analysis. Factors that have no influence on hazardous events can be recorded as not applicable.

Table B.2 — Example of misuse scenario table based on guide word approach similar to HAZOP

1) Potential SOTIF-related misuse scenario	2) Stake-holders	3) Misuse causes		4) Interactions between driver and system/ vehicle	5)Environmental conditions (refer to Table B.3)	Derived hazardous misuse scenario
		Process	Guide words			
While performing Level 2 DDT, like operating a lane keep assistance and adaptive cruise control on a highway, the vehicle cannot estimate the location of the lane boundary due to a performance insufficiency. The driver is notified, if lane boundary information is lost as the system is not able to detect if the vehicle would leave the lane.	Driver …	Recognition	1. Does not understand	Operation (usage)	…	…
				Vehicle behaviour	…	…
				Warning/ information	Highway, curve, lane white line suddenly changes to unclear.	Driver does not take over control of the vehicle and vehicle departs the lane because the driver does not know the meaning of the warning.
			2. False recognition	Operation (usage)	…	…
				Vehicle behaviour	…	…
				Warning/ information	…	…
		Judgment	3. Judgment error/ misjudgement	…	…	…
		Action	4. Slip/ mistake	…	…	…
			5. Intentional driver vacated seat	…	…	…
			6. Unable driver not paying attention driver asleep	…	…	…
…	…	…		…	…	…

B.2 Example construction of scenario factors for SOTIF safety analysis method

This subclause gives an example methodology for developing scenarios to support the hazard identification (Clause 6), the safety analysis (Clause 7) and the creation of verification/validation scenarios for known and unknown triggering conditions (Clauses 10 and 11).

The following steps are taken to identify and evaluate potential triggering conditions that affect system performance through causes such as parts characteristics, process, physical phenomena and environmental conditions.

1. For the purpose of this analysis, the system functions might be decomposed into the following elements: sense, plan, act.

2. Construct scenarios with potential functional insufficiencies from influencing factors (refer to Table B.3 or Table B.4) for each element of a triggering condition.

   NOTE 1 Tables from HARA situation generation in the context of the ISO 26262 series can be included into the generation of SOTIF-related scenarios.

   NOTE 2 A proposal on how to derive a representative set of concrete test scenarios for a manoeuvre under consideration can also be found in Reference [17].

Table B.3 — Examples for scenario factors (non-exhaustive) - Case 1

Category	Factor
Weather	fine
	cloudy
	rainy; “light rain”, “heavy rain”
	sleet
	snow (accumulation of snow); “light snow”, “heavy snow”
	hail
	fog; “dense fog”, “light fog”
	wind
Time of day	early morning
	daytime
	evening
	night
Shape of road/ lane	straight
	curve
	downhill
	uphill
	banked road
	step difference
	uneven spot (uneven road)
	Belgian brick road
	narrow road, wide road
	existence of median
	manhole cover
	merging on roadway
	branching
	pothole
Road feature	tunnel
	underpass
	bridges
	skyways
	cloverleaf
	diamond
	toll booth
	gate
Road condition	dry
	wet
	low μ surface
	crossover road
	water trough
	gravel road

Table B.3 *(continued)*

Category	Factor
Lighting	direct sunlight (glare)
	night with no moon
	moonlit night
	streetlamp
	backlight
	twilight
Condition of the ego vehicle	irregular disturbance of a sensor (e.g. impact causes change in field-of-view of the sensor)
	sensor variation (e.g. looseness at assembly)
	a sensor is fogged up
	a sensor is contaminated (dust, mud, snow, ice, etc.)
	a vehicle posture (e.g. sensor angle of vision changes when vehicle pitches due to a sudden braking event)
	a vehicle situation (e.g. sensor field-of-view is occluded when ego vehicle is towing a large trailer)
	real vehicle weight (e.g. with towing)
	distribution of weight
	tyre (e.g. temperature, tread or rubber hardness)
	brake pad (e.g. icing or temperature)
Ego vehicle operation	vehicle is accelerating
	vehicle is decelerating
	vehicle is driving at constant speed
	vehicle is stopping
	driving at high speed
	driving at low speed
	vehicle is making a turn
	vehicle is making a sudden path deviation
	passing
	right or left turn
	construction zone detour across existing lane markings
	approaching an intersection
	roundabout
	on-ramp and off-ramp
	crossing railroad track

Table B.3 *(continued)*

Category	Factor
Surrounding vehicle — preceding vehicle — to side vehicle — oncoming vehicle	position of surrounding vehicle
	preceding vehicle decelerates
	preceding vehicle decelerates suddenly
	preceding vehicle accelerates
	preceding vehicle accelerates suddenly
	interrupting vehicle
	trailing vehicle in stop and go traffic
	there is a vehicle to the right of ego vehicle going in the same direction
	there is a vehicle to the left of ego vehicle going in the same direction
	there is an oncoming vehicle
	high beam of oncoming vehicle
	passing by a motorcycle
	bicycle
	heavy interferences from surrounding vehicles (e.g. from radar sensor of surrounding vehicles)
Other road participants	pedestrian
	truck
	motorcycle
	peculiar vehicle
Objects off-roadway (surroundings)	side wall
	sign (various position orientation)
	pole
	tunnel
	parking space
	beneath a viaduct
	kerb
	guardrail
	pylon
	vehicle stopping on the side of the road
	animal jumping out
	railway crossing
	construction site
	marked crosswalk
	water alongside road
Objects on-roadway — lane marking	Botts' dots, cat's eyes, Stimsonite (recessed) reflectors
	solid lines – white, yellow
	dashed lines – white
	crosswalk
	rumble strips
	speed bumps
	informational (arrow, speed limit, yield, slow, etc.)
	no lane markings
	interrupted
	degraded lane markings
	multiple lane markings

Table B.3 *(continued)*

Category	Factor
Debris on roadway	animal corpses (roadkill)
	rubbish, tyre tread, etc.
	particulates, dust, dirt, sand, and mud
	construction materials, asphalt, concrete, nails, screws, and other often sharp objects
	solid objects accidentally or deliberately dropped from moving vehicles
	broken glass, plastics, and other solid materials that fall off vehicles during traffic collisions

Table B.4 — Examples for scenario factors structure (non-exhaustive) - Case 2

Layer 1 factor	Layer 2 factor	Layer 3 factor	Layer 4 factor
Road geometry and topology	Road type	Highway	
		Rural	
		Urban	
	Road geometry	Straight	
		Curve	
	Road elevation	Level	
		Uphill	
		Downhill	
	Road cross section	Number of lanes	
		Lane marking	
	Road surface	Roughness	Asphalt
			Concrete
			Pavement
			Gravel
		Damage	Crack
			Pothole
	Road intersections	Diverging	
		Merging	
		Weaving	
		Crossing	

NOTE Definitions of Layers in this table are as follows:

Layer 1 Street layout and condition of the surface;

Layer 2 Traffic guidance infrastructure, e.g. signs, barriers and markings;

Layer 3 Overlay of topology and geometry for temporary construction sites;

Layer 4 Road users and objects, including interactions based on manoeuvres;

Layer 5 Environmental conditions (e.g. weather and daytime), including their influence on Layers 1 to 4;

Layer 6 Digital information, including their influence on Layers 1 to 5.

Table B.4 *(continued)*

Road furniture and limitations	Boundary	Pole	
		Guardrail	
		Concrete barrier	
		Noise barrier	
		Tunnel	Overhead clearance
		Bridge	Overhead clearance
			Entities moving below bridge
	Traffic signs	Traffic lights	
		Warnings	
		Limits	
Temporary physical limitations	Lane reassignment		
	Lane markings		
	Road work signs		
	Road work barricades		

NOTE Definitions of Layers in this table are as follows:

Layer 1 Street layout and condition of the surface;

Layer 2 Traffic guidance infrastructure, e.g. signs, barriers and markings;

Layer 3 Overlay of topology and geometry for temporary construction sites;

Layer 4 Road users and objects, including interactions based on manoeuvres;

Layer 5 Environmental conditions (e.g. weather and daytime), including their influence on Layers 1 to 4;

Layer 6 Digital information, including their influence on Layers 1 to 5.

Table B.4 *(continued)*

Movable entities	Entity types	Vehicles	Cars
			Trucks
			Buses
			Light rail
			Motorcycles
			Emergency vehicles
			Agricultural vehicles
			Pedal cycles
		Pedestrians	Infant
			Toddlers
			Adult
		Animals	
		Objects	
	Manoeuvres	Cruising	High speed
			Low speed
		Speed change	Deceleration
			Acceleration
		Follow	
		Approach	
		Pass	
		Lane change	Left
			Right
		Turn	Left
			Right
		Turn back	
		Safe stop	
	Relative positions	Left	
		Right	
		In front of	
		Behind	

NOTE Definitions of Layers in this table are as follows:

Layer 1 Street layout and condition of the surface;

Layer 2 Traffic guidance infrastructure, e.g. signs, barriers and markings;

Layer 3 Overlay of topology and geometry for temporary construction sites;

Layer 4 Road users and objects, including interactions based on manoeuvres;

Layer 5 Environmental conditions (e.g. weather and daytime), including their influence on Layers 1 to 4;

Layer 6 Digital information, including their influence on Layers 1 to 5.

Table B.4 *(continued)*

Layer 5 factor			
Environmental conditions	Time of day	Early morning	
		Daytime	
		Evening	
		Night time	
	Atmospheric conditions	Temperature	
		Visibility	
		Wind	
		Clouds	
		Precipitation	Rain
			Hail
			Sleet
			Snow
	Lighting conditions	Sunlight	
		Moonlight	
	Road surface conditions	Dry	
		Wet	
		Snow covered	
		Icy	
Layer 6 factor			
Digital information	V2X information		
	Digital map data		

NOTE Definitions of Layers in this table are as follows:

Layer 1 Street layout and condition of the surface;

Layer 2 Traffic guidance infrastructure, e.g. signs, barriers and markings;

Layer 3 Overlay of topology and geometry for temporary construction sites;

Layer 4 Road users and objects, including interactions based on manoeuvres;

Layer 5 Environmental conditions (e.g. weather and daytime), including their influence on Layers 1 to 4;

Layer 6 Digital information, including their influence on Layers 1 to 5.

EXAMPLE 1 Use case construction: weather = rainy, time of day = daytime, shape of road = straight, downhill, road conditions = wet, ego vehicle operation= vehicle is stopping, other vehicles = oncoming and on right side, pedestrian = none, objects off-roadway = none.

NOTE 1 Table B.3 and Table B.4 are not comprehensive. Therefore, other factors can be considered when constructing scenarios such as local driving customs and infrastructure.

NOTE 2 When starting the SOTIF analysis to identify possible hazardous scenarios and their triggering conditions, the following functional insufficiency / triggering condition categories a), b), c) can be useful:

a) limitation of perception;

For example, climate, time of day, shape of road/lane, ego vehicle condition, vehicle around, other road participants and objects off-roadway could be possible triggering conditions.

b) traffic related conditions; and

For example, shape of road/lane, road condition, surrounding vehicles, ego vehicle operation, accidents, other road participants and objects off-roadway could be possible triggering conditions.

c) ego vehicle related issues (issues impacting the performance or the behaviour of the ego vehicle).

For example, ego vehicle sensor mounting position is susceptible to build up of debris or dust that restricts performance.

NOTE 3 The triggering condition could consist not only of a single factor but also of a combination of factors.

NOTE 4 During construction of the scenario, combinations of factors can be formalized in subsets based on the scenario factors relevance with the specific function, system/component or SOTIF activities (ODD definition, V&V planning...). Table B.5 shows an example subset applicable when planning the validation of a radar-based function.

In this example, by considering a purely radar based system, night or day is not a relevant factor and can be omitted from the subset.

Table B.5 — Factor subset example (e.g. considered for radar-based function validation)

Category	Factor	Subset
Climate	Rainy	Subset 1
Road feature	Tunnel	
Time of day	any / do not care	
Objects off-roadway	Sign (too high position)	
...	...	
...	...	Subset n

NOTE 5 Other standards providing a related taxonomy (e.g. Reference [18]) can be considered.

B.3 Examples of adaptation of safety analyses to identify and evaluate the potential triggering conditions and functional insufficiencies

B.3.1 Analysis methods for systematic identification of triggering conditions

With increasing levels of driving automation, triggering conditions become more complex and subtler to identify, requiring multiple analysis techniques in conjunction with road testing to adequately probe known and unknown hazardous scenarios. When conducting an analysis for the identification of triggering conditions the following methods can be considered: inductive analysis, deductive analysis, exploratory analysis, exploratory simulation (with advanced combinatorial techniques used in this example or others that are considered appropriate), and exploratory driving (with adequate safety measures).

Inductive and deductive analyses are useful to uncover contributors to hazardous events in terms of functional and output insufficiencies and triggering conditions, and to explore their causal relations. However, when novel technologies (e.g. machine learning) are used or when the ODD contains a huge space of scenarios, it cannot be claimed that those analyses are sufficient in order to find all relevant insufficiencies and triggering conditions.

With increasing levels of driving automation, the addition of exploratory analysis methods can be of benefit where an incorrect belief state is achieved by the system but the cause is not readily known. For example, the highly automated driving system incorrectly believes it is on a collision free path or incorrectly believes it can or has avoided a collision. The source of that incorrect belief state can stem from single or multiple elements. For example, the high threat object was incorrectly classified as a low threat object due to its proximity to other low threat objects, or the path could not be executed by the vehicle due to some physical limitations. An analysis such as System-Theoretic Process Analysis (STPA) can serve as a suitable technique because it considers interaction between system, scenario and human as source of a hazard.

Finally, exploratory simulation and exploratory driving are useful bottom up tools for identifying triggering conditions. However, each have their limitations. The limitations of the methods can be considered when applying the methodology and criteria for the evaluation of the achievement of the SOTIF.

B.3.2 Example of cause tree analysis

Based on the hazardous events identified in Clause 6, potential insufficiencies of specification, performance insufficiencies and triggering conditions can be determined, using an appropriate deductive risk assessment method (analogous to the classical fault tree analysis method used for functional safety).

NOTE Cause tree analysis is a suitable method for determining the root causes of an event and can be used for the identification and understanding of the triggering conditions of a specific hazardous event.

When the system insufficiencies and triggering conditions have been identified, the combination of events contributing to the hazard can be determined and the minimal cut sets that are sufficient for causing the hazard determined. The result can be used to identify important potential dependencies and the most significant insufficiencies and to determine if the measures that have been undertaken for risk mitigation are sufficient, see 7.4. Furthermore, the results can be used to prioritize or even cluster validation activities.

EXAMPLE The hazardous event of sudden undesired deceleration is analysed within the scope of an ACC system. The system is composed of a regulator that can control the power to the engine and actuate braking, based on input from the drivers requested speed and a stereo camera used for detecting obstacles as well as measuring the range to objects ahead of the vehicle. A functional insufficiencies tree model is defined in Figure B.3. Based on the functional insufficiencies analysis, minimal cut sets for the top event G0 can be expressed using the following equivalent Boolean algebra function:

$$TOP = B01 + B02 + (B03 \times B04) + (B05 \times B06)$$

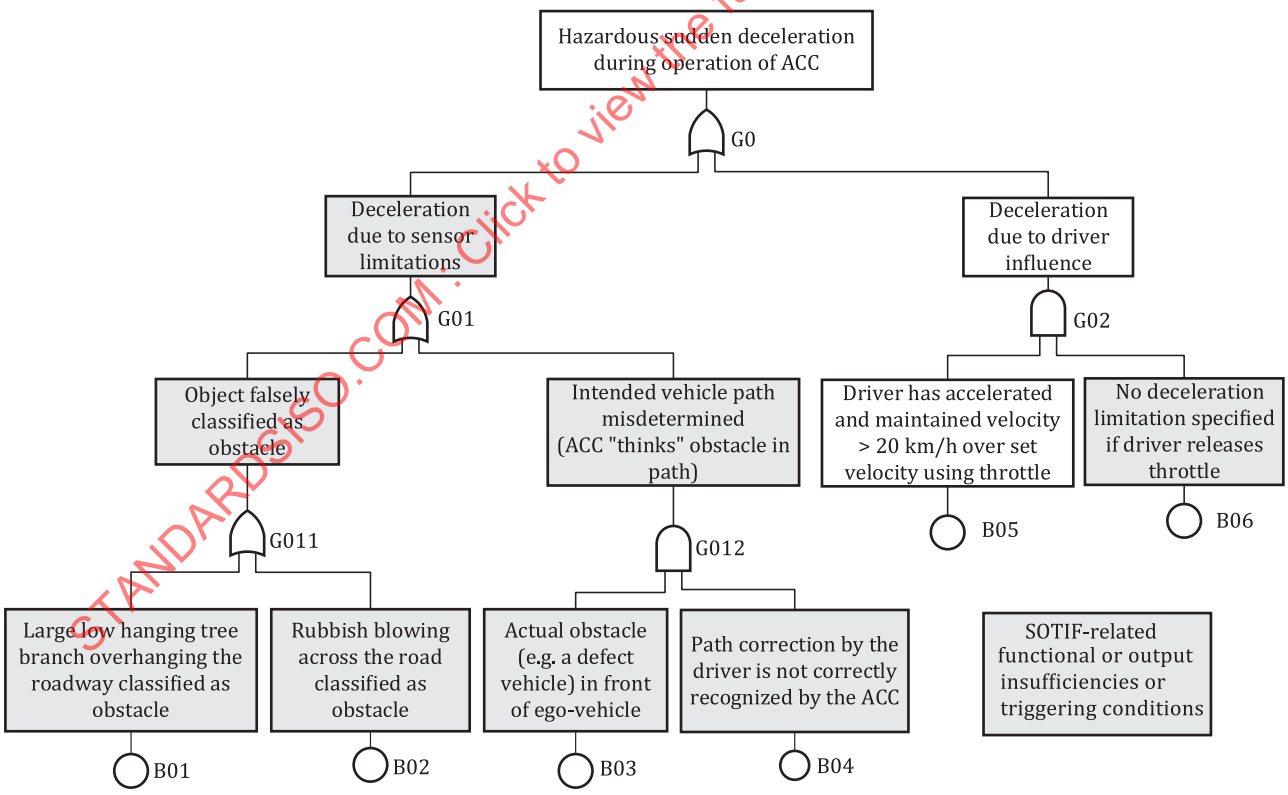


Figure B.3 — Cause tree analysis

In addition to the deductive analysis, an inductive analysis is typically performed to increase the safety analysis completeness by analysing the functional, architectural and detailed design and by assessing newly identified hazards introduced by the system implementation.

B.3.3 Example of inductive SOTIF analysis

B.3.3.1 Inductive SOTIF analysis workflow

The SOTIF analysis workflow as depicted in Figure B.4 aims to describe activities that support:

— identifying and evaluating the potential functional insufficiencies which could result in a hazardous behaviour initiated by known specific conditions of driving scenarios;

— identifying and evaluating the potential triggering conditions that could initiate a hazardous behaviour resulting from known potential functional insufficiencies; and

— identifying modification measures to avoid or mitigate the SOTIF-related risks.

The order in which the various aspects are considered (from potential functional insufficiencies to potential triggering conditions or from specific conditions of driving scenarios to potential functional insufficiencies) is up to the preference of the analyst.

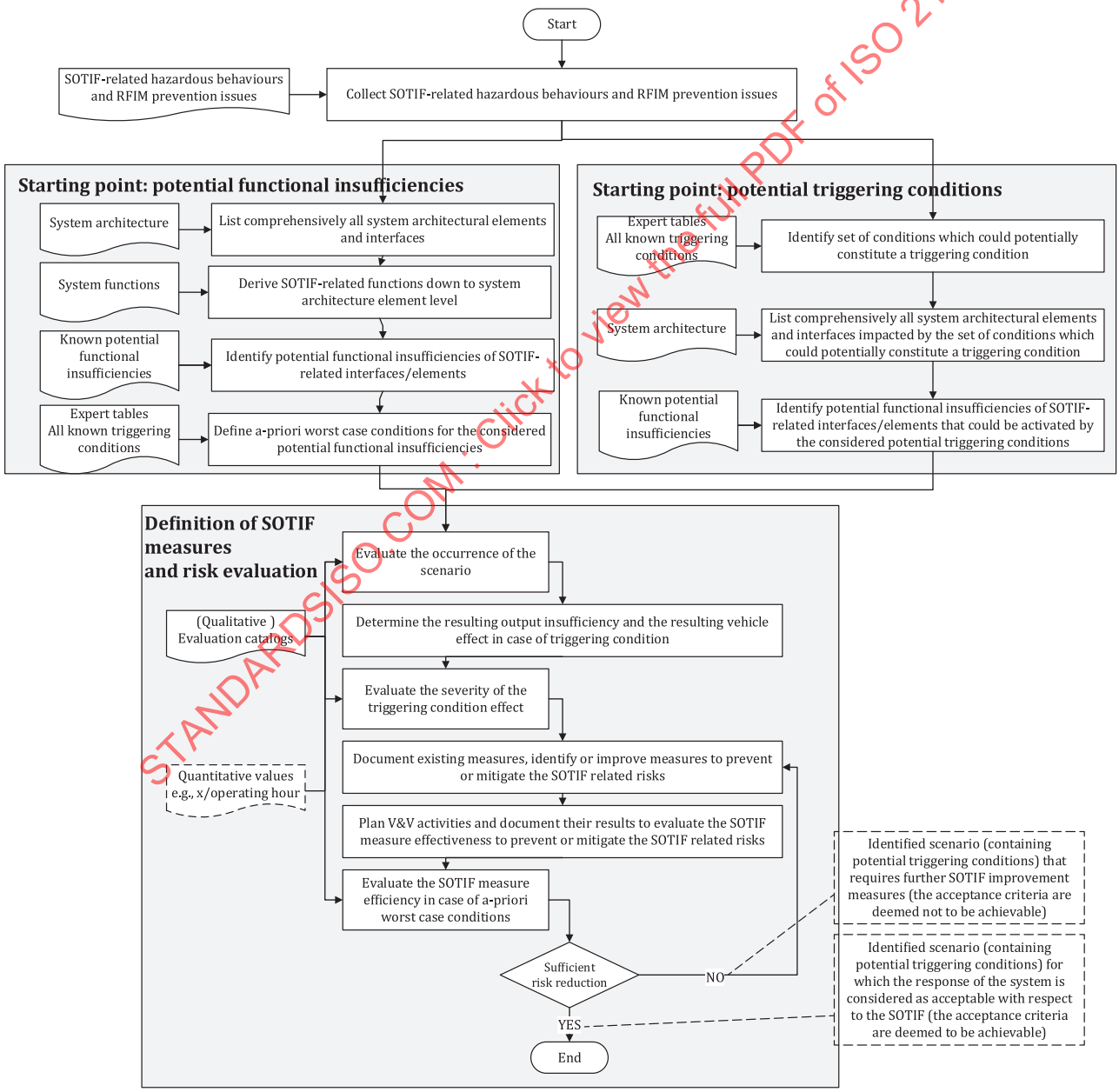


Figure B.4 — Inductive SOTIF analysis workflow

The SOTIF-related risk analysis can be based on qualitative rating scales for likelihood and impact or quantitative values, e.g. false positive rates, number of triggering conditions per operating hour. These results can be used to prioritize the evaluation of certain scenarios or elements above others.

NOTE 1 Statistical analyses and charts, for example, Pareto analysis, risk matrices, considering qualitative ratings can be used to support the determination of the acceptability of the triggering conditions as defined in 7.4. The use of pre-determined ratings to determine the acceptability in these qualitative analyses is however not appropriate due to the variability of the evaluation criteria.

B.3.3.2 Example of SOTIF analysis from potential functional insufficiencies to triggering condition (system-based analysis)

This inductive analysis aims to identify first the system element potential functional insufficiencies and second, the scenario conditions which could activate these identified potential insufficiencies, that could lead to an output insufficiency, a hazardous behaviour or a RFIM prevention issue.

NOTE 1 The term "RFIM prevention issue" is used in this B.3.3.2 to denote the inability of the system to avoid or mitigate a reasonably foreseeable indirect misuse (RFIM).

The following example depicts the inductive analysis of different elements of an emergency braking system. The analysis represented in Table B.6, Table B.7 and Figure B.5 is not meant to be exhaustive. It rather intends to illustrate the SOTIF analysis of different kinds of system elements involved in the Sense-Plan-Act model, namely:

— camera HW sensor imager (HW unit HW43);

— camera HW accelerator or 'IP' (HW unit HW32);

— camera SW classification function (SW unit SW11); and

— braking torque actuation system (System SYS 12).

These system elements contribute to the system function 'Brake in case of oncoming or crossing objects' (SYS23.1). The emergency braking is intended if the detected object is part of a specified object list (Ref. #RRR) and under specified emergency conditions (Ref. #CDNXX).

Each system element has its own potential functional insufficiencies that, in combination with 'a priori' worst-case conditions, could lead to a hazardous behaviour, a RFIM prevention issue or an output insufficiency.

NOTE 2 The functional insufficiency is a property of the system element whereas the 'a priori' worst-case conditions are a property of the considered scenario.

For each tuple (system element, related potential functional insufficiency, related potential triggering condition), a SOTIF-related risk analysis is carried out aiming at identifying measures to improve the SOTIF, verifying their effectiveness and evaluate the residual risk with an appropriate rationale.

Table B.6 — Example of SOTIF analysis from potential functional insufficiencies to triggering condition

ID	System elements potentially leading to SOTIF-related hazardous events				Potential triggering conditions A-priori worst case conditions for known potential functional insufficiencies				Potential triggering conditions effect		Measures to address the output insufficiency (including pre-existing as well as newly proposed)			Rationale of acceptance
	System architecture function	Allocation to system or HW/SW elements	SOTIF-related interfaces / elements	Known potential functional insufficiencies in the system design	Scene characteristics (Environmental conditions, road / urban infrastructure)	Driving scenario (actions, events, goals and values)	Behaviour of driver, other drivers, road users	Occurrence	Vehicle-level effect if the output insufficiency is not addressed by any measure	Severity of the hazardous event	Measures in design to improve the SOTIF	Verification measures to provide evidence of the system response, or of the design measure effectiveness	Measure effectiveness	
ID1.1	System element realizing function SYS23.1: Brake in case of oncoming / crossing objects (Object list: Ref. #RRR) under emergency conditions (Ref. #CDNXX)	HW unit HW32: Camera IP	IP result	Image resolution limitation affecting distance estimation	Daylight, dry road	Driving straight at 90 km/h	Preceding vehicle overflowing slightly on the lane of ego vehicle (≥100m)	*Completed according to a rating rule*	False positive: Oncoming object detection leading to unintended vehicle deceleration <-X m/s^2	*Completed according to a rating rule*	Use of sensors from diverse technology: lidar, radar	Test report TC#225 PASSED, Resp.: Team A	*Completed according to a rating rule*	See Table B.7
ID1.2		HW unit HW43: Camera sensor HW	Sensor result	Poor image rendering in low light conditions	Evening, dry road	All manoeuvres at low light conditions and dry roads	No further conditions	*Completed according to a rating rule*			Use of sensors from diverse technology: lidar, radar	Test report TC#226, PASSED Resp.: Team B	*Completed according to a rating rule*	See Table B.7
ID1.3		SW unit SW11: Object classification	Object classification result	Low performance in corner case CC#52	CC#52 conditions: incl. very high number of moving of objects in the scene to be processed	Rush hour, high traffic volume, busy intersection, group of cyclist, group of motorcycles, scenery with a lot of flags. Moving objects are in front of the car but not in its trajectory (e.g. due to a curve)	No further conditions	*Completed according to a rating rule*			New architecture New algorithms Action: OPL#227 Team C		*Completed according to a rating rule*	See Table B.7

Table B.6 *(continued)*

ID	System elements potentially leading to SOTIF-related hazardous events				Potential triggering conditions A-priori worst case conditions for known potential functional insufficiencies				Potential triggering conditions effect		Measures to address the output insufficiency (including pre-existing as well as newly proposed)			Rationale of acceptance
	System architecture function	Allocation to system or HW/SW elements	SOTIF-related interfaces / elements	Known potential functional insufficiencies in the system design	Scene characteristics (Environmental conditions, road / urban infrastructure)	Driving scenario (actions, events, goals and values)	Behaviour of driver, other drivers, road users	Occurrence	Vehicle-level effect if the output insufficiency is not addressed by any measure	Severity of the hazardous event	Measures in design to improve the SOTIF	Verification measures to provide evidence of the system response, or of the design measure effectiveness	Measure effectiveness	
ID1.4		System SYS 12: Braking torque actuation system	Braking torque	Actuator slow timing response at T<-10 °C and low voltage <9,5 V	Winter, snow, T<-15 °C	Battery low AEB intervention due to approaching slow vehicle	No further conditions	*Completed according to a rating rule*	Unintended loss of deceleration <-Z m/s^2 Lower AEB deceleration in case of AEB intervention	*Completed according to a rating rule*	New actuator Action: OPL#228 Team D		*Completed according to a rating rule*	See Table B.7
ID1.5		SW unit SW11: Object classification	Object classification result	Misclassification of unexpected / untrained objects	Rare objects, unusual objects	Driving during certain events (e.g. football game, parade), holidays (e.g. Christmas, carnival), car decorations, car loads	Driver mounted something overhanging on roof rack, protruding into camera image (e.g. a ladder or sport equipment with some textile material or rope hanging off)	*Completed according to a rating rule*	False positive: Oncoming object detection leading to unintended vehicle deceleration <-X m/s^2	*Completed according to a rating rule*	Check for unusual camera detected objects at beginning of driving cycle Continuous plausibility check of detected objects Entry in user manual of car instructing the driver to not let anything protrude into the camera field of view	Simulation or validation test	*Completed according to a rating rule*	See Table B.7

The SOTIF analysis Table B.6 is organized in four groups of columns that documents and analyses:

1) system elements potentially leading to an output insufficiency, i.e. potentially all system elements, described at an appropriate abstraction level, e.g. down to the lowest level of system architecture;

2) potential triggering conditions in relation with system elements listed in 1) described at external or internal environment level;

3) effects of these potential triggering conditions in absence of any SOTIF measures described at top abstraction level, e.g. vehicle level; and

4) existing and planned measures to address output insufficiencies listed in 1), described at an appropriate abstraction level, e.g. at implementation level.

Table B.7 — Example of SOTIF analysis from potential functional insufficiencies to triggering condition [continued]

ID	Rationale of acceptance
ID1.1	Directed tests on *multiple and diverse narrow roads* and endurance tests (<Road> is tagged 'Narrow', <Speed> >90 km/h, <Time_of_day> Daylight in the whole driving data set) demonstrate that: — the probability of occurrence of encountering situations where the image resolution limitation of the camera IP HW32 affects the distance estimation in such a way that it would lead to unintended vehicle deceleration due to false positive object detection in absence of SOTIF measures (by deactivating radar and lidar) is confirmed to be reasonably low: 0 events led to unintended vehicle deceleration; 0 occurrences led to detection of 'potential objects'; — combination of radar and lidar are confirmed to be effective measures if activated: Repeated tests in same conditions where image resolution limitation affects the distance limitation show better reaction time (-x%) and higher confidence estimation to confirm absence of objects when radar and lidar information are available in the fusion algorithm. Evidence: TC#225 passed. **Point can be closed.**
ID1.2	Directed tests and endurance tests during evening/night(<Time_of_day> 'Night' OR 'Dusk' in the whole driving data set) demonstrate that: — the probability of occurrence of encountering situations where the image rendering resulting from camera sensor HW43 limitations in low light conditions affects the image in such a way that it would lead to unintended vehicle deceleration due to false positive object detection in absence of SOTIF measures (by deactivating radar and lidar) is confirmed to be reasonably low: 0 events led to unintended vehicle deceleration; 6 occurrences led to detection of 'potential objects', however not confirmed by decision algorithm due to implausible conditions; — combination of radar and lidar are confirmed to be effective measures if activated: Repeated tests in same conditions show better reaction time (-x%) and confidence to confirm absence of objects when radar and lidar information are available in the fusion algorithm. **Point can be closed.**
ID1.3	Corner case CC#52 is a set of particular conditions that were not encountered during endurance tests and still ongoing fleet tests. However, as corner case CC#52 cannot be categorized as 'improbable', it has been reproduced in a traffic scene simulator environment. Alternative algorithms from Team C show a slight performance increase (higher confidence estimation) although not significant in this simulation environment. **Point still pending to confirm whether new architecture or new algorithms are required.**
ID1.4	Recent tests performed by Team D identified an insufficiency of specification of the current braking torque actuator (variant A). At low voltage value (still within specified range) and low ambient temperatures (-30 °C to -15 °C) in North Sweden, unintended loss of deceleration <-Z m/s^2 is confirmed. Same tests demonstrate the effectiveness of the robust braking actuator prototype (variant B) to reach the validation targets. Requirement specification has been updated. **Point still open to repeat same tests with released version of variant B.**
ID1.5	Pending simulation results

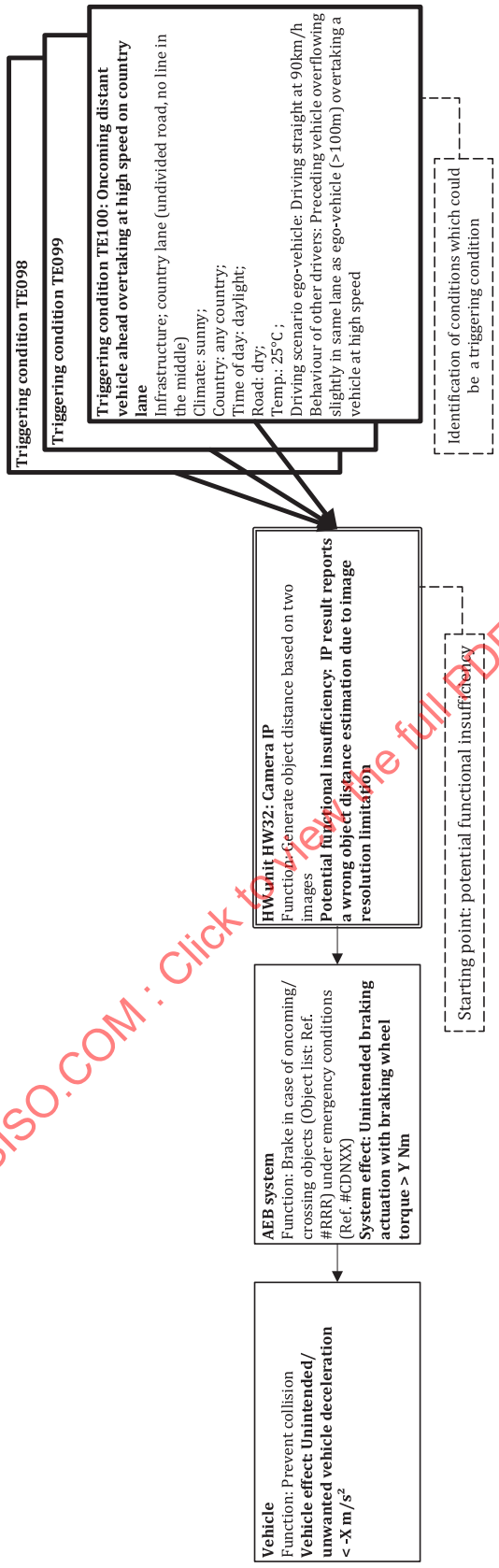


Figure B.5 — SOTIF cause-effect tree starting with potential functional insufficiency illustrating Tables B.6 and B.7

B.3.3.3 Example of SOTIF analysis from triggering condition to potential functional insufficiencies (scenario-based analysis)

This SOTIF inductive analysis aims to identify first conditions of driving scenarios that could lead to an output insufficiency, a hazardous behaviour or a RFIM prevention issue and second, the system architecture function or element impacted by these potential triggering conditions.

The following example depicts the inductive analysis of elements of an emergency braking system whose scenario condition 'Pedestrians painted on the road' could lead to a hazardous behaviour. The analysis represented in Table B.8, Table B.9 and Figure B.6 is not meant to be exhaustive. It rather intends to illustrate the SOTIF analysis of different kinds of system elements involved in the Sense-Plan-Act model, namely:

— radar HW element (HW unit HW53);

— camera HW accelerator or 'IP' (HW unit HW52);

— camera SW classification function (SW unit SW11); and

— braking torque actuation system (System SYS 12).

These system elements contribute to the system function 'Brake in case of oncoming or crossing objects' (SYS23.1). The emergency braking is intended if the detected object is part of a specified object list (Ref. #RRR) and under specified emergency conditions (Ref. #CDNXX).

The analysis tends to identify system element functional insufficiencies that could be impacted by the same potential triggering condition. For instance, in the example below, the algorithm of the camera IP (HW unit HW52) might trigger some false positive object detection in case of 'Pedestrians painted on the road', albeit only in particular corner cases (CC #536).

NOTE The functional insufficiency is a property of the system element whereas the potential triggering conditions are a property of the considered scenario.

For each tuple (potential triggering condition, related potential functional insufficiency of a system element), a SOTIF-related risk analysis is carried out aiming at identifying measures to improve the SOTIF and evaluate the residual risk with an appropriate rationale.

Table B.8 — Example of SOTIF analysis from triggering condition to potential functional insufficiencies

ID	Potential triggering conditions				System elements potentially leading SOTIF-related hazardous events				Potential triggering conditions effect		Measures to address the output insufficiency (including pre-existing as well as newly proposed)			Rationale of acceptance
	Known hazardous use case from expert table													
	Scene characteristics (Environmental conditions, road/urban infrastructure)	Driving scenario (actions, events, goals and values)	Behaviour of driver, other drivers, road users	Occurrence	System architecture function impacted by triggering conditions	System architectural elements impacted by triggering conditions	SOTIF-related interfaces/elements	Potential functional insufficiencies in the system design	Vehicle-level effect if the output insufficiency is not addressed by any measure	Severity of the hazardous event	Measures in design to improve the SOTIF	Verification measures to provide evidence of the system response, or of the design measure effectiveness	Measure effectiveness	
IDA.1	Infrastructure **Pedestrians painted on the road** Climate: fine, Country: ALL Time of day: evening low light, Road: dry Temp.: 25 °C	Drive in a straight line at 50 km/h (urban area)	Following vehicle close to ego vehicle (<5m)	Completed according to a rating rule	System element realizing function SYS23.1: Brake in case of oncoming / crossing objects	HW unit HW52: Camera IP	IP result	Inability to distinguish smoke or fog from solid object	False positive: pedestrian detection leading to unintended vehicle deceleration <-X m/s^2 leading to rear end collision with following vehicle	Completed according to a rating rule	Use of sensors from diverse technology: lidar, radar	TC#234 PASSED Resp: Team A	Completed according to a rating rule	See Table B.9
IDA.2						HW unit HW63: Radar element	Radar result	None for this scenario			None		N/A	See Table B.9

Table B.8 *(continued)*

ID	Potential triggering conditions				System elements potentially leading SOTIF-related hazardous events				Potential triggering conditions effect		Measures to address the output insufficiency (including pre-existing as well as newly proposed)			Rationale of acceptance
	Known hazardous use case from expert table			Occurrence	System architecture/function impacted by triggering conditions	System architectural elements impacted by triggering conditions	SOTIF-related interfaces/elements	Potential functional insufficiencies in the system design	Vehicle-level effect if the output insufficiency is not addressed by any measure	Severity of the hazardous event	Measures in design to improve the SOTIF	Verification measures to provide evidence of the system response, or of the design measure effectiveness	Measure effectiveness	
	Scene characteristics (Environmental conditions, road/urban infrastructure)	Driving scenario (actions, events, goals and values)	Behaviour of driver, other drivers, road users											
IDA.3						SW unit SW11: Object classification	Object classification result	None for this scenario (1oo2 input comparison/voting supposed to be free from insufficiencies)			Voter based on fully redundant and diverse algorithms (HW52, HW63, SW11),	Ref. VC2 PASSED	Completed according to a rating rule	See Table B.9
IDA.4						System SYS 12: Braking torque actuation system	Braking torque	None for this scenario			None		N/A	See Table B.9

The SOTIF analysis Table B.8 is organized in four macro columns that documents and analyses:

1) potential triggering conditions, for example, known potential triggering conditions or random potential triggering conditions, described at external or internal environment level;

2) system elements that could potentially lead to an output insufficiency in case they are exposed to potential triggering conditions listed in 1), described at an appropriate abstraction level, e.g. down to the lowest level of system architecture;

3) effects of these potential triggering conditions in absence of any SOTIF measures, described at top abstraction level, e.g. vehicle level; and

4) existing and planned measures to address output insufficiencies listed in 2) described at an appropriate abstraction level, e.g. at implementation level.

Table B.9 — Example of SOTIF analysis from triggering condition to potential functional insufficiencies [continued]

ID	Rationale of acceptance
IDA.1	Directed tests driving around Delta Avenue in Burnaby, BC Canada between Brentwood Park and Holy Cross elementary school — The probability of occurrence of encountering situations where the camera IP HW52 identifies ghost objects leading to unintended vehicle deceleration in absence of SOTIF measures (by deactivating radar, lidar and optical flow-based mechanisms) is confirmed to be reasonably low: 0 events led to unintended vehicle deceleration; 1 occurrence led to detection of 'potential objects', however not confirmed by decision algorithm due to insufficient confirmation time. Indeed, even at low driving speed, image is free from distortion only for a very short period time which is not sufficient to detect a pedestrian on the road. — Combination of radar and lidar are confirmed to be effective measures if activated: Repeated tests in same conditions show higher confidence to confirm absence of objects when radar and lidar information are available in the fusion algorithm. Evidence: TC#234 passed.
IDA.2	N/A. Radar element is not subject to misinterpretation of road markings.
IDA.3	No system design weaknesses have been identified in SW unit SW11 for this particular scenario. However, the decision algorithm based on several diverse algorithms having the ability to confirm the object presence is deemed a very effective measure to cope with SW11 unit functional insufficiencies, if any.
IDA.4	N/A. Braking torque actuator is not subject to misinterpretation of road markings.

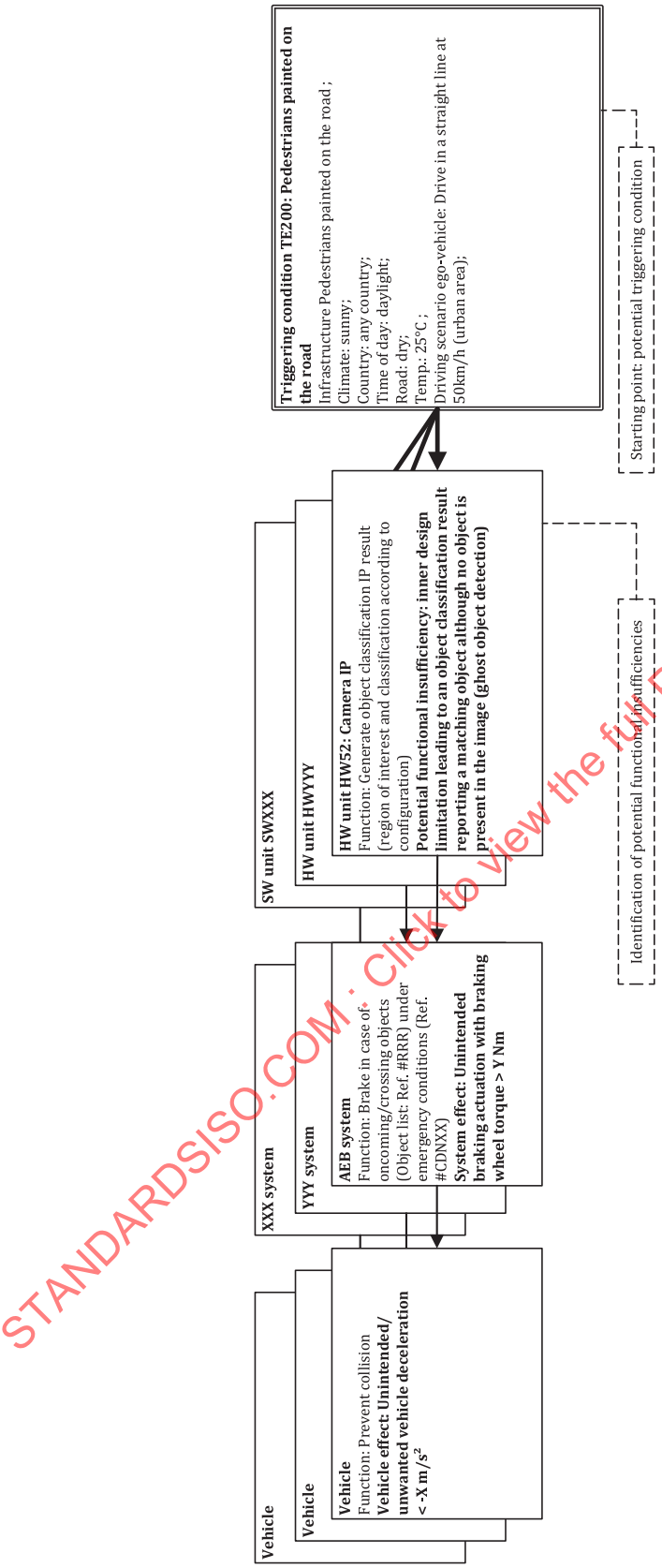


Figure B.6 — SOTIF cause-effect tree starting with potential triggering condition illustrating Tables B.8 and B.9

B.4 Applying STPA in the context of SOTIF for ADAS and automated vehicles

B.4.1 Introduction

STPA (System-Theoretic Process Analysis) (refer to References [19] and [20]) is a safety analysis approach designed for evaluating the safety of complex systems and identifying safety constraints and requirements. There are many papers published that describe how STPA can be applied to automotive systems, ADAS and automation (refer to References [21], [22], [23] and [24]). STPA is useful for SOTIF because it can address functional insufficiencies, system usage in an unsuitable environment, misuse by persons, etc.

B.4 provides a simplified highway-pilot SAE J3016 Level 3 system example demonstrating the usage of STPA to conduct the SOTIF analysis for Clause 6 (hazard identification) along with Clause 7 (the identification and evaluation of triggering conditions). The highway pilot (HP) controls the entire vehicle dynamics in a restricted environment, without immediate supervision of a human driver. A human driver is present and able to take back control within a defined time span of typically several seconds to not more than a maximum specified time.

B.4.2 STPA step 1: defining the purpose and scope of the analysis

The first step of STPA identifies the stakeholder losses to be prevented. Once STPA losses are identified, the STPA vehicle-level hazards are identified. These are vehicle-level states or conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. Table B.10 provides an example of STPA losses and STPA vehicle-level hazards for the highway pilot system.

Table B.10 — Example loss and hazard identification

Situation / scenario (excerpt from HARA)	Loss	Potential consequence (harm)	Vehicle-level hazards (from HARA)
Driving on a highway at night, bad visibility with high speed. Approaching a slower motorcycle rider from behind.	[L1] Loss of life or human harm	Severe or fatal injuries	[VH1] Ego vehicle violates minimum distance threshold/ requirement from/with other vehicles.
....	[L2] ...	...	[VH1] ...

NOTE The rest of B.4 contains examples of specification. In this context, “shall” statements are used. In B.4 “shall” statements are example requirements only and are not intended for compliance with this document.

Note that later STPA steps systematically analyse the controlling actions of each system controller, including humans, to identify specific behaviours and causes that could potentially lead to vehicle-level hazards for a specific scenario. Given the vehicle-level hazards, a set of vehicle-level SOTIF requirements are identified as part of the HARA, see Table B.11.

Table B.11 — Hazards and corresponding vehicle-level safety constraints

Hazard	SOTIF requirement at the vehicle level (vehicle-level safety constraint)
[VH1] Ego vehicle violates minimum distance threshold/requirement from/with other vehicles.	[SC-1] Ego vehicle shall ensure a safe distance to other vehicles.
...	

B.4.3 STPA step 2: modelling of the control structure

The system and functional specification are analysed to identify a control hierarchy of the system and its interfacing surroundings. This is referred to as the “control structure”. The controller commands known as “control actions” and feedback from the controlled process and environment are captured for the analysis.

An example control structure for a highway pilot is shown in Figure B.7.

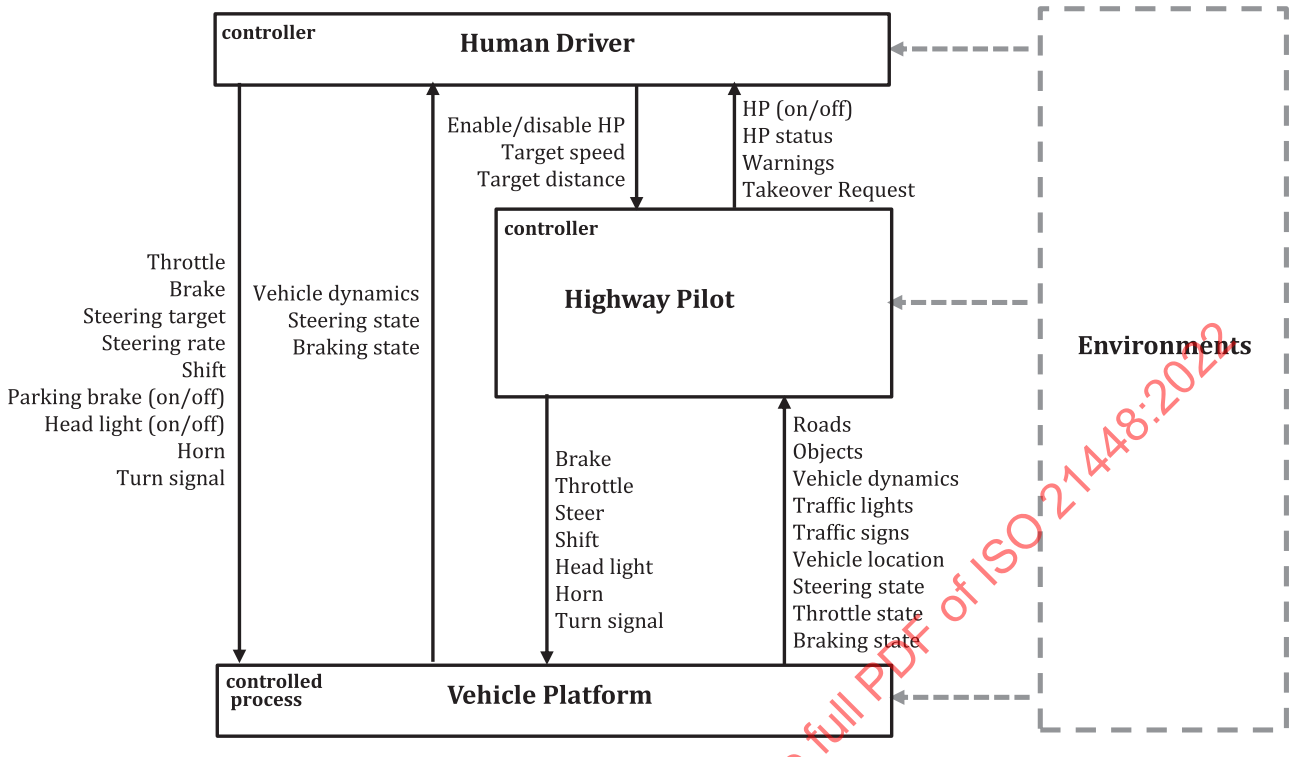


Figure B.7 — High-level control structure for highway pilot

Due to restricted space, the STPA in B.4 does not go any deeper, but the reader interested in an example for the next refinement level of the control loop model for this kind of function is referred to Figure 5 in Reference [25].

B.4.4 STPA step 3: identification of unsafe control actions

The next step of the STPA procedure identifies the Unsafe Control Actions (UCAs), which are actions that, in a particular context and worst-case environment, will lead to a vehicle-level hazard. The UCA with its associated hazard and HARA are used to fulfil the hazard identification and risk evaluation, see Clause 6. An unsafe control action consists of five elements, shown in Figure B.8.

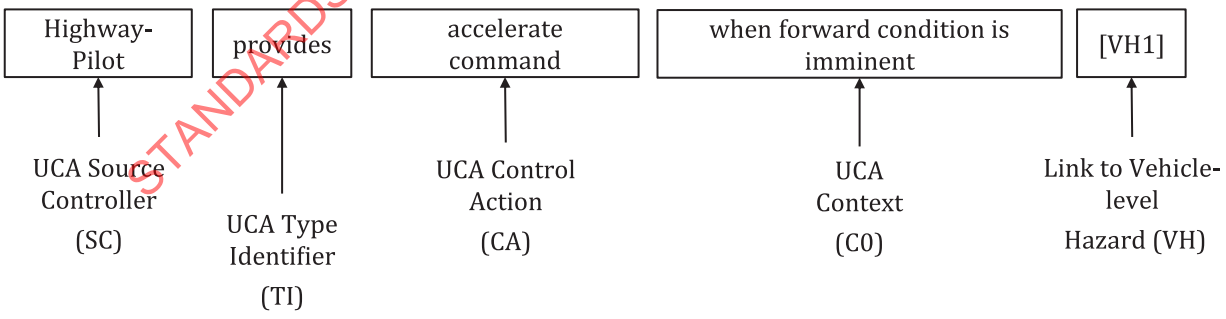


Figure B.8 — Five elements of an unsafe control action

A few examples of unsafe control actions for the highway pilot brake command are shown in Table B.12.

Table B.12 — Examples of unsafe control actions for the control action brake command of the controller HP

Control action	Not providing	Providing	Providing too early, too late, or in the wrong order	Providing for too long or stopping too soon
Brake command	UCA-1: Highway pilot does not provide a brake command when a forward collision is imminent. [VH1]	UCA-2: Highway pilot provides a brake command with insufficient amount of braking when a forward collision is imminent. [VH1] UCA-3: Highway pilot provides a brake command when driver is providing throttle command. [VH2]	UCA-4: Highway pilot provides a brake command too late after a forward collision is imminent. [VH1]	UCA-5: Highway pilot stops providing a brake command too soon after a collision has occurred (i.e. stops providing a brake command before the driver has resumed manual control). [VH1]

Note that each unsafe control action potentially leads to at least one vehicle-level hazard (otherwise it would not be unsafe) but can also lead to more than one vehicle-level hazard.

Given the UCAs, controller safety constraints can be defined to ensure the UCAs are prevented. A controller safety constraint specifies assertions or invariants on the controller behaviours that need to be satisfied to prevent UCAs from occurring.

Some controller safety constraints (regarding some braking-related UCAs) are shown in Table B.13.

Table B.13 — Transformation of UCAs into requirements (safety constraints)

Unsafe control action	Safety constraint
UCA-1: Highway pilot does not provide a brake command when a forward collision is imminent. [VH-1]	SC-1: Highway pilot shall provide a brake command when a forward collision is imminent. [UCA-1]
UCA-2: Highway pilot provides a brake command with insufficient amount of braking when a forward collision is imminent. [VH-1]	SC-2: Highway pilot shall provide a brake command with sufficient amount of braking above the minimum amount needed to avert a forward collision. [UCA-2]
UCA-3: Highway pilot provides a brake command when driver is providing throttle command. [VH2]	SC-3: Highway pilot shall not provide brake command when driver is providing throttle command. [UCA-3]
UCA-4: Highway pilot provides a brake command too late after forward collision is imminent. [VH-1]	SC-4: Highway pilot shall provide a brake command at least (TBD) seconds before a forward collision is imminent. [UCA-4]
UCA-5: Highway pilot stops providing a brake command too soon after a collision has occurred, and driver has not resumed manual control. [VH1]	SC-5: Highway pilot shall provide a brake command until the driver resumes manual control. [UCA-5]

B.4.5 STPA step 4: identification of causal scenarios

The final core step of STPA identifies the causal scenarios that lead to hazards and the corresponding causal factors (i.e. triggering conditions, see 7.3). Table B.14 outlines causal scenarios for the highway pilot UCA-1 to identify the causal factors.

As a first step of this analysis the combination of one or more output insufficiencies of other elements or of the elements of the system controller itself, that can lead to the UCA under consideration, are identified. This combination of one or more output insufficiencies is referred to as “insufficiency condition” in Table B.14. As a next step the causal factors leading to the identified insufficiency conditions are identified. These can be output insufficiencies, functional insufficiencies and triggering conditions.

Table B.14 — Identification of causal factors

Causal scenario	UCA (hazardous behaviour)	Insufficiency condition	Causal factors (triggering condition, functional insufficiencies, output insufficiencies)
CS-1	UCA-1: Highway pilot does not provide a brake command when a forward collision is imminent.	IC-1: HP erroneously believes that there is no collision imminent due to inadequate feedback: Relative position, speed, acceleration, direction to an obstacle.	CF-1: Sensors mounted incorrectly, sensor focus or position compromised, sensor blocked, etc. CF-2: Feedback delayed and not received in time because the bus is busy, inadequate message priority or arbitration, EMI, etc. CF-3: Feedback is deemed to be incorrect (ignored by HP) because it conflicts with other feedback (e.g. other feedback indicates the wheel speed is zero).
CS-2	UCA-1: Highway pilot does not provide a brake command when a forward collision is imminent.	IC -2: HP erroneously believes that there is no collision imminent due to inadequate feedback: Brakes applied	CF-4: HP receives incorrect feedback that sufficient braking or steering is already applied.
CS-3	UCA-1: Highway Pilot does not provide a brake command when a forward collision is imminent.	IC -3: HP erroneously believes that there is no collision imminent due to inadequate feedback: Size or type of obstacle.	CF-5: HP receives inadequate feedback indicating that the obstacle type does not pose a collision danger. CF-6: HP receives feedback that there is no obstacle to collide with (e.g. due to obscured sensor, sensor mounted in wrong position/orientation, sensors offline, obstacle outside of sensor view, adverse weather conditions identified incorrectly (missing algorithm functionality), not calibrated, etc.).
CS-4...	UCA-2: Highway Pilot...	IC -4: HP...	CF-7: HP ...

NOTE In this example STPA SOTIF-related issues as well as functional safety related issues are considered.

B.4.6 Identify controls and mitigations, improve the system design and derive requirements

Once the core activities of STPA in the context of this document have been completed, the remaining activities from STPA can be delegated to the corresponding process steps, for functional modifications addressing SOTIF-related risks see Clause 8, or for failure-related causes, to ISO 26262-4:2018, Clause 6, respectively. This involves formulating implementable requirements that are suitable to fulfil the safety constraints from the STPA.

Annex C
(informative)

Guidance on SOTIF verification and validation

C.1 Purpose of the verification and validation strategy

Functional insufficiencies of the system are the source of SOTIF issues. A verification and validation strategy is designed to show that the residual risk due to known and unknown scenarios is sufficiently low and complies with the quantitative target defined in 6.5. Concepts for deriving and testing the validation targets are presented.

Once the validation target is defined, a validation test plan can be designed in accordance with Clauses 9 and 11 to show the absence of unreasonable risk due to known and unknown hazardous scenarios (areas 2 and 3). Validation typically involves some combination of physical (test track, real-world) and simulation testing. As part of the validation strategy defined in Clause 9, the quantitative target is often allocated between physical and simulation testing.

Validation can consist of testing the vehicle under a wide range of operating conditions. It can be a mixture of SIL, HIL and real-world operation conditions. It can contain some structured testing (e.g. tests designed and implemented on a test track), dedicated analysis and simulation but the key aspect, especially for area 3, is to have sufficient testing under sufficiently comprehensive operating conditions to expose potentially unknown unsafe scenarios as extensively as required by the validation strategy.

These test scenarios addressing area 3 can include:

1) random combinations of known parameters of identified use cases (e.g. combination of adverse weather and specific traffic conditions);

2) random combinations of known scenarios;

3) unidentified specific scenarios that could trigger a hazardous system behaviour in open road testing.

Simulation can be used to quickly explore a wide variety of relevant scenarios. However, simulation can be limited by the underlying assumptions on the environment, sensors, and vehicle model. How accurately the models represent the real world is part of the safety argument. Moreover, simulations can only be based on identified parameters [C.1 1)] or identified scenarios [C.1 2)].

Real-life testing is able to test the system using realistic inputs but is limited by the numbers of kilometres, hours and scenarios that can be realistically driven and by the randomness of the actual scenes encountered during testing [C.1 3)]. With real-life testing it is possible to discover previously unknown parameters.

Prior knowledge on similar functions and their relevant potentially hazardous scenarios can be considered to tailor the validation strategy, for instance derived from lessons learnt from the field history of similar systems. Strategies can also be used to reduce the amount of testing required while still meeting the validation targets.

Annex C is structured as follows:

— C.2 discusses meeting the acceptance criteria using rate of the hazardous behaviour and gives an example for defining and evaluating the acceptance criteria and validation targets;

— C.3 illustrates how the statistics and safety margin can be used;

— C.4 gives an example of how the various types of testing can be used in sensor verification and validation;

— C.5 discusses how constrained random testing and importance sampling can be used to lessen the amount of simulation testing; and

— C.6 discusses how the physical architecture of the system can be used to justify a reduction in the amount of testing.

C.2 Derivation of validation targets

C.2.1 Meeting the acceptance criteria using rate of the hazardous behaviour

Acceptance criteria are usually very small, e.g. $10^{-8}\ /\ h$. To validate these very low rates a significant effort is often necessary. Therefore, it is important to find a method to reduce the validation target while still demonstrating that the acceptance criterion is met. One possible method is to consider the rate of the relevant hazardous behaviour R_{HB}.

The objective of C.2.1 is not to define an acceptance criterion, but to derive from the acceptance criteria an acceptable rate of the hazardous behaviour, which can in turn be used to define a validation target.

In Clause 6 the possible hazardous events caused by the hazardous behaviour of the intended functionality and their consequences are identified and evaluated. Every identified hazardous behaviour is linked to an acceptance criterion of this behaviour as defined in Clause 6. The validation target for each hazardous behaviour is then derived from the acceptance criterion associated with the hazardous behaviour.

NOTE 1 The method to derive the acceptance criterion or the rationale to support the acceptance criterion is not considered by C.2.1. It is assumed that the acceptance criterion is a rate determined by a well-established and accepted method.

An R_{HB} value compliant with a defined acceptance criterion can be derived from the following steps:

— identification of accidents/incidents leading to harm H due to the analysed hazardous behaviour (e.g. rear end crash due to undesired braking);

— identification of the acceptance criterion for these accidents/incidents A_{H} (this value is derived from original acceptance criteria in combination with safety margin);

— identification of potentially hazardous scenarios in which the identified accidents can occur as a consequence of the hazardous behaviour under consideration (e.g. driving at high speed with a car following with close distance). The conditional probability of being exposed to such circumstances, assuming that the hazardous behaviour under consideration occurred in that scenario, is $P_{\mathrm{E|HB}}$;

  NOTE 2 The potentially hazardous scenarios include the triggering conditions for the hazardous behaviour.

— identification of the probability that the hazardous behaviour is not controllable in these scenarios $P_{\mathrm{C|E}}$, assuming that it occurred in an exposed scenario; and

— identification of the distribution of the severity resulting from the identified accidents/incidents A_{H}, assuming that the controllability action was not successful. This distribution describes the probability $P_{\mathrm{S|C}}$ of a certain degree of severity to occur in these accidents.

NOTE 3 Depending on the acceptance criteria used, $P_{\mathrm{S|C}}$ can be used for a certain degree of a severity (e.g. X % of the involved persons are heavily injured) but also for the probability that the severity is at least at a certain degree (e.g. Y % of the involved persons are at least slightly injured).

NOTE 4 The identified parameters $P_{E|HB}$, $P_{C|E}$, and $P_{S|C}$, can be checked for consistency with the parameters E, C and S respectively of the functional safety HARA according to ISO 26262 for a similar hazardous event. The considerations from ISO 26262-3 on the frequency vs duration of exposure can also be applicable for SOTIF hazardous behaviour.

Assuming that a hazardous behaviour does not lead always to a harm, the acceptance criterion A_H can be decomposed as Formula (C.1):

$$A_H = R_{HB} \times P_{E|HB} \times P_{C|E} \times P_{S|C} \tag{C.1}$$

The rate of the hazardous behaviour R_{HB} is the rate that can be tolerated, as a probability of occurrence of this hazardous behaviour over a given period of time. R_{HB} is directly resulting from the occurrence rate of the triggering conditions that can activate the functional insufficiencies leading to hazardous behaviour. Therefore, it can be used to derive an applicable validation target [Formula (C.2)]:

$$R_{HB} = \frac{A_H}{P_{E|HB} \times P_{C|E} \times P_{S|C}} \tag{C.2}$$

NOTE 5 In the case where the triggering conditions are independent from the exposure to circumstances in which the hazardous behaviour leads to harm, the conditional probabilities can be simplified to a simple product of probabilities.

EXAMPLE In the risk identification and evaluation, a harm H has been identified and was linked to an acceptance criterion $A_H = 10^{-8}/h$. From field data, it is known that the hazardous behaviour leading to this harm is not controllable in $P_{C|E} = 10\ \%$ of the cases. The severity addressed with the acceptance criterion is reached in $P_{S|C} = 1\ \%$ of the cases. The probability of a user being in a scenario occurrence where the occurrence of the hazardous behaviour can lead to the harm is estimated to be $P_{E|HB} = 5\ \%$ of the driving time. Using these values, the rate of the hazardous behaviour to be used for the validation target calculation is as given in Formula (C.3):

$$R_{HB} = \frac{A_H}{P_{E|HB} \times P_{C|E} \times P_{S|C}} = \frac{10^{-8}/h}{0{,}05 \times 0{,}1 \times 0{,}01} = 2 \times 10^{-4}/h \tag{C.3}$$

Using $R_{HB} = 2 \times 10^{-4}/h$ as new starting point for the determination of the validation target can lead to a reduced validation effort. Using Formula (C.7) and associated assumptions, if no hazardous behaviour is encountered in 5 000 h of testing, the acceptance criterion can be shown to have been met with 63 % confidence.

C.2.2 Example for definition and validation of an acceptable false positive activation rate in AEB systems

C.2.2.1 Objective

C.2.2 provides an example of how to calculate a SOTIF-recommended minimum validation distance to be driven (in kilometres) based on published traffic accident statistics. Long term vehicle test/fleet test was chosen as the validation method. The target mileage was calculated using statistical methods and a 4-step analysis. The list of steps is given below and for each step its partial objective is formulated as follows.

1. Possible causes of the hazardous events (C.2.2.2):
   - for the target system, identify hazardous events caused by functional insufficiencies; and
   - clarify the known parameters of the scenarios of realization of the hazardous events and relevant combination of these parameters.

2. Modelling of hazardous events (C.2.2.3):
   - consider representative parameters that can activate system functional insufficiencies; and
   - model the scenarios of hazardous events (accidents).
3. Analysis of traffic statistics (C.2.2.4):
   - identify distributions for basic statistical variables relevant to the scenarios derived on the previous step; and
   - calculate validation mileage benchmarks based on the available statistics.
4. Definition of test scenarios (C.2.2.5):
   - select test scenarios, designed to validate the target application, according to the mission profile and the hazardous scenarios under consideration; and
   - for these scenarios, define the minimum validation effort. C.2.2.5 defines the minimum validation effort in the form of a distance to be driven (in kilometres).

NOTE 1 C.2.2 is related to both area 2 and area 3. SOTIF analyses (Clauses 6 and 7) and the verification of the SOTIF are assumed to be executed prior to production vehicle deployment.

NOTE 2 C.2.2 is based on Reference [30].

C.2.2.2 Possible causes of the hazardous events

Vehicle control systems, which have some authority over the braking system (e.g. AEB), can potentially place the driver or other road users at risk through an erroneous actuation. False activation of emergency braking, caused, for example, by a functional insufficiency in object recognition, swiftly decelerates a vehicle and brings it to a complete stop when not needed.

The triggering conditions that stimulate the hazardous behaviour are identified and evaluated according to this document (see Figure 4, Clause 4), e.g. a collision with a following vehicle due to an unintended AEB actuation. The mentioned performance insufficiency can be triggered by multiple external factors.

For this example, the acceptance criterion is the likelihood of a hazardous event caused by AEB functionality is equal to or smaller than the likelihood of the same hazardous event caused by humans, see Formula (C.4).

$$P_{\text{ha, AEB}} \leq P_{\text{ha, hu}} \tag{C.4}$$

where

$P_{\text{ha, AEB}}$ is the probability of hazardous events caused by AEB functionality;

$P_{\text{ha, hu}}$ is the probability of hazardous events caused by humans.

NOTE C.2.2.2 does not address whether this criterion is sufficient to justify release to the public.

The probability of hazard depends on the scenario, and in particular on values of parameters (e.g. triggering conditions) critical for safety within the scenario. Examples of parameters critical for safety are light conditions for camera-based systems, presence of radar beam reflecting materials for radar-based systems, etc. However, in the area 3 (“unknown hazardous scenarios”) neither all the parameters affecting safety, nor their values are known. Scenarios are defined and their risk estimated based on the known dependencies.

C.2.2.3 Modelling of the hazardous event

The example of C.2.2.3 – C.2.2.5 considers a system able to perform AEB with the deceleration profile shown in Figure C.1 and within the following potential design constraints:

— AEB system commands braking with maximum deceleration of 9 m/s^2 in response to a moving object;

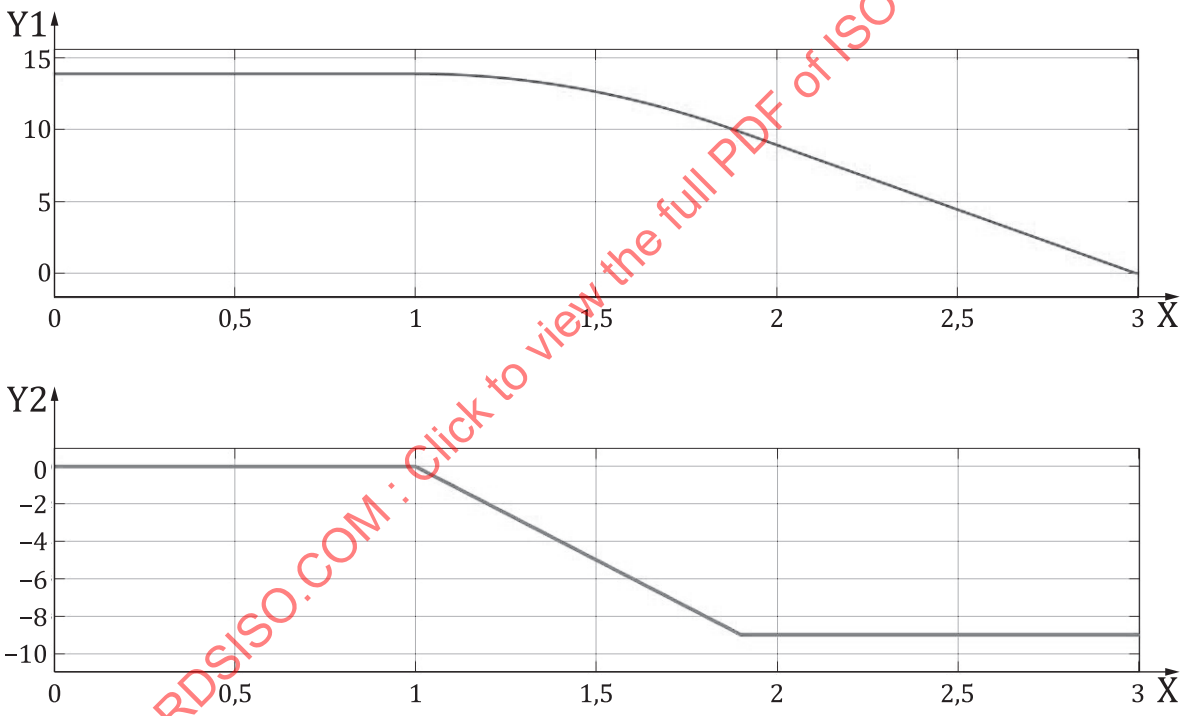
— brake rise time is subject to a brake system pre-fill and limited to 15 m/s^3;

— AEB feature is available above 5 km/h;

— a maximum speed reduction of 50 km/h is allowed; and

— safety mechanisms in the sensor and the braking systems will prevent AEB commanding deceleration outside the designated speed range.

Figure C.1 shows the ideal variation of host vehicle speed as consequence of the AEB deceleration for a starting speed of 50 km/h (equivalent to 13,9 m/s).



Key

X time [s]

Y1 host speed [m/s]

Y2 host vehicle deceleration [m/s^2]

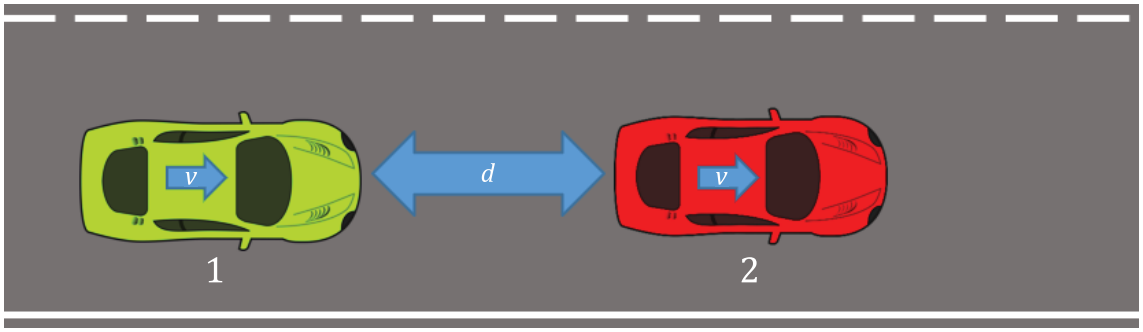
Figure C.1 — Deceleration profile for AEB

The SOTIF-related hazard and the relevant hazardous scenario are:

— **hazardous behaviour**: unintended AEB braking within design intent for longer than 340 ms.

— **hazardous scenario**: undesired braking of the AEB for longer than 340 ms in combination with a closely following vehicle. Under these conditions the undesired braking can lead to a rear-end collision.

This hazardous event can be modelled as a straight road car-following scenario for first order effects (see Figure C.2)[30].



Key

1 trailing vehicle

2 host vehicle

Figure C.2 — Car-following scenario used in the hazardous event model

The scenario is based on the following assumptions:

— at the beginning, both cars are travelling at the same speed *v*;

— the speed dependent trailing distance *d* has known probability distribution[27][28][30];

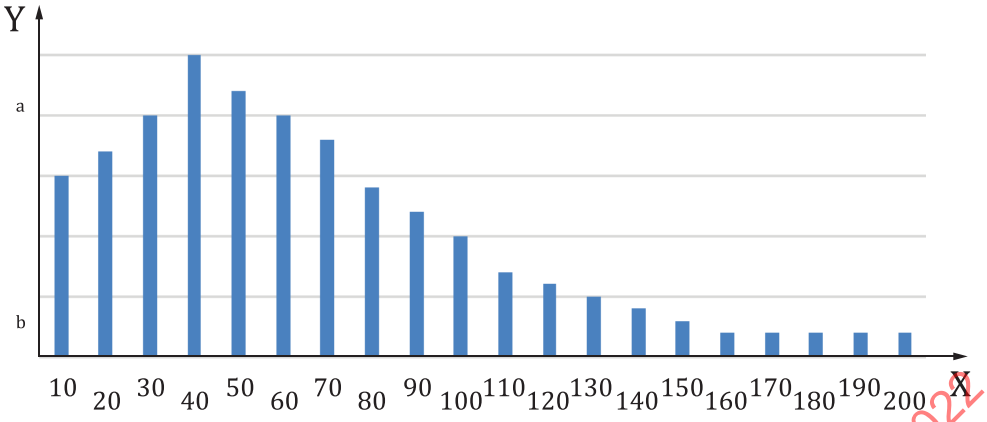
— the first vehicle's AEB activates emergency braking, even though the driving situation does not require that;

— all AEB braking events follow the braking profile pictured on Figure C.1; and

— the following driver perceives the hazardous situation and reacts by braking. The reaction time has a known probability distribution.

The scenario pictured on Figure C.2 ("scenario 1") was analysed using Monte Carlo simulation using trailing distance and reaction time of the following vehicle as input variables to estimate the probability of the hazardous event (rear-end collision). The outcome of the scenario was found to largely depend on the speed of the vehicles at the moment when AEB unintendedly activates. The simulation takes the start speed *v* as input, while the percentage of the simulations that result in a collision is delivered at the output.

Figure C.3 shows that the probability of collision is higher at lower speeds because of the short trailing distance. The rate of collision drops above 50 km/h because of the increased trailing distance and the existence of a maximum speed reduction threshold. Figure C.3 would be different (monotonically increasing) without a speed reduction threshold.



Key

X start speed [km/h]

Y probability of collision

a High.

b Low.

Figure C.3 — Probability of induced rear-end collision in Scenario 1 depending on the speed

C.2.2.4 Analysis of traffic statistics

It is assumed that for AEB the most common accident resulting in injury arises from rear-end collisions between two cars in car-following scenario ("Scenario 1" depicted in Figure C.2). An analysis was performed to identify the maximum tolerable (accepted) occurrence rate of rear-end collisions, i.e. $P_{ha,\,hu}$ in Formula (C.4).

Traffic statistics provided by national road safety authorities (an example is the NHTSA GES data for the US[8], classified by the posted speed in the locality of the accident) can offer an overview of the existing rate at which the collision happens in the field.

Traffic statistics usually provide the following data:

— number of passenger cars in the field (N);

— average distance travelled by each passenger car per year (K);

— alternatively, the total number of vehicle kilometres travelled per year (M) can be provided. If the parameter is not provided, it can be estimated using the formula: $M = N{\cdot}K$; and

— number of relevant accidents (rear end collisions) in the field per year (A).

Confidence in the estimation obtained through further analysis is increased by adopting a statistical model for the variables under consideration. Based on this information, average distance travelled by human drivers between collisions (benchmark, B) can be calculated:

$$B = \frac{M}{A} \tag{C.5}$$

where

B is the average distance travelled by human drivers between collisions (benchmark, B);

M is the total number of vehicle kilometres travelled per year;

A is the number of relevant accidents (rear end collisions) in the field per year.

To obtain the worst-case estimation, the upper bound is to be used for M and the lower bound for the A value.

The safety argument requires evidence that an AEB-equipped vehicle can run at least B kilometres without causing an accident, or that the probability of accident caused by the functional insufficiencies of the AEB system is under $1/B$ per kilometre [compare to Formula (C.4)].

NOTE 1 The criterion presented above is only a probabilistic theoretical measurement to evaluate the risk that can be tolerated in the decision to release the product to the market. Therefore, even if this validation target is met, when undesired AEB occurs in the actual market, the judgment of whether countermeasures are necessary requires additional analyses and considerations based (as an example) on the system architecture, ODD and system specification.

NOTE 2 The benchmark in Formula (C.5) can be considered as lower bound for system validation. Depending on the uncertainty on the traffic statistics, this benchmark can be increased or reduced by multiplying B by factors $\kappa_1\kappa_2$. The definition of benchmark will then be: $B = \kappa_1 \kappa_2 (M/A)$.

EXAMPLE 1 Multiplying the benchmark B by a factor $\kappa_1 > 1$ can be used to conservatively argue that the AEB function will not result in an increase in the number of accidents recorded by the traffic statistics.

EXAMPLE 2 Traffic statistics include justified and unjustified braking events. For false positive AEB braking only the unjustified braking leading to a hazardous event (rear-end collision) is relevant to define a benchmark. κ_2 is defined as the probability of the hazardous event and $\kappa_2 = 1/n$ can be used to adjust for the case that only one in n real-life braking events are leading to a hazardous event due unjustified braking.

NOTE 3 Simulation as described in C.2.2.3 can be used for the estimation of the probability hazardous event due to the unjustified braking κ_2.

C.2.2.5 Definition of the test scenarios

It might not be necessary to drive the number of kilometres equal or exceeding B to show that an acceptable level of residual risk is achieved, provided the acceptance criterion is met with the necessary confidence. Vehicle mission profile (see Table C.1) and the data on the system behaviour can be used to refine the data collection and validation strategy.

Simulation (see C.2.2.3) shows that the highest risk of the AEB is achieved at the speed of 50 km/h. Scenario 1 (Figure C.2) is divided into three scenarios:

— scenario 1.1: v = 0 – 40 km/h;

— scenario 1.2: v = 40 – 80 km/h; and

— scenario 1.3: v > 80 km/h.

Table C.1 provides an analysis of the probability distribution of the severity of rear-end collisions in the US between the years 2010 and 2017 using publicly available data[30]. In this data, the probability of collision and associated severity levels are available per posted speed limit:

— urban roads [speed limits (0-25) mph / (0-40) km/h];

— country roads [speed limits between (25-60) mph / (40-100) km/h]; and

— highways and interstates (speed limits above 60 mph – 100 km/h).

Comparing the areas with highest probability of collision depicted in Figure C.3, with the distribution of severities in Table C.1, we see that those areas coincide for rear-end collisions induced by humans and by the AEB system. The highest risk area corresponds to scenario 1.2.

NOTE A potential AEB activation at a speed of more than 80 km/h violates the limitations of the system. This can, for example, be implemented by an external measure as suggested in the ISO 26262 series and is therefore considered outside the scope of C.2.2.

Table C.1 — Probability distribution of the severity risk of rear-end collision per posted speed limit in the US

Posted speed limit (km/h)	0 – 40	40 – 80	80 – 100	> 100	All speeds
% of rear end collisions (including rear to rear)	9,4 %	69,9 %	12,8 %	7,9 %	100,0 %
No injury	80,0 %	73,3 %	74,6 %	72,9 %	74,1 %
Non-incapacitating injury	18,9 %	24,7 %	22,7 %	25,0 %	24,0 %
Incapacitating injury	1,1 %	1,8 %	2,3 %	1,6 %	1,8 %
Fatal	0,055 %	0,52 %	0,33 %	0,55 %	0,13 %

Assuming statistical data are available, the benchmark [Formula (C.6)] can be recalculated for scenario 1.2:

$$B_{40..80} = \frac{M_{40..80}}{A_{40..80}} \tag{C.6}$$

where

$B_{40\,80}$ is the average distance travelled by human drivers between collisions (benchmark, B) driving between 40 km/h and 80 km/h;

$M_{40\,80}$ is the total number of vehicle kilometres travelled per year when driving between 40 km/h and 80 km/h;

$A_{40\,80}$ is the number of relevant accidents (rear end collisions) in the field per year when driving between 40 km/h and 80 km/h.

For the parameters for which influence on the risk is unknown, data collection can include a comprehensive variety of driving conditions, e.g.:

— weather condition: the AEB system can be tested according to a representative set of weather conditions. This includes dry, fog, snow, rain, overcast etc.; and

— time of day: depending on the type of sensor, data collection can include different times of day, such as night, dusk, etc.

In addition, the data collection can include relevant driving situations derived from analysis of sensor limitations and feature-specific limitations.

An example of vehicle mission profile is given in Table C.2. The specification is based on real-life profiles for weather, speed and other parameters. It can also be based on the data covering scenario occurrence rates, obtained either via simulation or via estimation.

Table C.2 — Example of vehicle mission profile

Time of day		
Type		**Percentage**
Day		50 %
Night		35 %
Dusk		15 %
Vehicle speed		
	Speed [km/h]	**Percentage**
	0..50	60 %
	50..80	40 %
	> 80	0 %

Table C.2 *(continued)*

Weather conditions	
Type	**Percentage**
Dry/clear sky	65 %
Rain	7 %
Fog	5 %
Snow	5 %
Overcast	10 %
Heavy rain	5 %
Other weather conditions	3 %

C.2.2.6 Benchmark considerations

A traffic statistics-based approach as described in C.2.2 can be used to both define a target mean time between collisions (MTBC) benchmark that can be used to validate the driving automation system robustness prior to mass production or field operation. Nevertheless, the main considerations for this method are:

— scalability: applying this method to a fully automated vehicle can prove impractical unless specific considerations with respect to system architecture are made. For the AEB example in C.2.2, extending the feature applicable speed range up to highway speeds (example: 130 km/h) increased the benchmark validation mileage due to the lower frequency of rear-end collisions at such speeds; and

— system architecture independence: considerations on the system architecture can be used to optimise the target validation mileage. In case of complex features in which more than one subsystem is used to redundantly validate a specific control action, the MTBC derived from traffic statistics can be optimised by observing the individual metrics that influence the vehicle-level MTBC (e.g. false positive rate of a camera or radar-based object detection of each subsystem);

— dependency on the validation route: specific driving routes selected after an analysis of system limitations can produce a more accurate definition of the MTBC allowing for a reduction in the quantity of data needed to be collected.

C.3 Validation of SOTIF applicable systems

Figure C.4 denotes a possible model for how V&V iterations, combined with coverage goals and constrained random testing, can be used to discover unknown hazardous scenarios or functional insufficiencies (i.e. reduce area 3) in support of the SOTIF development (Figure 7). In the Initial State (leftmost circle), which is prior to the initiation of V&V, some potential functional insufficiencies, dark grey circles representing area 2, have been identified during the safety analyses. Other functional insufficiencies can exist but are not identified at this stage [black circles, the unknown hazardous scenarios (area 3)]. The dashed square represents the used functionality out of the full set of functionalities (e.g. functionality used within the ODD).

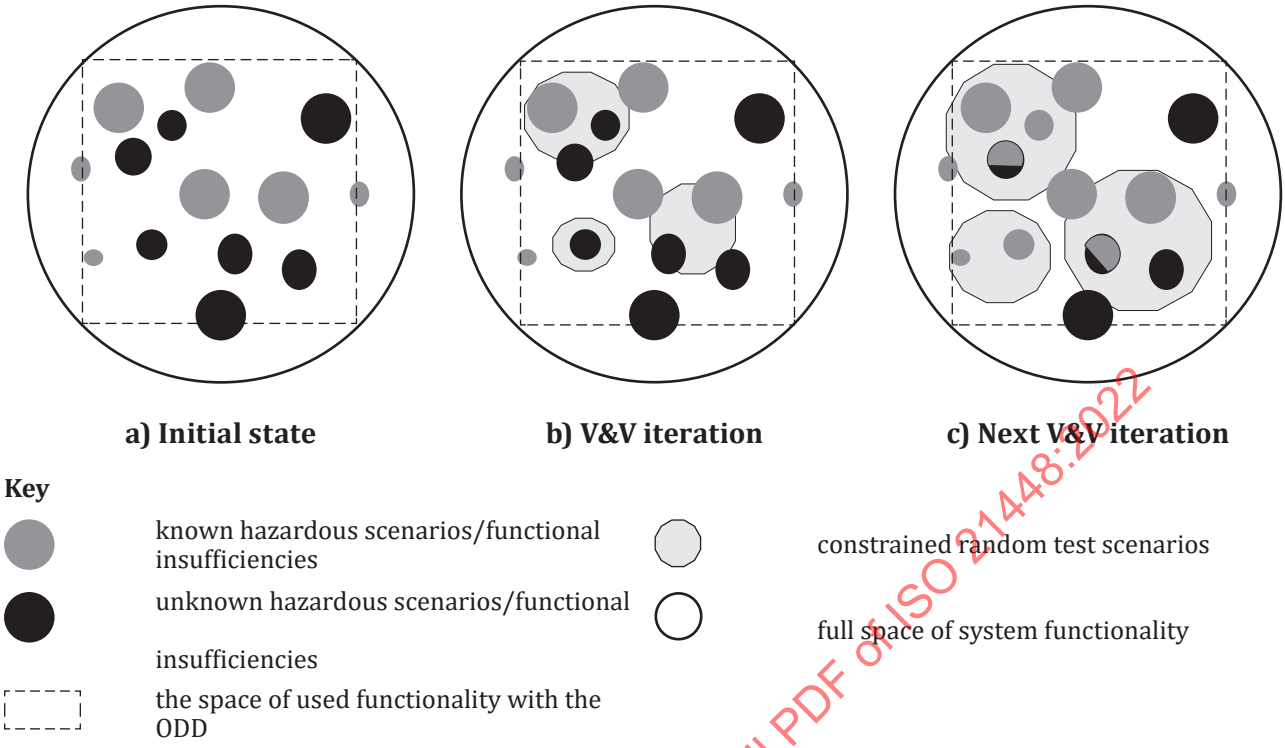


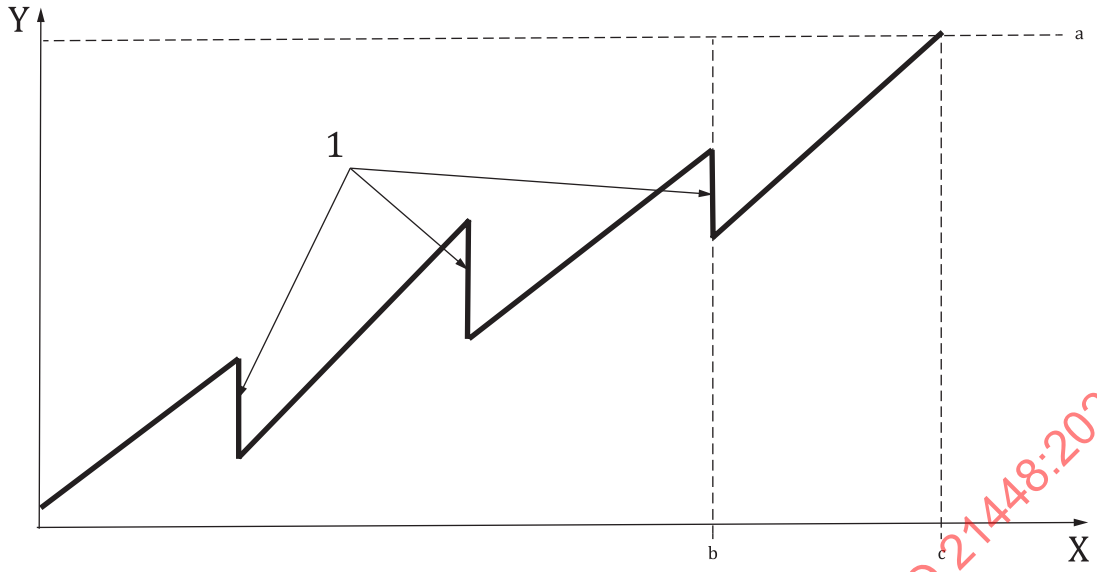
Figure C.4 — SOTIF development testing iterations

The overall V&V goal is to minimize the occurrence of unknown hazardous scenarios, given the ODD boundaries. One method could be to use known scenarios as a basis for constrained random generation of tests of new scenarios, so the testing coverage space is increased incrementally. These new scenarios/tests can be designed to expose unknown hazardous scenarios [Figure C.4 b)] by increasing the covered test space.

The next V&V iteration builds upon the previous one. Exposed unknown scenarios, which are now known, serve as an additional basis for coverage expansion, by extending the random space covered. The previous known scenarios can also be used as a basis for creation of more random tests and scenarios.

This iterative process continues, until sufficient coverage of the used functionality space is achieved. The result is discovery of area 3 scenarios which are then converted into area 2 scenarios [Figure C.4 c)]. Some uncovered hazardous scenarios can be mitigated by reducing the ODD.

The model of Figure C.4 can also be applied to the typical vehicle software development strategy for SOTIF applicable systems. As the software is tested and potentially hazardous behaviours are removed, the average kilometres between potentially hazardous behaviours is expected to rise. However, as new features/functions are introduced or enabled, the average hours or kilometres per potentially hazardous behaviours could drop and then rise as the bugs introduced with the new feature/functions are addressed. Eventually, the validation target threshold is reached for the specified use case and functionality, and the validation activity can be considered to be satisfied. This concept is illustrated by Figure C.5.



Key

X development time
Y average kilometres per unintended behaviour
1 new feature/function implemented
a Validation target.
b Feature/function complete (release candidate).
c Validation criteria met.

Figure C.5 — Expected profile of potentially hazardous behaviour rate during development

For example, prior to testing, the system owner specifies the following:

1) validation target (stopping rule);

2) distribution of test effort between testing modes, real-world tests, HIL, SIL, etc.;

3) definition of potentially hazardous behaviours, criterion for restarting distance counter.

The process of validating SOTIF applicable systems starts with the selection of an acceptance criterion (see 6.5). From this acceptance criterion a validation target is derived. The target can be calculated based on the system use case (e.g. assisted parking, automatic emergency braking, lane keeping, automated parallel parking, low speed automated car park shuttle, highway autopilot, automated taxi), crash statistics for the use case and a safety margin.

The following can be used to form the target:

— statistic to be used;

EXAMPLE 1 Reported collisions.

— human performance in statistic;

EXAMPLE 2 Reported collision 1/500 000 miles 2015 NHTSA crash statistics[29].

— safety margin;

— statistical confidence limit.

EXAMPLE 3 For a particular use case, human drivers experience an average of x kilometres between incidents. For safety reasons an additional margin y>1 is specified. The acceptance criterion for the SOTIF applicable system selected is $B \times y$ average kilometres between potentially hazardous behaviours or a target incident rate of $A_H = 1 / (B \times y)$. The stopping rule assumes that the incidents have a Poisson distribution. Using the validation target τ, the system can be shown to have an incident rate lower than or equal to A_H with a confidence α, if there is τ quantity of driving with no potentially hazardous behaviour, where τ is given in Formula (C.7)[31]:

$$\tau = - \ln(1 - \alpha) / A_H \quad \text{(C.7)}$$

NOTE 1 τ can be in units of time or distance depending on the units of incident rate.

NOTE 2 For $\alpha \approx 0{,}63$, $\tau = 1/ A_H = B * y$.

NOTE 3 The distribution can change over time. For example, it could be necessary to control for the presence of an existing ADAS system such as AEB in the statistics by comparing rates of an events before and after a system's widespread introduction.

In practice, τ, the number of validation kilometres or hours to be driven can be quite large and therefore not practical in some cases. The real-world driving requirement can be lessened by using expert knowledge with similar systems and MIL, SIL and HIL simulated kilometres. An acceptable split between real-world and simulated testing can be specified based on the capabilities of the simulation (e.g. the simulation is only realistic in specific scenarios). Real-world and simulated validation test conditions are varied in a reasonable way (e.g. different weather conditions, time of day, road conditions, traffic conditions, pedestrian conditions, etc.) to try and uncover rare operating situations.

C.4 Perception system verification and validation

C.4.1 Perception system verification and validation framework

C.4.1.1 General

C.4.1 provides an example method that can be used to incrementally verify and validate the performance of a given perception system. Perception systems play a significant role in the SOTIF of an automated vehicle at any level of driving automation. This example method can be applicable to any type of perception technology used in the ADS-equipped vehicle (e.g. radar, camera, lidar, ultrasonic).

Perception system performance is affected by different types of issues that can be introduced in any development phase. It is thus valuable that the perception system undergoes an incremental verification and validation process as described in Figure C.6.

NOTE 1 This sequence of steps is presented as incremental but does not impose a sequence in the execution of such steps.

NOTE 2 The steps can be spanned and shared among multiple companies (see 4.4.2).

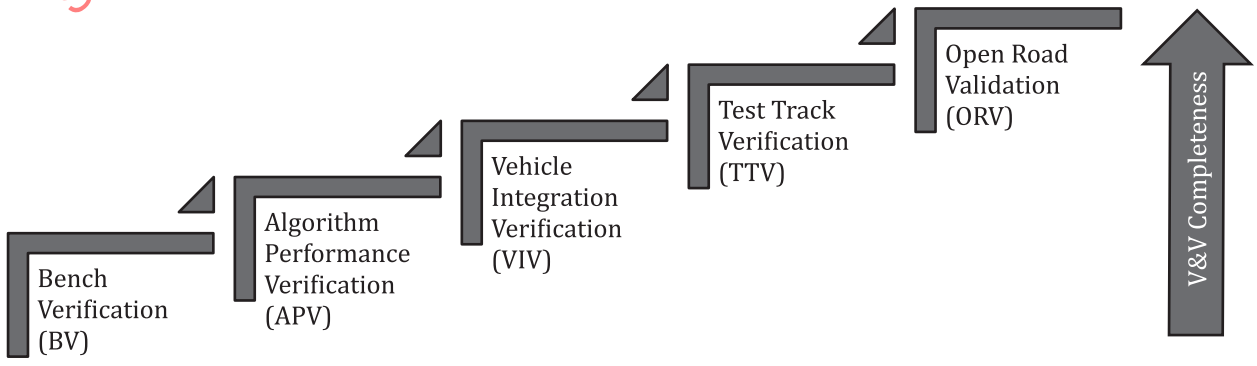


Figure C.6 — Example steps of perception verification and validation

The perception system verification and validation process can include multiple steps:

— bench verification (BV): initial verification of the perception system detection capabilities in a controlled environment;

— algorithm performance verification (APV): perception system performance is verified using larger scale data;

— vehicle integration verification (VIV): perception system performance is verified after integration in the target vehicle;

— test track verification (TTV): perception system performance is verified on a test track against several reference use cases; and

— open road validation (ORV): perception system performance is validated in open road against all relevant scenarios.

C.4.1.2 – C.4.1.6 show analysis examples using SIPOC (Supplier, Input, Process, Output, Customer). SIPOC is a tool that summarizes the inputs and outputs of one or more processes in tabular form and is used to define a process from beginning to end[32]. SIPOC is an analysis method used in quality management and process improvement, but other methods can also be used in the analysis of perception system verification and validation processes.

C.4.1.2 Bench verification

Bench verification activities can be defined to verify the detection capability of the assembled perception system on a reference environment (bench testing). This test is useful to verify the perception system robustness against specific production tolerances in a controlled environment (as an example different tolerable radar antenna sensitivities or different camera focus distances). Table C.3 provides examples of these type of tests.

Table C.3 — Bench verification

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Def	Engineering	Detection requirements (e.g. discrimination and separation capability, accuracy)	Verify the perception system detection performance in a controlled environment according to the product specification.	**Verification passed:** perception system with verified performance in controlled environment **Verification failed:** scrapped perception system (for rework or disposal)	Engineering team (for further testing) OEM/TierX supplier
	Manufacturing	Assembled system (after SMV)			
Ex1	Engineering	Radar detection requirements (KPI)	Verify the correct detection capability in anechoic chamber using a radar target generator.	**Verification passed:** radar with verified detection capability on reference data **Verification failed:** scrapped radar (for rework or disposal)	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled radar (after SMV)			

Table C.3 *(continued)*

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Ex2	Engineering	Camera detection requirements (KPI)	Verify the correct detection capability in front of a screen playing already recorded data or synthetic clips.	**Verification passed:** camera with verified detection capability on reference data **Verification failed:** scrapped camera (for rework or disposal)	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled camera (after SMV)			

C.4.1.3 Algorithm performance verification

Algorithm performance verification activities can be defined to verify the detection capability of the perception system algorithms on a set of reference data (as an example reusing simulations or previously collected data). This test can be useful to verify the absence of performance regressions between incremental SW releases using the same HW:

— different stages of the code expose system behaviour and possible functional insufficiencies;

— derive better robustness from process repetition;

— prevent problems from re-emerging later on during the development process; and

— provide stable base for root cause analysis.

The algorithm performance verification step can be executed either on the target HW (an example of HIL test) or on an emulator (an example of SIL test) by injecting previously recorded or synthetic data. Due to the differences between these two methods, Table C.4 does not provide examples for the application of this verification step to different perception systems. See C.4.1.4 for the description of a technique that can be used for algorithm performance verification.

Table C.4 — Algorithm performance verification

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Def	Engineering	Reference data (pre-collected data or simulated data) Detection requirements/KPI	Verify the correct algorithm performance against a set of reference data (data injection or simulation).	**Verification passed:** verified perception system algorithms **Verification failed:** revise or redesign the perception system algorithm(s)	Engineering team (for further testing) OEM/TierX supplier
		Algorithms and emulation SW (in case of SW in the loop)			
	Manufacturing	Assembled system (in case of HW in the loop)			

C.4.1.4 Vehicle integration verification

Vehicle integration verification activities can be defined to verify that the perception system is capable of performing in the target vehicle and that there are no unexpected performance degradation/alterations. This verification step can be useful to better understand the following:

— that the perception system is capable of using the information provided by the target vehicle (in-vehicle signals like vehicle dynamics signals, etc.); and

— that the perception system can operate without performance degradation due to a specification insufficiency related to the target implementation (e.g. windshield reflectivity for a camera, paint type and thickness in case of a radar integrated behind bumper or incorrect dielectric material placed in front of radar).

Table C.5 presents an example of vehicle integration verification.

Table C.5 — Vehicle integration verification

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Def	Engineering	Vehicle performance specification	Verify that the perception system works according to the specification when used in the target vehicle.	**Verification passed:** verified perception system to vehicle integration **Verification failed 1:** revise or redesign the perception system **Verification failed 2:** revise or redesign the perception system	Engineering team (for further testing) OEM/TierX supplier
	Manufacturing	Assembled perception system Vehicle (representative of target environment)			
Ex1	Engineering	Vehicle communication protocol	Verify that the perception system can use the in-vehicle signals: — vehicle dynamics are received with the right latency. Electrical signals are within specification limit.	Integrated perception system in the vehicle **Verification failed 1:** revise or redesign the perception system **Verification failed 2:** revise or redesign the perception system or vehicle interface	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled perception system Vehicle (representative of target environment)			

Table C.5 *(continued)*

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Ex2	Engineering	Radar expected degradation	The radar system degradation is tested: — degraded performance coming from incorrectly specified bumper shape/curvature (radar behind bumper or logo) — degraded performance coming from incorrectly specified paint (radar behind bumper or logo with incorrect paint thickness or type)	**Verification passed:** integration of radar behind vehicle bumper **Verification failed 1:** revise or redesign the perception system **Verification failed 2:** revise or redesign the perception system or vehicle bumper	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled perception system Vehicle (representative of target environment) / part of the vehicle (representative of target design)	Degraded performance for incorrect dielectric characteristics (incorrectly specified bumper material, incorrect logo design…)		
Ex3	Engineering	Camera Expected degradation	The camera system degradation is tested: — integration of camera behind the windshield Verification of the camera-bracket-windshield assembly	**Verification passed:** integration of camera behind windshield **Verification failed 1:** scrapped perception system (for rework or disposal) Revise or redesign the perception system **Verification failed 2:** revise or redesign the perception system or vehicle bumper	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled perception system Vehicle (representative of target environment) / part of the vehicle (representative of target design)			

C.4.1.5 Test track verification

Test track verification activities can be defined to verify the detection capability of the perception system against a specific set of reference use cases (scenarios, including specific triggering conditions). While use cases (scenarios) themselves generally are “technology agnostic” (do not depend on the

nature of the perception system), a technology-specific set of use cases (scenarios, including specific triggering conditions) can be selected or prioritized to verify the following aspects:

— perception system performance on specific use cases (object detection at specific distances, test scenario like those in protocols developed by car safety performance assessment programmes: Euro NCAP, JNCAP, NHTSA, KNCAP, C-NCAP, Latin NCAP or similar);

— perception system verification in specific scenarios aimed at exploiting perception system limitations (as an example angular accuracy in a radar);

— interaction between ego-vehicle sensor with other ego-vehicle sensors or sensors on other vehicles (e.g. radars jamming each other).

Table C.6 describes an example of test track verification.

Table C.6 — Test track verification

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Def	Engineering	List of use cases Perception system known performance insufficiencies	Verify the perception system performance in specific use cases relevant for the end function.	**Verification passed:** verified perception system performance **Verification failed:** revise or redesign the perception system	Engineering team (for further testing) OEM/TierX supplier
	Manufacturing	Assembled (in vehicle) perception system (after VIV)			
Ex1	Engineering	List of use cases Perception system known performance insufficiencies	Verify the perception system ability to distinguish a pedestrian from a parked vehicle in a given time as part of the AEB Euro NCAP. Obscured vulnerable road user (VRU) scenario proposed by car safety performance assessment programmes.	**Verification passed:** verified perception system performance **Verification failed:** revise or redesign the perception system	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled (in vehicle) perception system (after VIV)			
Ex2	Engineering	Radar-based perception system jamming frequencies	Verify the radar-based perception system anti-jamming capabilities.	**Verification passed:** free from interference radar-based perception system **Verification failed:** revise or redesign the perception system	Engineering team for further testing OEM/TierX supplier
	Manufacturing	Assembled (in vehicle) perception system (after VIV)			

C.4.1.6 Open road validation

Open road validation activities can be defined to validate the perception system performance on the target environment. The goal of the validation phase can include:

— continuous collection of representative data in multiple markets, in a variety of environmental conditions;

— specific data collection, in conditions which are normally rare and less represented in normal driving but that can impact perception, for example:
  — vision perception: data at dusk or dawn;
  — radar perception: rain and splash conditions, salted spray roads;
  — lidar perception: adverse weather conditions; and
  — all perception: tunnel entry/exit;
— specific data collection, in uncommon scenarios that can increase the likelihood of a hazardous behaviour, for example:
  — driving on roads with sparse traffic and no lead cars can increase the probability of incorrect in-path target selection and detection of ghost targets;
  — overtaking a line of trucks with long shadows covering the passing lane(s); and
  — snow sprayed when passing by a snowplough can lead to a sudden blindness of one or more perception systems;
— specific data collection, based on system limitations, for example:
  — technological limitations (radars on metal bridges); and
  — functional/algorithmic limitations (beam control in absence of traffic);
— different driving habits;
— dedicated testing in adverse conditions, for example:
  — weather;
  — infrastructure quality;
  — traffic habits (chaotic vs organised);
  — driving dynamics (lateral and longitudinal);
  — near road clutter (presence of multiple light sources or complicated road furnishings); and
  — traffic conditions (vulnerable road users rich environment versus highway).

Table C.7 describes an example of open road validation.

Table C.7 — Open road validation

Type	Supplier (S)	Input (I)	Process (P)	Output (O)	Customer (C)
Def	Engineering	List of use cases Perception system known performance insufficiencies (after TTV or APV or continuously updated after multiple TTV or APV sessions)	Validate the perception system performance in target use cases depending on the target market, target functionalities and perception system limitations.	**Validation passed:** validate perception system performance in all relevant conditions **Validation failed:** revise or redesign the perception system	Engineering team (for further testing) OEM/TierX supplier
	Manufacturing	Assembled (in vehicle) perception system (after VIV)			

C.4.2 Stochastic sensors models

Complex driving automation systems can require an amount of testing that is not achievable in the physical reality. Simulation in a virtual environment can address a significant part of that testing activity, as a complement to physical testing. Simulation of sensors is one of the critical aspects, since modern sensors are complex and subject to complex, often random phenomena.

Detailed sensor models, based on physics, require large modelling efforts and huge amounts of computing power. Stochastic sensor models offer the following benefits:

— much less need to know every detail of the sensor implementation;

— easy application of Monte-Carlo testing of diverse parameters and situations; and

— medium/low computing power needed.

The approach can be based on parametric or non-parametric approaches: parametric statistics is a branch of statistics which assumes that sample data comes from a population that follows a probability distribution based on a fixed set of parameters. Most well-known elementary statistical methods are parametric. A non-parametric model differs in that the parameter set is not fixed and can increase, or even decrease if new relevant information is collected. Since a parametric model relies on a fixed parameter set, it makes more assumptions about a given population than non-parametric methods. When the assumptions are correct, parametric methods will produce more accurate and precise estimates than non-parametric methods, i.e. have more statistical power. However, when the assumptions are not correct, parametric methods have a greater chance of failing, and for this reason are not robust statistical methods.

For a parametric approach, the sensor model typically reflects the sensor functional structure:

— the sensor is decomposed into functional modules;

— each module is responsible for modelling a specific effect of the detection/measurement process;

— each module is modelled independently;

— each module is characterized by a set of configurable parameters; and

— the output of the emulator is the combination of all steps modelled.

Alternatively, the non-parametric approach focusses on statistical representation of the sensing result, without using detailed modelling of the sensor internal structure, which is modelled as a black box[33].

The typical functional architecture of statistical experiments for the estimation of the sensors parameters is shown in Figure C.7 for the case of a camera sensor model. The input is a database of data recorded from the real world. This input is injected in parallel into the camera test bench and into the stochastic sensor model. The response of the model is compared to the response of the camera test bench. A key performance indicator rewards the model, and an optimization function updates the parameters of the model until the difference is minimized.