



[ISO/TC 22/SC 32/WG 8](#)

Functional safety

E-mail of Secretary: [fritzsche@vda.de](mailto:fritzsche@vda.de)

Secretariat: DIN

### **ISO PAS 21448 FIN 20180620 (2)**

Date of document      2018-06-27

Expected action      Info

#### **Background**

ATTENTION: This is a pre-information. The attached document is not the version for which ISO CS is currently preparing the ISO PAS publication. It is the version which covers the decisions as taken during the observation of the D PAS ISO 21448 and is the document which was submitted for publication to ISO CS.

Please do not further circulate this version. It is an individual copy for you as a member of the development team (ISO TC22/SC32/WG8) to respect your personal engagement in this work.

Only the final version as published by ISO is the official document. We will inform you when it is available, but we are not allowed to share it with you. It is published by ISO and can be purchased via your National Standardization Bodies.

## Road vehicles— Safety of the Intended Functionality

PAS

### Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

© ISO 2018

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland.

## Contents

<b>Foreword .....</b>	<b>5</b>
<b>Introduction.....</b>	<b>6</b>
<b>1 Scope.....</b>	<b>8</b>
<b>2 Normative references.....</b>	<b>8</b>
<b>3 Terms and definitions .....</b>	<b>8</b>
<b>4 Overview of ISO/PAS 21448 activities in the development process .....</b>	<b>13</b>
<b>5 Functional and system specification (intended functionality content) .....</b>	<b>18</b>
5.1 Objectives .....	18
5.2 Functional description.....	18
5.3 Consideration on system design and architecture .....	19
<b>6 Identification and Evaluation of hazards caused by the intended functionality .....</b>	<b>20</b>
6.1 Objectives .....	20
6.2 Hazard identification .....	20
6.3 Hazard analysis .....	22
6.4 Risk evaluation of the intended function .....	23
6.5 Specification of a validation target.....	23
<b>7 Identification and Evaluation of triggering events .....</b>	<b>24</b>
7.1 Objectives .....	24
7.2 Analysis of triggering events .....	24
7.3 Acceptability of the triggering events.....	26
<b>8 Functional modifications to reduce SOTIF related risks .....</b>	<b>27</b>
8.1 Objectives .....	27
8.2 General.....	27
8.3 Measures to improve the SOTIF.....	27
8.4 Updating the system specification .....	29
<b>9 Definition of the Verification and Validation strategy .....</b>	<b>29</b>
9.1 Objectives .....	29
9.2 Planning and specification of integration and testing .....	30
<b>10 Verification of the SOTIF (Area 2) .....</b>	<b>31</b>

10.1 Objectives.....	31
10.2 Sensor verification .....	32
10.3 Decision algorithm verification .....	32
10.4 Actuation verification .....	33
10.5 Integrated system verification.....	33
<b>11 Validation of the SOTIF (Area 3) .....</b>	<b>34</b>
11.1 Objectives.....	34
11.2 Evaluation of residual risk.....	34
11.3 Validation test parameters.....	35
<b>12 Methodology and criteria for SOTIF release.....</b>	<b>36</b>
12.1 Objectives.....	36
12.2 Methodology for evaluating SOTIF for release.....	36
12.3 Criteria for SOTIF release.....	37
<b>Annex A (informative): Examples of the application of SOTIF activities.....</b>	<b>39</b>
<b>Annex B (Informative): Example for definition and validation of an acceptable false alarm rate in AEB systems.....</b>	<b>42</b>
B.1 Objective and Structure of this Annex.....	42
B.2 Partition of system failures.....	43
B.3 Modelling of the hazardous event.....	44
B.4 Analysis of traffic statistics .....	46
B.5 Definition of the amount of data collection.....	47
<b>Annex C (informative): Validation of SOTIF Applicable Systems .....</b>	<b>49</b>
<b>Annex D (informative): Automotive perception systems verification and validation .....</b>	<b>51</b>
<b>Annex E (informative) Method for deriving SOTIF misuse scenarios .....</b>	<b>53</b>
<b>Annex F (informative) Example construction of scenario for SOTIF safety analysis method .....</b>	<b>56</b>
<b>Annex G (informative): Implications for Off-line Training.....</b>	<b>58</b>

## 1 Foreword

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

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

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

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

19 For an explanation on the meaning of ISO specific terms and expressions related to conformity  
20 assessment, as well as information about ISO's adherence to the WTO principles in the Technical  
21 Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

22 The committee responsible for this document is ISO/TC22/SC32/WG8

23 PAS 21448 consists of this document only.

24

## 26 Introduction

27 The safety of road vehicles during their operation phase is of paramount concern for the road vehicles  
 28 industry. Recent years have seen a huge increase in the number of advanced functionalities included in  
 29 vehicles. These rely on sensing, processing of complex algorithms and actuation implemented by  
 30 electrical and/or electronic (E/E) systems.

31 An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by  
 32 every hazard associated with the intended functionality and its implementation, especially those not  
 33 due to failures, e.g. due to performance limitations. ISO 26262 defines the vehicle safety as the absence  
 34 of unreasonable risks that arise from malfunctions of the E/E system. ISO 26262-3 specifies a Hazard  
 35 Analysis and Risk Assessment to determine vehicle level hazards. This evaluates the potential risks due  
 36 to malfunctioning behaviour of the item and enables the definition of top-level safety requirements, i.e.  
 37 the safety goals, necessary to mitigate the risks. The other parts of ISO 26262 provide requirements and  
 38 recommendations to avoid and control random hardware failures and systematic failures that could  
 39 violate safety goals.

40 For some systems, which rely on sensing the external or internal environment, there can be potentially  
 41 hazardous behavior caused by the intended functionality or performance limitation of a system that is  
 42 free from the faults addressed in ISO26262. Examples of such limitations include:

- 43 • The inability of the function to correctly comprehend the situation and operate safely; this also  
 44 includes functions that use machine learning algorithms;
- 45 • Insufficient robustness of the function with respect to sensor input variations or diverse  
 46 environmental conditions.

47 The absence of unreasonable risk due to these potentially hazardous behaviours related to such  
 48 limitations is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed  
 49 by ISO 26262) and SOTIF are distinct and complementary aspects of safety.

50 To address the SOTIF, activities are implemented during the following phases:

- 51 • Measures in the design phase;  
 52       EXAMPLE     Requirement on sensor performance.
- 53 • Measures in the verification phase;  
 54       EXAMPLE     Technical Reviews, test cases with a high coverage of relevant scenarios, injection of  
 55                      potential triggering events, in the loop testing (e.g. SIL / HIL / MIL) of selected SOTIF are relevant use  
 56                      cases.
- 57 • Measures in the Validation phase;  
 58       EXAMPLE     Long term vehicle test, simulations.

59 A proper understanding of the function by the user, its behavior and its limitations (including the  
 60 human/machine interface) is the key to ensuring safety.

61 In many instances, a triggering event is necessary to cause a potentially hazardous behaviour; hence the  
62 importance of analysing hazards in the context of particular use cases.

63 In this document the hazards caused by a potentially hazardous system behaviour, due to a triggering  
64 event, are considered both for use cases when the vehicle is correctly used and for use cases when it is  
65 incorrectly used in a reasonably foreseeable way (this excludes intentional alterations made to the  
66 system's operation).

67 EXAMPLE Lack of driver attention while using a level 2 driving automation

68 In addition, reasonably foreseeable misuse, which could lead directly to potentially hazardous system  
69 behaviour, is also considered as a possible triggering event.

70 A successful attack exploiting vehicle security vulnerabilities can also have very serious consequences  
71 (i.e. data or identity theft, privacy violation, etc.). Although security risks can also lead to potentially  
72 hazardous behaviour that needs to be addressed, security is not addressed by this document.

73 It is assumed that the E/E random hardware faults and systematic faults of the E/E system are  
74 addressed using ISO 26262. The activities mentioned in this document are complementary to those  
75 given in ISO 26262.

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

77 Table 1: Overview of safety relevant topics addressed by different ISO standards

Source	Cause of hazardous event	Within scope of
System	E/E System failures	ISO 26262
	Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO/PAS 21448
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload)	ISO/PAS 21448 ISO 26262 European statement of principal on the design of human-machine-interface
	Hazards caused by the system technology	Specific standards
External factor	successful attack exploiting vehicle security vulnerabilities	ISO21434 or SAE J3061
	Impact from active Infrastructure and/or vehicle to vehicle communication, external devices and cloud services.	ISO 20077; ISO 26262
	Impact from car surroundings (other users, "passive" infrastructure, environmental conditions: weather, Electro-Magnetic Interference...)	ISO/PAS 21448 ISO 26262

78

79 NOTE Options for automated driving level definitions (from NHTSA, SAE and OICA etc.) are discussed in the ITS-  
80 Informal Group ECE/TRANS/WP29.



## 81 1 Scope

82 The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the  
83 intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of  
84 The Intended Functionality (SOTIF). This document provides guidance on the applicable design,  
85 verification and validation measures needed to achieve the SOTIF. This document does not apply to  
86 faults covered by ISO26262 or to hazards directly caused by the system technology (e.g. eye damage  
87 from a laser sensor).

88 This document is intended to be applied to intended functionality where proper situational awareness  
89 is critical to safety, and where that situational awareness is derived from complex sensors and  
90 processing algorithms; especially emergency intervention systems (e.g. emergency braking systems)  
91 and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA / SAE standard J3016  
92 automation scales. This edition of the document can be considered for higher levels of automation,  
93 however additional measures might be necessary. This document is not intended for functions of  
94 existing systems for which well-established and well-trusted design, verification and validation (V&V)  
95 measures exist at the time of publication (e.g. Dynamic Stability Control (DSC) systems, airbag, etc.).  
96 Some measures described in this document are applicable to innovative functions of such systems, if  
97 situational awareness derived from complex sensors and processing algorithms is part of the  
98 innovation.

99 Intended use and reasonably foreseeable misuse are considered in combination with potentially  
100 hazardous system behaviour when identifying hazardous events.

101 Reasonably foreseeable misuse, which could lead directly to potentially hazardous system behaviour, is  
102 also considered as a possible event that could directly trigger a SOTIF-related hazardous event.

103 Intentional alteration to the system operation is considered feature abuse. Feature abuse is not in scope  
104 of this document.

## 105 2 Normative references

106 Documents (in whole or in part) that are normatively referenced in this document are indispensable for  
107 its application. For dated references, only the edition cited applies. For undated references, the latest  
108 edition of the referenced document (including any amendments) applies.

109 ISO 26262 - 1:2018, *Road vehicles — Functional Safety Part 1: Vocabulary*

## 110 3 Terms and definitions

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

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

113 — ISO Online browsing platform: available at <http://www.iso.org/obp>.

114 For the purposes of the ISO 26262 series of standards, the terms and definitions from ISO 26262:2018-  
115 1 apply, with the following additions:

### 116 3.1

#### 117 action

118 atomic behaviour that is executed by any actor in a scene

119 Note to entry: The temporal sequence of actions/events and scenes specify a scenario.

120 EXAMPLE to entry Ego vehicle activates the hazard warning lights

### 121 3.2

#### 122 erroneous pattern

123 input that can trigger unintended behaviour

### 124 3.3

#### 125 event

126 occurrence at a certain place and at a particular point in time

127 Note 1 to entry: The temporal sequence of actions/events and scenes specify a scenario.

128 Note 2 to entry: In particular this document addresses *triggering events* (3.15) and hazardous events. A hazardous  
129 event is the combination of a hazard (caused by malfunctioning behaviour) and a specific operational situation.  
130 Refer to Figure 11 for details.

131 EXAMPLE 1 to entry: Tree falling on a street 50 m ahead of a vehicle XY

132 EXAMPLE 2 to entry: Traffic light turning green at time XX:XX.

### 133 3.4

#### 134 functional improvement

135 modification to a function, system or element specification to reduce risk

### 136 3.5

#### 137 intended behaviour

138 specified behaviour of the intended functionality including interaction with items

139 Note 1 to entry: See Clause 5 for additional information about the specification of intended behaviour.

140 Note 2 to entry: The specified behaviour is the behaviour that the developer of the item considers to be the  
141 nominal (i.e. fault-free) functionality, with its capability limitations due to inherent characteristics of the  
142 components and technology used.

### 143 3.6

#### 144 intended functionality

145 behaviour specified for a system

### 146 3.7

#### 147 misuse

148 usage of the system by a human in a way not intended by the manufacturer of the system

149 Note 1 to entry: Misuse can result from overconfidence in the performance of the system.

150 Note 2 to entry: Misuse includes human behaviour that is not specified but does not include deliberate system  
151 alterations.

### 152 3.8

#### 153 misuse scenario

154 scenario in which misuse occurs

### 155 3.9

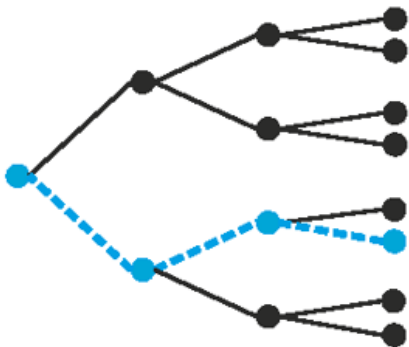
156 **performance limitation**  
 157 insufficiencies in the implementation of the intended functionality

158 EXAMPLE incomplete perception of the scene, insufficiency of the decision algorithm, insufficient  
 159 performance of actuation

160 **3.10**  
 161 **Safety Of The Intended Functionality (SOTIF)**  
 162 absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended  
 163 functionality or from reasonably foreseeable misuse by persons

164 Note 1 to entry: Nominal performance includes intended functionality and the implementation of intended  
 165 functionality that can be affected by performance limitations or by foreseeable misuse by persons.

166 **3.11**  
 167 **scenario**  
 168 description of the temporal development between several scenes in a sequence of scenes

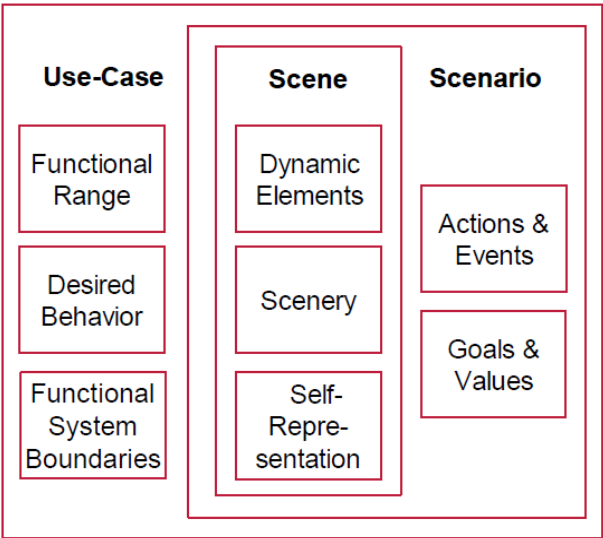


169

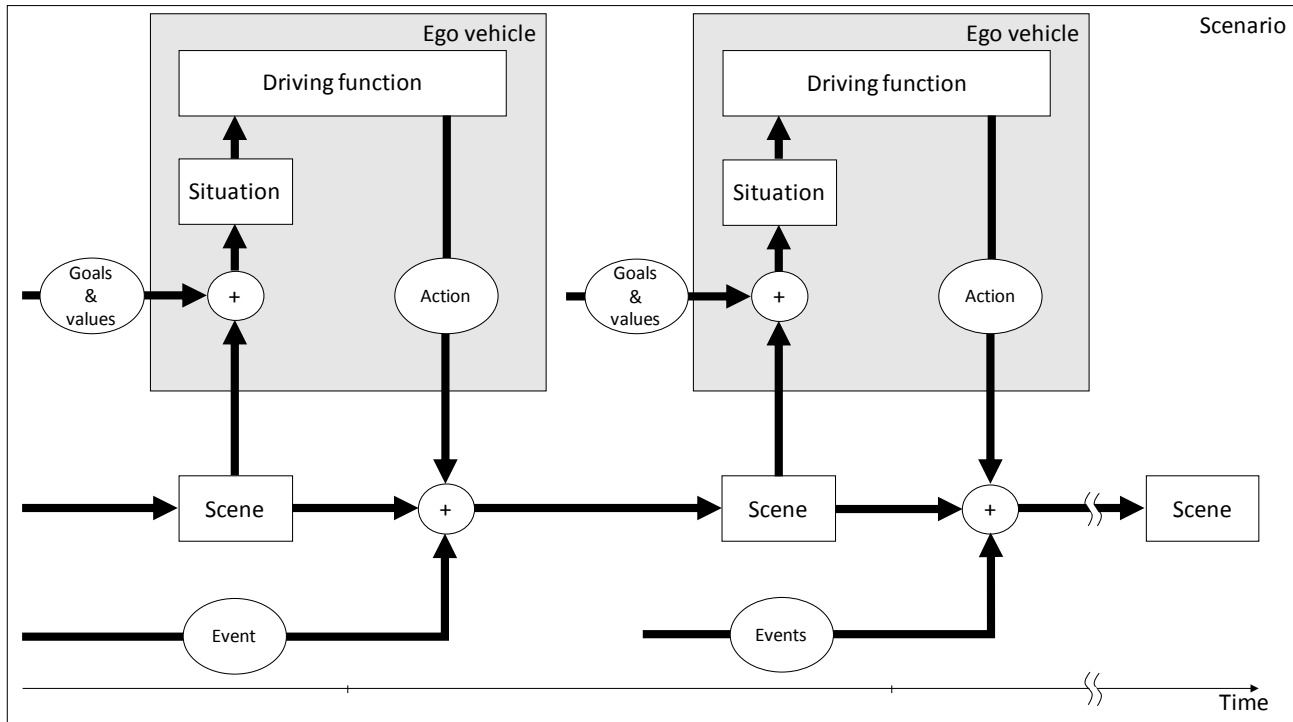
170 **Figure 1: Scenario (dashed) as a temporal sequence of actions/events (edges) and scenes**  
 171 **(nodes)**

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

175 Note 2 to entry: See figures 2 and 3 [1].



### Figure 2: Taxonomy of use case, scene and scenario



**Figure 3: Temporal view of scenes, events, actions and situations in a scenario**

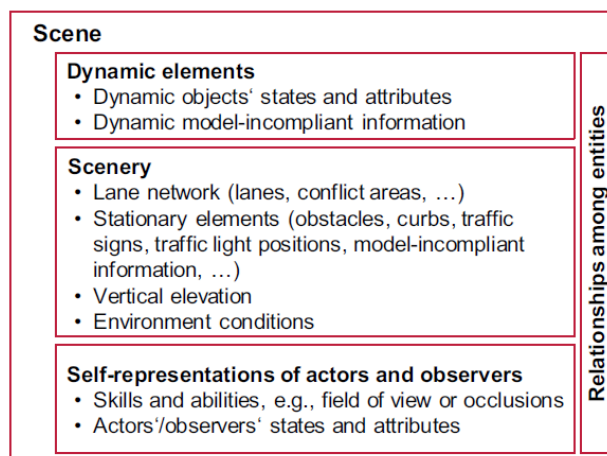
### 3.12

**scene**

snapshot of the environment including the scenery, dynamic elements, and all actor and observer self-representations, and the relationships between those entities.

Note 1 to entry: Only a scene representation in a simulated world can be all-encompassing (i.e. an objective scene, or ground truth). In the real world the scene is incomplete, incorrect, uncertain, and from one or several observers' points of view (i.e. a subjective scene).

Note 2 to entry: Refer to [1].



### Figure 4: Characteristics of a scene

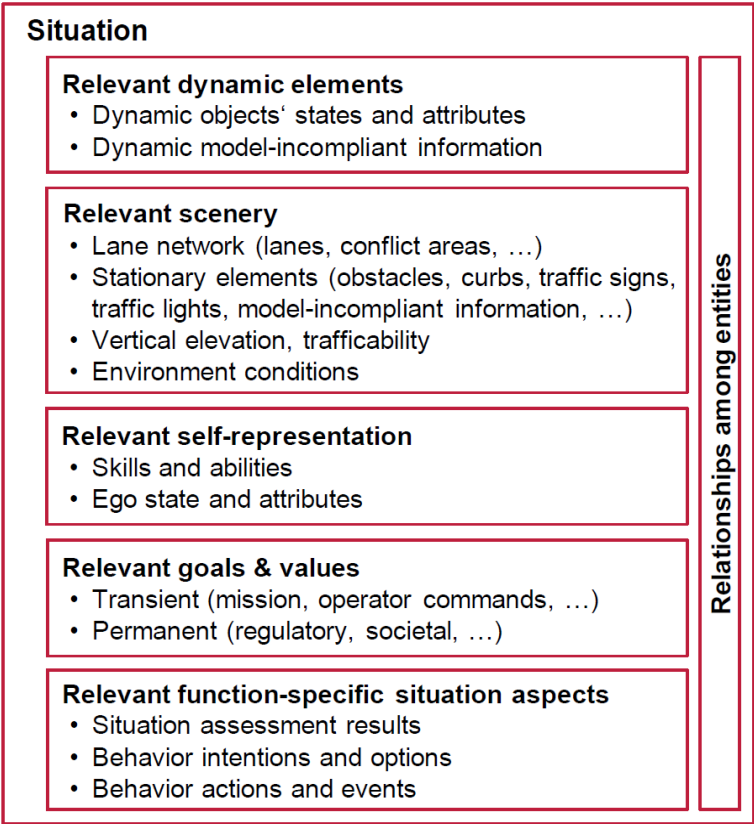
### 3.13

**situation**

selection of an appropriate behaviour pattern at a particular point of time

193 Note 1 to entry: A situation entails all relevant conditions, options and determinants for the behaviour. A situation  
 194 is derived from the scene, by an information selection and augmentation process that is based on transient (e.g.  
 195 mission-specific) as well as permanent goals and values. Hence, a situation is always subjective as it represents an  
 196 element's point of view.

197 Note 2 to entry: Refer to [1]



198  
 199 **Figure 5 : characteristics of a situation**

200 **3.14**  
 201 **test case**

202 set of conditions to determine if a system is working according to its intended functionality

203 Note 1 to entry: A test case entails a (logical) scenario with a specific set of parametric values for each aspect of  
 204 the scenario, together with the pass-fail criteria on which to evaluate it.

205 Note 2 to entry: Refer [2]

206 **3.15**  
 207 **triggering event**

208 specific conditions of a driving scenario that serve as an initiator for a subsequent system reaction  
 209 possibly leading to a hazardous event

210 **EXAMPLE** While operating on a highway, a vehicle's automated emergency braking (AEB) system  
 211 misidentifies a road sign as a lead vehicle resulting in braking at X g for Y seconds.

212 **3.16**

213 **use case**

214 specification of a generalized field of application, possibly entailing the following information about the  
215 system:

- 216 • one or several scenarios;
- 217 • the functional range;
- 218 • the desired behaviour; and
- 219 • the system boundaries.

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

222 **3.17**

223 **unexpected item behaviour**

224 unintended behaviour not specified

225 Note to entry: The unintended behaviour might be discovered during validation.

226 **3.18**

227 **validation**

228 set of activities gaining confidence that an item is able to accomplish its expected functionalities and  
229 missions

230 Note to entry: Verification activities address mainly Area 2 of Figures 7, 8 and 9 including the verification of  
231 known use cases, whereas Validation activities address mainly Area 3 of Figures 7, 8 and 9 including the validation  
232 of SOTIF in unknown use cases.

## 233 **4 Overview of ISO/PAS 21448 activities in the development process**

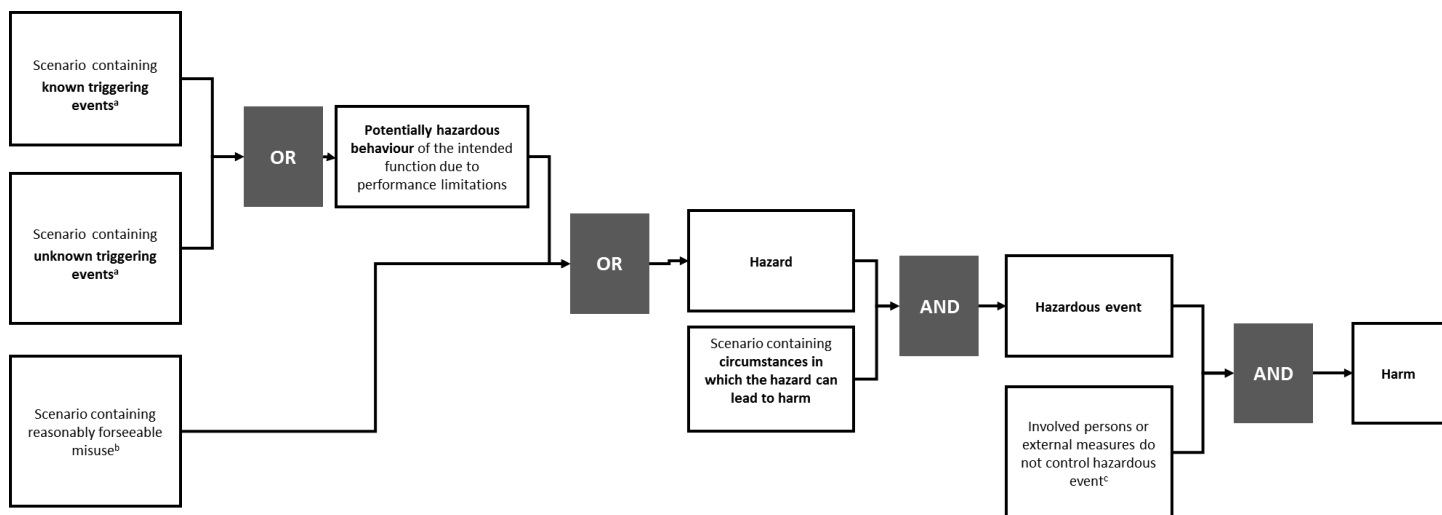
234 The objective clauses of ISO 21448 (Clauses 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1 and 12.1) are normative. All  
235 other content is informative. Compliance to this document can be claimed by listing the objectives and  
236 providing an argument that the objectives have been achieved.

237 A development interface agreement can be defined between all development parties when applicable  
238 for a distributed product development. The goal of an agreement is to confirm in the early stages of a  
239 project all responsibilities of the SOTIF activities.

240 Achieving SOTIF requires some activities which are complementary to ISO 26262:2018. One of the main  
241 objectives of ISO/PAS 21448 is to document the process and rationale used to ensure that the likelihood  
242 of a hazardous event is sufficiently low. Furthermore, ISO/PAS 21448 also seeks to assess that the  
243 remaining residual risk from

- 244 i. a system not able to process a given scenario in a safe manner and
- 245 ii. the involved persons (driver, other vehicle occupants, or bystanders) are not capable of
- 246 mitigating the hazardous event, is acceptable (see Figure 6).

The functional and system specification includes relevant use cases and those use cases are comprised of several relevant scenarios. These scenarios could contain triggering events (see Clause 3 definitions) that lead to harm (see Figure 6).



247 Key:

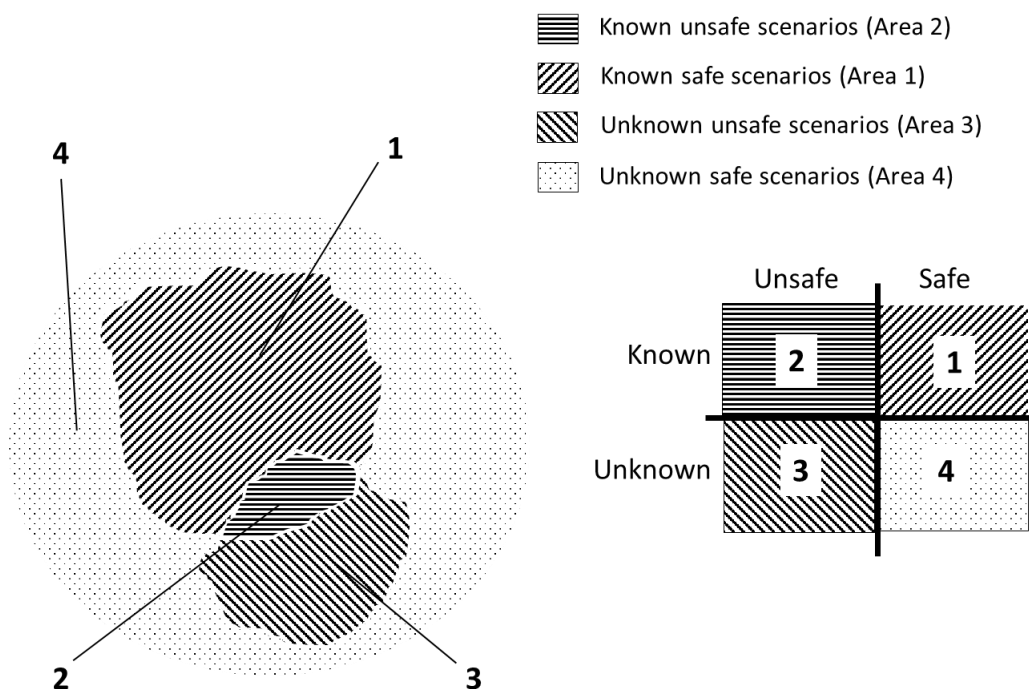
248 <sup>a</sup>These scenarios can also be caused by reasonably foreseeable misuse, e.g. activating a functionality intended for  
 249 the highway in an urban setting causes the vehicle to be in a scenario in which it does not detect a red traffic light

<sup>b</sup> Reasonably foreseeable misuse can lead directly to a hazard, e.g. in case of mode confusion where the driver assumes that the system is active even though it is deactivated.

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

250 **Figure 6—Visualisation of a Potential SOTIF-related Hazardous Event Model**

251 Within this document, the scenarios which are part of the relevant use cases are therefore classified  
 252 into four areas (see Figure 7).



253

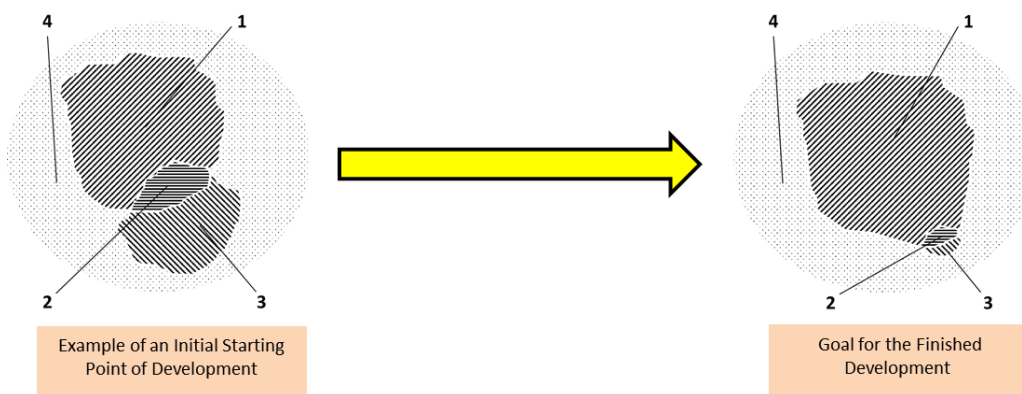
254 **Figure 7 —Visualisation of the Known/Unknown and Safe/Hazardous Scenario categories**

255 Areas 1, 2 and 3 are used as a mental model to structure this document. Area 4 is referenced for  
256 completeness but is not needed for the purposes of this document and therefore not used further. When  
257 considering the areas in the model, it can be useful to imagine their size as representing the proportion  
258 of each type of scenario that falls within each respective area.

259 A given use case can include known as well as unknown scenarios.

260 At the beginning of the development Areas 2 and Area 3 might be too large, resulting in unacceptable  
261 residual risk. The ultimate goal of the SOTIF activities to evaluate the SOTIF in Area 2 and Area 3 and to  
262 provide an argument that these areas are sufficiently small and therefore that the resulting residual risk  
263 is acceptable. While the known scenarios and the corresponding use cases of Area 2 can be explicitly  
264 evaluated, the scenarios and corresponding use cases of Area 3 are evaluated by industry best practice  
265 or by other approaches such as design measures, systematic analyses, or dedicated experiments. The  
266 results of these evaluations provide an argument that Area 3 is sufficiently small and Area 2 is managed  
267 through SOTIF improvements and therefore the probability of encountering these kinds of scenarios is  
268 sufficiently low.

269 It is expected that Areas 2 and Area 3 will be reduced and Area 1 will grow during development (see  
270 Figure 8).



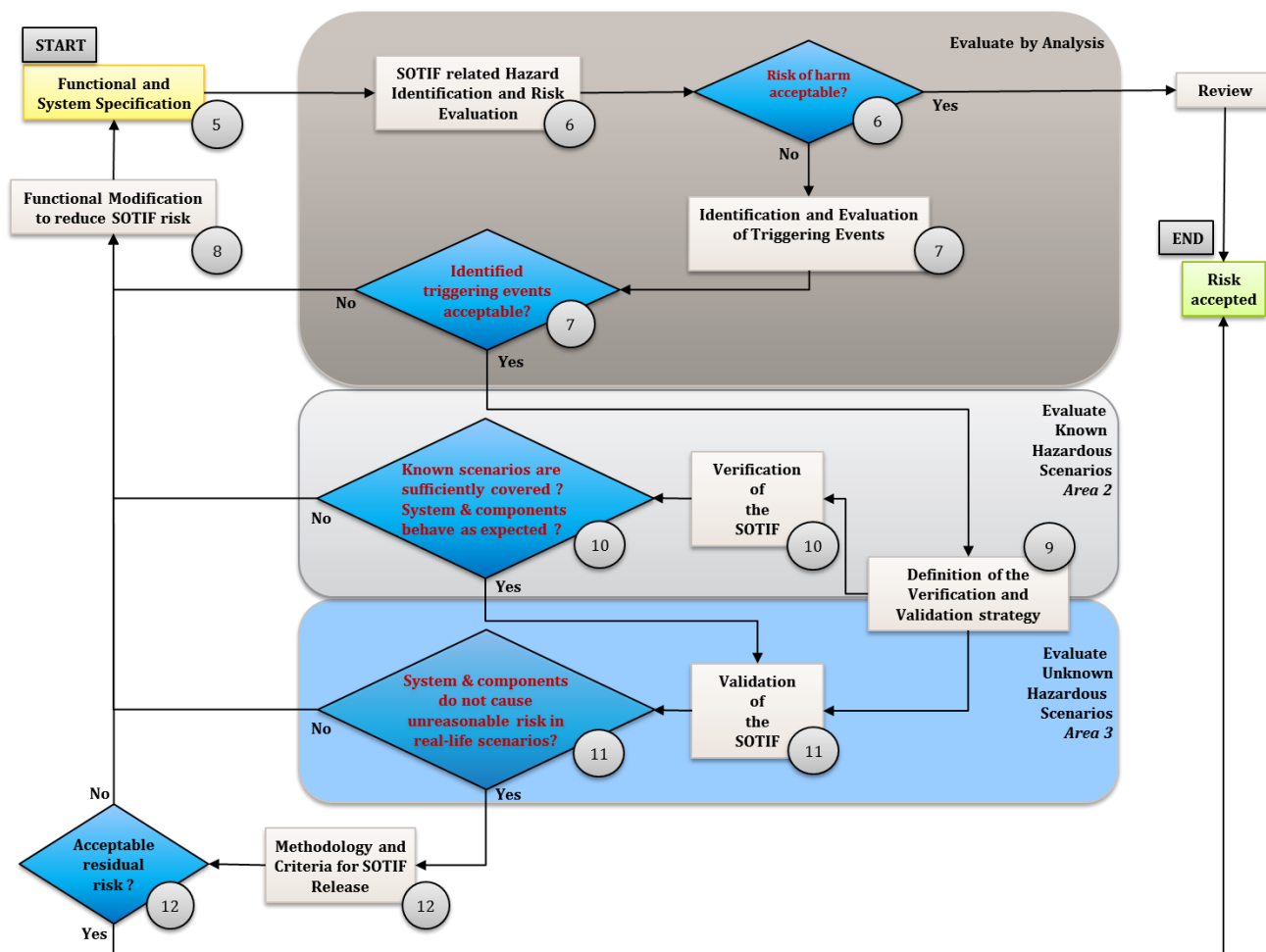
272 **Figure 8 – Evolution of the scenario categories resulting from the ISO/PAS 21448 activities**

273 The goals of the SOTIF process with respect to Area 1, Area 2, and Area 3 and relevant scenarios are:

- 274 – Area 1: Maximize or maintain area, while minimizing Areas 2 & 3. This retains or improves safe  
275 functionality.
- 276 – Area 2: Minimize area with technical measures to an acceptably small level, with statistical  
277 significance of that level appropriate to the relative impact of the technical measure; evaluate  
278 the potential risk and, if necessary, move hazardous scenarios into Area 1 by improving the  
279 function or by restricting the use/performance of the function.
- 280 – Area 3: Minimize area (the risk of the unknown) as much as possible with an acceptable level of  
281 effort (every detected hazardous scenario is moved into Area 2)

282 Figure 9 describes a flowchart for the improvement of the intended functionality to ensure its safety.  
283 The circled numbers denote the corresponding clauses within this document.





**Figure 9—Flowchart of the ISO/PAS 21448 activities**

In Figure 9, the process starts with a **definition of the functional and system specification** (see Clause 5). The possible hazardous behaviours of the intended function are subjected to a **Hazard Identification and Risk Evaluation** (see Clause 6) that identifies potential hazardous events. If it is shown that these potentially hazardous events do not lead to harm, then no improvement is necessary and the intended functionality can be considered free from unreasonable risk.

If it is shown that harm is possible, then an **analysis of the possible hazardous triggering events** (e.g. misdetection of certain objects under certain environmental conditions or driver misuse) is conducted (see Clause 7).

Clause 6 and Clause 7 address different aspects of the SOTIF. **Clause 6 does not consider the causes of possible hazardous intended behaviour of the function, but only their consequences for safety.** Clause 6 is, therefore, focused on evaluating hazardous events that could result from hazardous intended behaviour, and on defining the verification and validation targets to be met. **Clause 7 addresses the analysis of the causes of potentially hazardous behaviour.** These are mitigated in Clause 8 and verified and validated in Clause 9, Clause 10 and Clause 11.

**Functional improvement or restrictions of the use cases are applied to avoid these hazards or to further reduce the resulting risk** (see Clause 8).

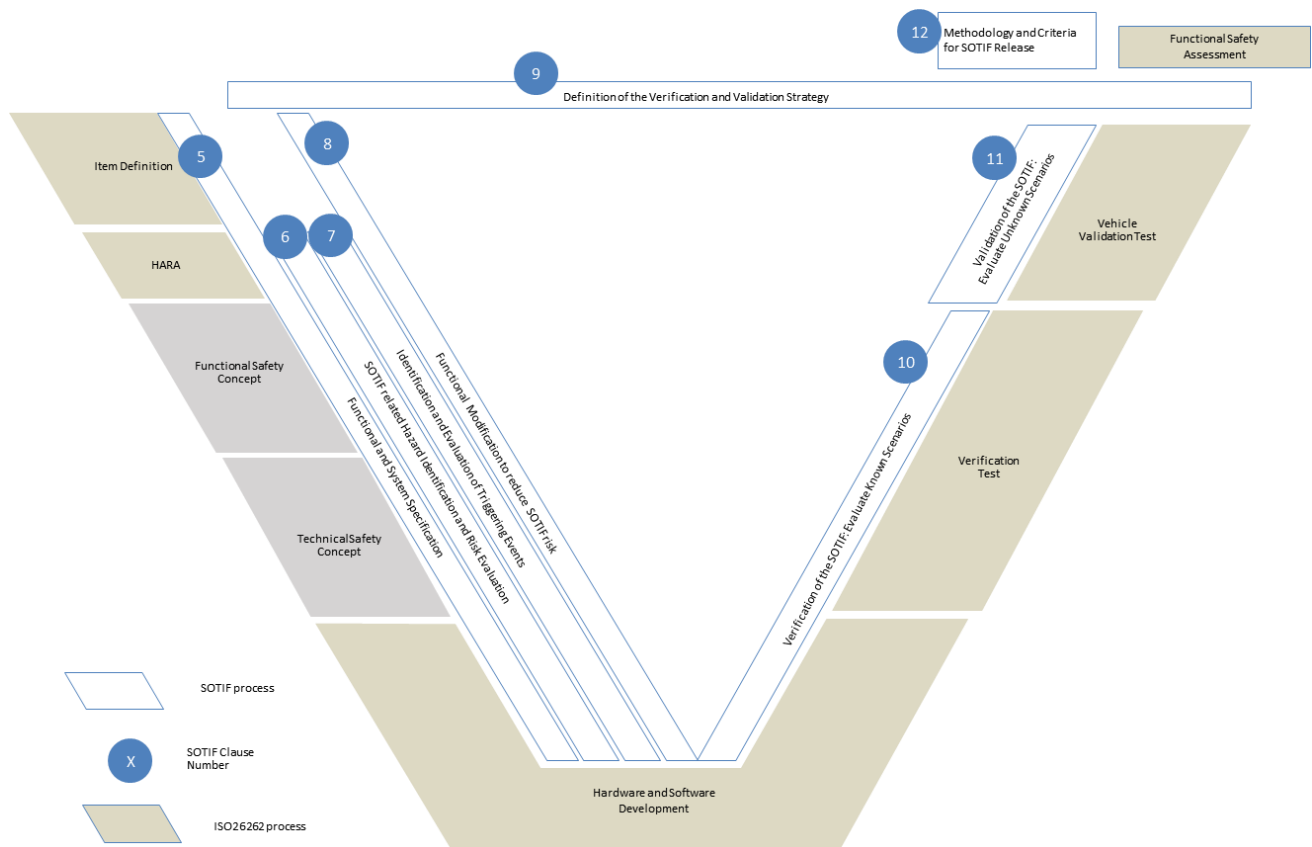
A **verification and validation strategy** is developed to provide an argument that the residual risk is below an acceptable level (see Clause 9). This includes enforcement of the resulting strategy. Corresponding **verification and validation test cases** can be derived from this analysis (see Clauses 10 & 11).

306 Finally, the residual risk is evaluated (Clause 12) considering the results from verification and  
 307 validation. If the risk is determined to be unacceptable, further functional improvement or restrictions  
 308 of the use cases can be necessary (Clause 8). This verification and validation strategy can include  
 309 model-in-the-loop (MIL), software-in-the-loop (SIL), hardware-in-the-loop (HIL), test track  
 310 experiments, dedicated analyses, long-term endurance tests, or other approaches.

311 Possible causes of unintended behaviour considered in this document are closely related to the  
 312 performance of sensing, processing of algorithms, actuation, and their implementation for the  
 313 functionality under development. Therefore, ISO/PAS 21448 activities are applicable to the vehicle,  
 314 system, and component levels.

315 Similarly, the selection of a capable, overall system architecture becomes a primary concern to ensure  
 316 the SOTIF, and, to ensure that overall capability, corresponding activities take place both at early stages  
 317 and throughout the overall functional development lifecycle.

318 It can be necessary to include specific mechanisms to ensure the SOTIF. For instance, a dedicated  
 319 Human-Machine Interface (HMI) can be defined to prevent/mitigate some reasonably foreseeable  
 320 misuses by the driver (see Annex E). During the product development, both ISO/PAS 21448 activities  
 321 and ISO 26262 activities are carried out and the measures for SOTIF are evaluated.



322

323 **Figure 10 - Possible Interactions of Product Development activities between ISO/PAS 21448 and**  
 324 **ISO26262 processes**

325 Figure 10 describes possible interactions between the ISO/PAS 21448 and ISO 26262 activities. The  
 326 product development phases will typically require several iterations to produce a final functional and  
 327 system specification. These iterations are not represented in the figure.

328 A set of methods and measures are selected in order to:

- 329 – Identify and evaluate the SOTIF related hazards associated with the intended functionality  
330 (Clause 6);
- 331 – Identify and evaluate hazardous triggering events (Clause 7);
- 332 – Improve the system design as necessary through functional modifications or use case restriction  
333 to reduce SOTIF risk (Clause 8) and
- 334 – Verify and validate the appropriateness of the design with respect to the SOTIF (Clause 9-11).

335 NOTE The hazard identification process is similar to the process described in ISO 26262-3:2018, because the  
336 vehicle-level effects of SOTIF related potentially hazardous behaviour and the system failures covered by ISO  
337 26262 can be identical.

338 This document provides a non-exhaustive collection of methods and measures, from which the  
339 development team can select the appropriate combination. Other equivalent methods can also be  
340 applied.

## 341 **5 Functional and system specification (intended functionality content)**

### 342 **5.1 Objectives**

343 The functional and system specification activity shall:

- 344 • Compile and create evidence containing the information sufficient to initiate the SOTIF related  
345 activities;
- 346 • Update the evidence as necessary after each iteration of the SOTIF related activities (see Figure  
347 9)

### 348 **5.2 Functional description**

349 The functional and system specification includes (where applicable):

#### 350 Function related:

- 351 • The goals of the intended functionality;
- 352 • The use cases in which the intended functionality is activated, deactivated and active;
- 353 • The description of the intended functionality;
- 354 • The level of automation / authority over the vehicle dynamics; and
- 355 • The dependencies on, and interaction with:
  - 356 ○ the car driver, passengers, pedestrians and other road users;
  - 357 ○ relevant environmental conditions and
  - 358 ○ the interfaces with the road infrastructure.

#### 359 System related:

- 360 • The description of the system and elements implementing the intended functionality.
- 361 • The description and behaviour of the installed sensors, controllers and actuators used by the  
362 intended functionality.
- 363 • The assumptions about how the intended functionality makes use of inputs from other elements.
- 364 • The assumptions about how other elements make use of outputs from the intended  
365 functionality.
- 366 • The concepts and technologies for the system and sub systems.
- 367 • The limitations and their countermeasures.
- 368 • The system architecture supporting the countermeasures.
- 369 • The degradation concept.
- 370 • The warning strategies.
- 371 • The dependencies on, and interaction with other functions and systems of the vehicle.

372 NOTE This specification and the ISO26262 item definition may contain common information.

### 373 **5.3 Consideration on system design and architecture**

374 The functional and system specification provides an adequate understanding of the system and its  
375 functionality so that the activities in subsequent phases can be performed. This includes a list of all  
376 performance limitations and their countermeasures. Some limitations and countermeasures are known  
377 and documented before the SOTIF related process begins while others are revealed as a result of the  
378 SOTIF activities.

379 Each iteration of the SOTIF related activity (Figure 9) can result in engineering activity and an update to  
380 this specification. Each iteration relies on this specification being up to date, such that it reflects all  
381 information discovered in previous iterations. Cooperation between all development parties (OEM,  
382 Tier1, TierN) is used to discover limitations and develop countermeasures during all development  
383 phases.

384 The functional and system specification lists performance limitations of every individual mechanisms,  
385 algorithms, or elements related to the safety of the intended functionality. The system is thus designed  
386 considering such limitations and ensuring that countermeasures are taken to mitigate their effect on the  
387 overall system if needed.

388 As the SOTIF activities identify new limitations and consequences (Clause 7), and define new mitigation  
389 measures (Clause 8), the functional and system specification is updated. This will ensure that all the  
390 required work is done both for closure of previous iterations, and at the beginning of the next iteration.

391 Specifically, the design includes considerations of system limitations that can result in erroneous  
392 subsystem output values being reported with high confidence (low confidence values might be ignored  
393 by design) and which can lead to potentially hazardous behaviour. Examples of limitations include  
394 incorrect classification, incorrect measurements, incorrect tracking, misdetection, ghosts, incorrect  
395 target selection, incorrect kinematic estimation, etc.

396 The final system architecture achieves robustness by considering every component, technology and  
397 system limitation. The system development is based on the assumption made about the limitations in  
398 design. Implementing measures to ensure SOTIF and integrating them into the functional and system  
399 specification, decreases the sizes of Area 2 and Area 3, and increases overall robustness by increasing  
400 the size of Area 1. Area 3 testing is used to uncover new issues only when the countermeasures, with  
401 respect to the original system design, are incomplete or not applicable to newly introduced use cases.

402 NOTE 1 Methods such as qualitative fault tree, HAZOP, FMEA, STPA and event tree analysis can be used to  
403 increase the confidence for the SOTIF.

404 NOTE 2 Performance limitations can be addressed by redundancy, diversity, functional restrictions or other  
405 measures.

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

412 EXAMPLE 2 An object detection algorithm detects a person on a skateboard as a pedestrian but rejects the  
413 object as due to its speed being implausible. A collision with the skateboarder is mitigated by a collision mitigation  
414 braking system which uses sensing and processing that is independent from that of the object detection algorithm.

415 EXAMPLE 3 An optical illusion drawing of a child running into the road is used to alert drivers in some areas.  
416 The image is drawn specifically to fool the human perception and can also fool a vision system into detecting a  
417 non-existent object. In this case, an optical flow-based analysis mechanism can prevent false braking. Optical flow  
418 analyses as well as radar-based environment recognition are alternative countermeasures for such cases, as well  
419 as other common detection cases such as ghosts that result from classification errors.



420

421 Figure 11: Example of optical illusion drawing that could fool a vision system.

422 EXAMPLE 4 Using an automated parking system with a big item protruding from the open trunk can lead to a  
423 hazardous event. A countermeasure in the system design can be to only permit automatic parking when the trunk  
424 is closed.

## 425 6 Identification and Evaluation of hazards caused by the intended functionality

### 426 6.1 Objectives

427 The potential hazards related to the SOTIF shall be systematically identified and evaluated such that:

- 428 – The possible hazardous events, caused by functionality that results in potentially hazardous  
429 behaviour and their potential consequences, are identified and evaluated.
- 430 – The acceptance criteria (e.g. a validation target) to evaluate the design in the validation phase  
431 are specified.

432 NOTE: Such acceptance criteria could be the minimum length of the required endurance run combined  
433 with a maximum number of observed failures for each type (e.g. false positives, false negatives).

- 434 – The possible hazardous events caused by reasonably foreseeable misuse of the function, by the  
435 user, are identified and evaluated.

### 436 6.2 Hazard identification

437 The hazards, caused by the unintended behaviour of the function, are determined systematically. This  
438 systematic identification is primarily based on knowledge about the function and its possible  
439 deviations. This can be achieved by applying the methods proposed in ISO 26262-3:2018 while  
440 considering performance limitations of the intended functionality. An illustration of the common

441 elements of the hazard analyse process required by both the ISO 26262 standard and by this clause can  
442 be found in Figure 12. Figure 13 uses an automated emergency braking (AEB) system as an example to  
443 show how the terms from Figure 12 are used.

444 EXAMPLE 1 For an AEB system, an incorrect detection can cause unintended full braking. However, the  
445 system can be designed to limit the allowable braking commanded by AEB. An incorrect detection of a lead vehicle  
446 can therefore only trigger braking up to this intended limit. Nevertheless, unwanted braking (due to incorrect  
447 detection) limited to the specified authority can have safety consequences. Such unwanted braking events are  
448 considered in the SOTIF related risk evaluation.

449 EXAMPLE 2 A system specified to implement an adaptive cruise control (ACC) function might exhibit  
450 undesirable behaviour if several vehicles are using ACC to drive one after another in a line. In such cases, high  
451 control loop latencies can lead to an “accordion effect” building-up, until the system is unable to brake hard  
452 enough and the driver has to intervene. Although this operational situation might be considered controllable by  
453 the driver, the need to avoid such build-up effects might still be analysed as part of the SOTIF.

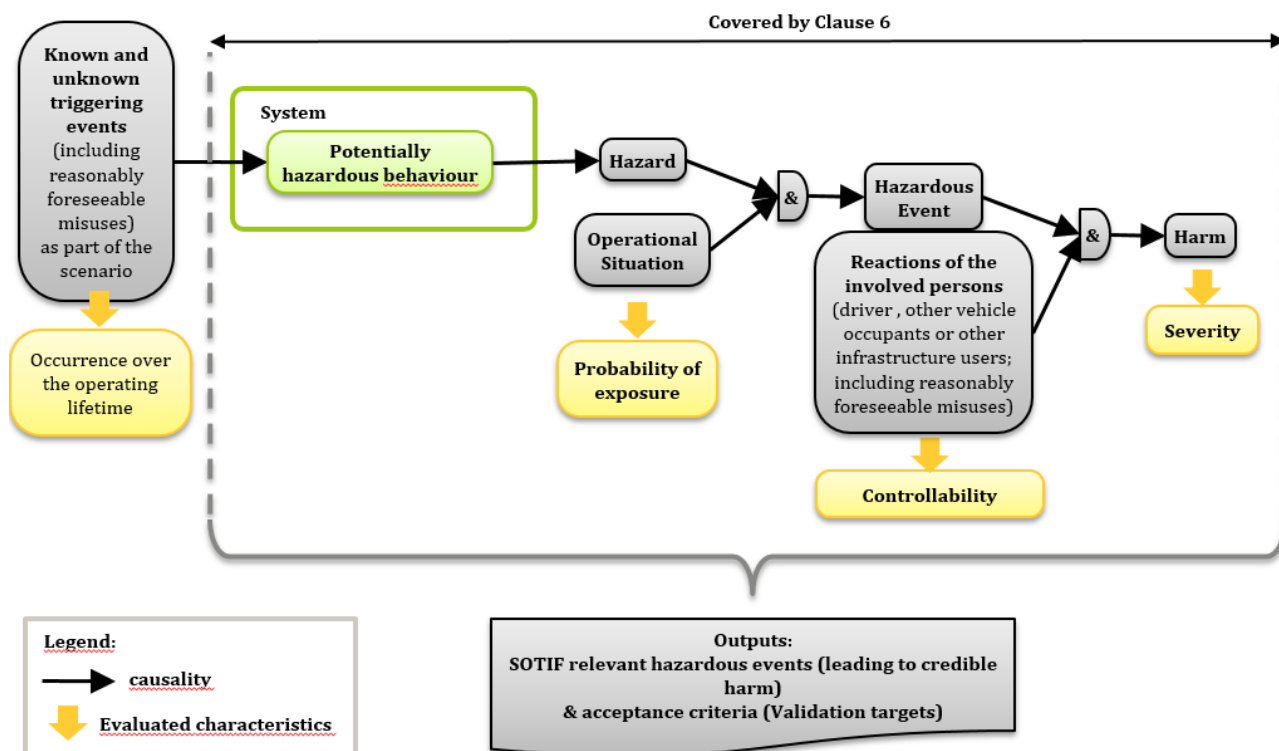


Figure 12: An illustration of common elements of hazard analysis in ISO 26262 and in this document

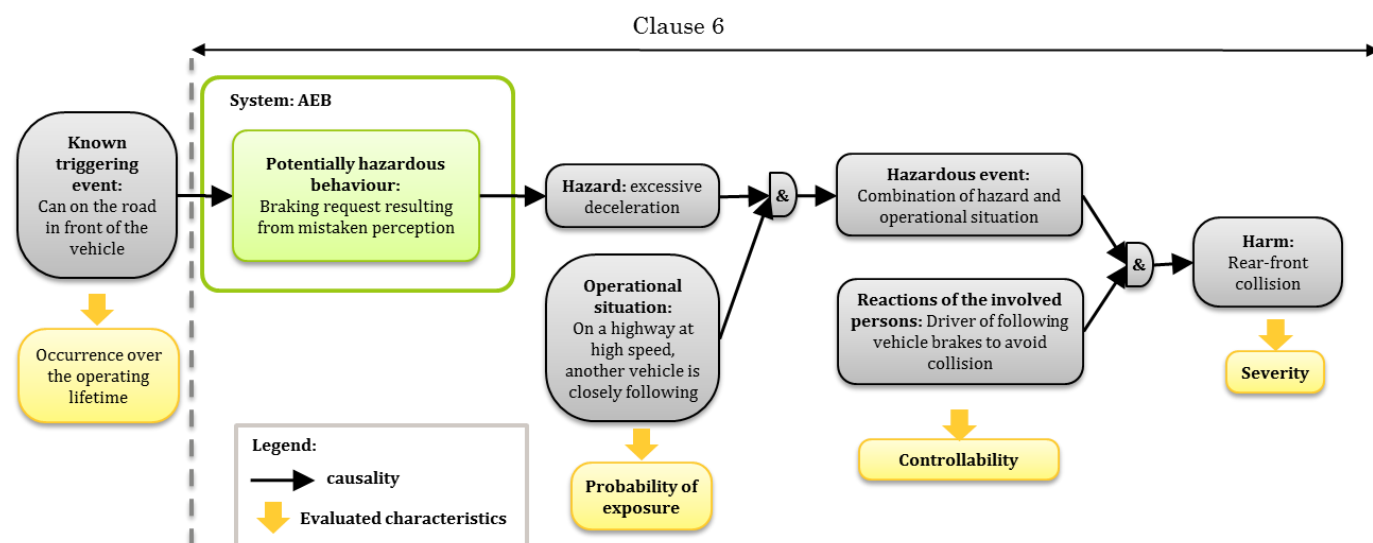


Figure 13: An AEB example using terms from Figure 12

NOTE Unlike ISO 26262, when analysing a SOTIF related hazard, no ASIL is determined for a hazardous event. However, the S, E and C parameters can be used to adjust the validation effort.

### 6.3 Hazard analysis

The harm and controllability of hazardous events can be estimated using the method described in ISO 26262-3:2018, Clause 6 but their evaluation for an individual hazardous event can be specific to a given SOTIF related hazard.

EXAMPLE 1 The severity of a rear collision, caused by emergency braking, can be reduced by limiting the brake intervention magnitude. The magnitude limit can be seen as a safety mechanism to increase controllability,



467 or as a modification to the intended behaviour. When analysing the hazard, the limit is considered part of the  
 468 intended behaviour; whereas functional failures relating to the implementation of the limit would be the subject of  
 469 other safety standards, such as ISO 26262.

470 The severity and controllability of the potentially hazardous behaviour, in a given scenario, are  
 471 considered to determine whether a credible harm can result. For hazardous event classification a  
 472 delayed or no reaction to control the hazard, from the involved persons, can be considered.

473 EXAMPLE 2 An environmental condition that is not supported by an ADAS that requires the driver to resume  
 474 control.

475 Delays due to the reaction time of the driver can impact the controllability evaluation and can be a topic  
 476 of the SOTIF related analysis.

477 EXAMPLE 3 Table 2 gives an example of the evaluation of a potential consequence for an AEB system and a  
 478 SOTIF related hazardous event.

479 **Table 2 Example of a hazardous event**

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

480

## 481 6.4 Risk evaluation of the intended function

482 The risk evaluation considers the performance limitations of the intended functionality to judge  
 483 whether controllability or severity is acceptable; that is controllability is “controllable in general” or  
 484 severity is “no resulting harm”. The severity and controllability evaluation can take into account the  
 485 expected system limitations and the measures that have been implemented to mitigate their effects  
 486 (according to the functional and system specification described in Clause 5).

## 487 6.5 Specification of a validation target

488 Validation targets take into account any applicable governmental and industry regulations as well as  
 489 the current level of functional performance needed to ensure safety. The specified validation targets  
 490 will depend on the methods chosen in the validation strategy.

491 EXAMPLE 1 Deductive analysis requires a list of all known and relevant triggering events to be considered.  
 492 For such analysis, a relevant validation target would ensure the coverage of all events on this list. In contrast, an  
 493 inductive analysis of SOTIF related hazards would involve a search for previously unknown triggering events that  
 494 are relevant to the application. In this case, validation targets would be defined with a statistical confidence that  
 495 the empirical data supports the hypothesis that triggering events do not impose unreasonable risk.

496 Approaches that can be considered when specifying these targets include:

- 497 – the available traffic data for the target market (e.g. accident statistics, traffic analyses) (see D.3  
 498 of Annex D) and
- 499 – pre-existing targets from similar functions operating in the field.



500 EXAMPLE 2 The pass/fail criteria for simulation testing, in a given situation, could be defined as: The  
501 allowable false positive and false negative rates for a function executing when not required, and, the allowable  
502 false positive and false negative rates for a function not executing when required.

503 If only a subset of scenarios is relevant to a specific hazard, then the exposure to the relevant scenarios  
504 (similar to the exposure in ISO 26262-3:2018, Clause 6) can be considered when determining the target  
505 value for this hazard and the associated validation duration.

506 When evaluating the likelihood that, in a given scenario, a triggering event will violate the quantitative  
507 target, the exposure, controllability and severity of the resulting behaviour are factors that can be taken  
508 into account. This can result in a reduction in the effort required to demonstrate the occurrence rate of  
509 the triggering event in Area 3, see Annex B of this document.

510 EXAMPLE 3 Consider the example from 6.3 where unintended braking only results in a rear crash if a trailing  
511 vehicle is present. The exposure rate to a trailing vehicle can be considered when specifying a validation target.

512 If applicable traffic statistics or field data are unavailable, then an appropriate target can be chosen  
513 provided a valid rationale is given.

514 NOTE 1 A rationale could be based on a risk tolerability principle, such as the French GAMAB or GAME; both have  
515 the meaning "globally at least as good". Following this principle, the residual risk (with respect to safety) of any  
516 new system is not significantly higher than those of existing systems having comparable functionality and hazards.  
517 The application of such a risk tolerability principle to the overall residual risk, that considers all hazards of the  
518 new system, allows relevant risk trade-offs to be made. For example, a system may be released even though the  
519 residual risk for a given hazard has increased, provided that this is compensated by counter balancing reductions  
520 in one or more other residual risks.

521 NOTE 2 A rationale could also be based on the ALARP (as low as reasonably practicable) principle. The ALARP  
522 Risk Management framework can provide a useful risk reduction principle, particularly with regard to the  
523 development and introduction of novel technologies where "good practice" does not currently exist. By  
524 acknowledging that a state of zero / no risk is not possible, the ALARP principle aims to reduce risk to a level  
525 considered "reasonably practicable" by weighing the risk against the sacrifice needed to further reduce it.

526 **7 Identification and Evaluation of triggering events**

527 **7.1 Objectives**

528 The triggering events:

529 – that can trigger potentially hazardous behaviour shall be identified;

530 – shall be evaluated for their acceptability with respect to the SOTIF.

531 NOTE Triggering event identification can be supported by a detailed environmental model.

532 **7.2 Analysis of triggering events**

533 A systematic method can be established to perform the analysis of triggering events. This  
534 method can consider knowledge gained from similar projects and field experience. The analysis  
535 aims to identify the system weaknesses (including those of its sensors, algorithms, actuators) and the  
536 related scenarios that could lead to an identified hazard.

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

538 • the known limitations of the system components to determine scenarios that could result in  
539 hazardous behaviour due to these limitations; and from

- the identified environment conditions and foreseeable misuses to determine the system limitations that could trigger potentially hazardous behaviour of the system. (Further detail is given in Annex E and Annex F).

These analyses will increase the understanding of the limitations of the systems and will improve the identification of unknown triggering events.

NOTE The analysis can be supported by inductive and/or deductive methods.

#### **7.2.1 Triggering events related to algorithms:**

An analysis of triggering events related to algorithms is used to determine:

- SOTIF risk mitigation methods and measures according to Clause 8.3;
- decision algorithm verification according to Clause 10.3; and
- validation of functionality according to Clause 11.

The analysis considers categories such as:

- environment and location;
- road infrastructure;
- urban infrastructure;
- highway infrastructure;
- driver behaviour (including reasonably foreseeable driver misuse);
- expected behaviour of other drivers/road users;
- driving scenario (e.g. a construction site, an accident, a traffic jam with emergency corridor, driving the wrong-way); and
- algorithm limitation, (e.g. capability to handle possible scenarios, or non-deterministic behaviour.).

NOTE The identified functional limitations are included in the list mentioned in Clause 5.

#### **7.2.2 Triggering events related to sensors and actuators:**

An analysis of triggering events related to sensor disturbances and actuator limitations is used to determine:

- SOTIF risk improvement methods and measures according to Clause 8.3;
- sensor verification strategy according to Clause 10.2;
- actuator verification strategy according to Clause 10.4; and
- validation of functionality according to Clause 11.

The analysis considers categories that can cause triggering events such as:

- 571       – weather conditions;
- 572       – mechanical disturbance (including installation, design location, transmission of signals);
- 573       – EMI interference;
- 574       – interference from other vehicles or other sources (e.g. radar or lidar);
- 575       – acoustic disturbance;
- 576       – glare
- 577       – poor-quality reflection;
- 578       – accuracy;
- 579       – range;
- 580       – response time;
- 581       – durability; and
- 582       – authority capability (applicable to actuators).

583   EXAMPLE 1       Rain and snow can affect radar performance.

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

585   EXAMPLE 3       A heavy woollen coat can affect the performance of ultrasonic sensors.

586   EXAMPLE 4       An improper alignment can affect many sensor types.

587   NOTE 1           The considered sensors can include inertial sensors, cameras, radar etc.

588   NOTE 2           A potential scenario can be a scenario resulting from a theoretical combination of already  
589   observed scenarios.

590   NOTE 3           For specific analysis categories see Annexes D, E and F. For each category, a list of detailed  
591   disturbances is determined based on knowledge and experience (including knowledge gained on similar projects  
592   and in field experience).

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

### 595   **7.3 Acceptability of the triggering events**

596   The identified triggering events are evaluated considering the acceptance criteria that are specified  
597   during the SOTIF risk identification and evaluation (as described in Clause 6).

598   The response of the system to these triggering events can be considered as acceptable with respect to  
599   the SOTIF without need of further functional improvement (as described in Clause 8) if:

- 600       • The probability of the system causing a hazardous event is lower than the validation  
601       target value specified in Clause 6.5; and
- 602       • There is no systematically unacceptable scenario in relation to a specific vehicle that has  
603       the potential to lead to a hazardous event.

NOTE Even if a fleet has a very low probability of a triggering event, it can be unacceptable if for a specific systematic vehicle behaviour, the probability is high.  
EXAMPLE A particular structure that always causes the AEB system to brake excessively.

## 8 Functional modifications to reduce SOTIF related risks

### 8.1 Objectives

The development activities of the functional modifications to reduce the SOTIF related risks shall achieve the following objectives:

- identification and allocation of measures to avoid, reduce, or mitigate the SOTIF related risks;
- estimation of the effect of the SOTIF related measures on the intended function; and
- improvement of the information required by Clause 5 (Functional and system specification).

### 8.2 General

This clause deals with identification of measures to avoid, reduce, or mitigate the SOTIF related risks. The function and system descriptions are developed through several iterations and each time the Functional and System specification (required by Clause 5) is updated with information about the identified measures.

A functional modification to reduce SOTIF related risks may be needed when the identified triggering events:

- a) have the possibility to trigger a potentially hazardous behaviour leading to a hazardous event with credible harm (according to Clause 6); and
- b) cannot be evaluated as acceptable with respect to the safety of the intended functionality (according to Clause 7).

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

- a) information on the system architectural design;
- b) the functionality which is defined and described in accordance with Clause 5;
- c) the evaluation of the potential outcome of possible hazardous events in accordance with Clause 6;
- d) the possible scenarios that can trigger an unintended system behaviour leading to a hazardous event in accordance with Clause 7;
- e) knowledge derived from previous verification results, where the system and components did not behave as expected for specific use cases during verification in accordance with Clause 10 (if any); and
- f) knowledge derived from previous validation results including real-life use cases, where the function did not behave as expected and the system and component limitations cause an unreasonable level of risk in accordance with Clause 11 (if any).

### 8.3 Measures to improve the SOTIF

Measures to improve the SOTIF address the identified system limitations (in accordance with Clause 7.2) that lead to a safety violation. Depending on the evaluated SOTIF related risks, the measures to improve the SOTIF can be aimed at avoidance, reduction, or mitigation.

The improvement measures can include:

- 643 a) System improvement to avoid or reduce the SOTIF related risks, including but not limited to:
- 644 1) Increased sensor performance and/or accuracy by:
- 645 – sensor algorithm improvement
- 646 – adequate sensor technology
- 647 – sensor location modification
- 648 – sensor disturbance detection that triggers an appropriate warning and degradation
- 649 strategy
- 650 – recognition of exiting the operational design domain [3], i.e. recognition of a known
- 651 unsupported environmental condition that requires a transition to an appropriate
- 652 sensor usage strategy
- 653 – diverse sensor technology
- 654 2) Increased actuator performance and/or accuracy by:
- 655 – adequate actuator technology (e.g. increase accuracy, extend range of output,
- 656 shorter response times, improve durability, arbitrate authority capability)
- 657 3) Increased performance of the recognition and decision algorithms by:
- 658 – algorithmic improvements
- 659 – recognition of exiting the operational design domain [3] i.e. recognition of a known
- 660 unsupported environmental condition that requires a transition to an appropriate
- 661 warning and degradation strategy
- 662 – design strategy that incorporates the triggering of an appropriate warning and
- 663 degradation strategy for a known unsupported SOTIF use case.
- 664 EXAMPLE lane keeping.
- 665 – strategy for mitigation and resolution of functional interference/conflict (avoidance
- 666 of unintended behaviour due to inter-system dead lock/ live lock)
- 667 EXAMPLE conflict between lane keeping and automatic lane change.
- 668 4) Improved testability by:
- 669 – allowing verification of system and component behaviour
- 670 b) Functional restriction made to the intended function to reduce, or mitigate the SOTIF related
- 671 risks, including but not limited to:
- 672 1) Restriction of the intended function for specific SOTIF use cases
- 673 EXAMPLE lane keeping assist functionality is reduced to avoid an undesired steering intervention
- 674 when lane detection devices cannot clearly detect the lane
- 675 2) Restriction of authority for the intended function for specific use cases
- 676 EXAMPLE camera blinded by a reflection of surrounding light caused by the afternoon sun,
- 677 operation continues with restricted authority using radar and other sensors
- 678 3) Restriction of overall authority for the intended function for specific use cases.
- 679 EXAMPLE all perception sensors blinded by a snow storm, driver requested to take over control
- 680 c) Handing over the authority from a system to the driver to improve the controllability (the
- 681 transition itself being controllable and not representing additional risk to the driver) of the
- 682 critical operational situation's effect, including but not limited to:

- 683 1) Improving the Human-Machine Interface  
 684 2) Improving the warning and degradation strategy  
 685 3) Taking guidance from other sources  
 686 EXAMPLE RESPONSE3 [4]  
 687 d) Reduction or mitigation of reasonably foreseeable misuse effects, including but not limited  
 688 to:  
 689 1) Improving the information provided to the driver about the intended functionality  
 690 EXAMPLE user manual  
 691 2) Improving the Human-Machine Interface  
 692 3) Implementation of a monitoring and warning system  
 693 EXAMPLE driver warning when the steering wheel is released.

694 EXAMPLE Table 3 gives an example derivation of SOTIF related measures.

695 **Table 3: Example of derived SOTIF related measures**

	Causal factor of hazard with example	Example of derived SOTIF measure
E/E System Factor	Exceeding E/E System performance limitation	<ul style="list-style-type: none"> <li>• Reduce the performance of the system and inform the driver of the reduced or disabled functionality and hand over the authority to the driver.</li> <li>• Gently terminate the function</li> <li>• Degrade and keep the function</li> </ul>
Driver Factor	Reasonably foreseeable misuse	<ul style="list-style-type: none"> <li>• Provide measures against inadvertent or careless operation by the driver.</li> <li>• Inform driver about correct operation.</li> <li>• Monitor and warn the driver when an incorrect operation is detected.</li> </ul>

696

## 697 8.4 Updating the system specification

698 The following information is identified in order to update the functional and system specification:

- 699 – measures of system improvements to avoid, reduce, or mitigate the SOTIF related risks;  
 700 – measures of functional restrictions to reduce or mitigate critical operational situation effects;  
 701 – measures of improvement of the Human-Machine Interface and warning and degradation  
 702 strategy; and  
 703 – measures resulting from the handling of reasonably foreseeable misuses.

## 704 9 Definition of the Verification and Validation strategy

### 705 9.1 Objectives

706 A verification and validation strategy shall be defined such that:

- 707 – It supports the rationale for the SOTIF;
  - 708 – The necessary evidence (e.g. analysis results, test reports, dedicated investigations) is  
709 generated; and
  - 710 – The procedures to generate the evidence are developed.
- 711 The system verification and validation activities with regard to the risk of potentially hazardous  
712 behaviour (excluding the faults addressed by ISO 26262) include integration testing activities to  
713 address the following scope:
- 714 – The ability of sensors and the sensor processing algorithms to model the environment;
  - 715 – The ability of the decision algorithms to handle both known and unknown situations and to  
716 make the appropriate decisions according to the environment model and the system  
717 architecture;
  - 718 – The robustness of the system or function;
  - 719 – The ability of the HMI to prevent reasonably foreseeable misuse; and
  - 720 – The manageability of the handover scenario by the driver.
- 721 To support the achievement of the objectives of this clause, the following information can be  
722 considered:
- 723 – Functional concept, including sensors, actuators and algorithm specifications;
  - 724 – System design specification;
  - 725 – Verification and validation targets;
  - 726 – Vehicle architecture;
  - 727 – Analysis of triggering events results as described in Clause 7.2;
  - 728 – System design;
  - 729 – System integration & testing plan;
  - 730 – Lessons learned.

## 731 **9.2 Planning and specification of integration and testing**

732 A verification and validation strategy is defined to provide evidence that the objectives are achieved and  
733 to state how the targets are to be met. The verification and validation strategy can cover both E/E  
734 elements and elements of other technologies considered relevant to the achievement of the SOTIF.

735 Verification and validation activities consider calibration and configuration data to achieve the SOTIF.

736 NOTE 1 Variability of the triggering event parameters is considered by evaluating the verification and  
737 validation strategy. See Annex D for further practices for the verification and validation of automotive perception  
738 systems.

739 NOTE 2 As functional improvements are made, the system is analysed to determine if additional functions are  
740 retested during verification and validation. These dependent functions are verified with regression tests. This  
741 ensures that known or new triggering events do not cause potentially hazardous behaviour in unchanged  
742 functions. Triggering events found during verification and validation activities, where potentially hazardous  
743 behaviour is present, are retested on every release. With a proper rationale, the testing scope can be reduced. To

744 ensure that correct functional behaviour is maintained, complete testing is documented for any release intended  
 745 for production. This includes documentation of parts that have not been affected and retesting of parts that have  
 746 been affected by changes.

747 Methods to specify the verification and validation activities (e.g. integration test cases, analysis) can be  
 748 derived using an appropriate combination of methods, and by considering the integration level, as  
 749 illustrated by Table 4.

**Table 4: Methods for deriving verification and validation activities**

Methods	
A	Analysis of requirements
B	Analysis of external and internal interfaces
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, sequences, and sources of dependent failures
H	Analysis of environmental conditions and operational use cases <sup>a)</sup>
I	Analysis of field experience and lessons learned <sup>b)</sup>
J	Analysis of system architecture (including redundancies)
K	Analysis of sensors design and their known potential limitations
L	Analysis of algorithms and their decision paths
M	Analysis of system ageing
N	Analysis of triggering events
	<sup>a)</sup> including known sources of potentially hazardous behaviour of the element or system <sup>b)</sup> this considers various driving conditions, driving styles, driving environment and end customer claims NOTE Annex G discusses verification and validation activities for off-line training such as used for machine learning.

751

## 752 10 Verification of the SOTIF (Area 2)

### 753 10.1 Objectives

754 The system and components (sensors, algorithms and actuators) shall be verified to show that they  
 755 behave as expected for known hazardous scenarios and reasonably foreseeable misuse (derived from  
 756 previous analyses and knowledge). It shall be verified that system and components are covered  
 757 sufficiently by the tests (see Area 2 of Figure 9).

758 To support the achievement of the objectives of this clause, the following information can be  
 759 considered:

- 760 – Verification strategy, as defined in Clause 9;
- 761 – Functional concept, including sensors, actuators and algorithm specification;





779

**Table 6: Decision Algorithm verification**

Methods	
A	Verification of robustness 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. classification, sensor data fusion, situation analysis, function)
C	Verification of the architectural properties including independence, if applicable
D	In the loop testing (e.g. SIL / HIL / MIL) on selected SOTIF relevant use cases and scenarios
E	Vehicle level testing on selected SOTIF relevant use cases and scenarios
F	Inject inputs into the system that trigger potentially hazardous behaviour
	NOTE For test case derivation the method of combinatorial testing can be used [5]

780

781 **10.4 Actuation verification**

782 Methods to verify the actuators for their intended use and for their reasonably foreseeable misuse in  
783 the decision algorithm can be applied as illustrated by Table 7.

784

**Table 7: Actuation verification**

785

Methods	
A	Requirements-based test (e.g. precision, resolution, timing constraints, bandwidth)
B	Verification of actuator characteristics, when integrated within the vehicle environment
C	Actuator test under different environmental conditions (e.g. cold conditions, damp conditions)
D	Actuator test between different preload conditions (e.g. change from medium to maximum load)
E	Verification of actuator ageing effects (e.g. accelerated life testing)
F	In the loop testing (e.g. SIL / HIL / MIL) on selected SOTIF relevant use cases and scenarios
G	Vehicle level testing on selected SOTIF relevant use cases and scenarios

786

787 **10.5 Integrated system verification**

788 Methods to verify the robustness and the controllability of the system integrated into the vehicle can be  
789 applied as illustrated by **Fehler! Verweisquelle konnte nicht gefunden werden.8.**

Table 8: Integrated system verification

Methods	
A	Verification of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing)
B	Requirement-based Test when integrated within the vehicle environment (e.g. range, precision, resolution, timing constraints, bandwidth)
C	In the loop testing (e.g. SIL / HIL / MIL) on selected SOTIF relevant use cases and scenarios
D	System test under different environmental conditions (e.g. cold, damp, light, visibility conditions)
E	Verification of system ageing affects. (e.g. accelerated life testing)
F	Randomized input tests <sup>a)</sup>
G	Vehicle level testing on selected SOTIF relevant use cases and scenarios
H	Controllability tests (including reasonably foreseeable misuse)
<sup>a)</sup> Randomized input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images or altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns.	

Annex D provides examples for the verification of perception systems.

11 Validation of the SOTIF (Area 3)

11.1 Objectives

The functions of the system and the components (sensors, decision-algorithms and actuators) shall be validated to show that they do not cause an unreasonable level of risk in real-life use cases (see Area 3 of Figure 9). This requires evidence that the validation targets are met.

To support the achievement of this objective the following information can be considered:

- Validation strategy, as defined in Clause 9;
- Verification results in defined use cases, as defined in Clause 10;
- Functional concept, including sensors, actuators and decision-algorithm specification;
- System design specification;
- Validation targets, as defined in Clause 6;
- Vehicle design (e.g. sensor mounting position); and
- Analysis of triggering events results as described in Clause 7.2.

11.2 Evaluation of residual risk

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 Fehler! Verweisquelle konnte nicht gefunden werden.9.

Table 9: Evaluation of residual risk

Methods	
A	Validation of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing)
B	Verification of the architectural properties including independence, if applicable
C	In the loop testing on randomized test cases (derived from a technical analysis and by error guessing)
D	Randomized input tests <sup>a)</sup>
E	Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)
F	Long term vehicle test
G	Fleet tests
H	Test derived from field experience
I	Tests of corner cases <sup>b)</sup> and reasonably foreseeable misuse
J	Comparison with existing systems
K	Simulation of selected scenarios
L	Analysis of worst case scenarios
<sup>a)</sup> Randomised input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images, altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns. <sup>b)</sup> A corner case is a rare or unusual condition	

810

811 **11.3 Validation test parameters**

812 For each of the applied methods described in **Fehler! Verweisquelle konnte nicht gefunden werden**.9, an appropriate cumulated test length is selected. A rationale for the test length selected is  
813 provided and correlated with the number and distribution of scenarios. Generally, for all selected test  
814 methods a rationale is provided establishing that the resulting distribution of system inputs is  
815 representative of either the general operational environment or the specific use case, scene or scenario.  
816 Vehicle test length determination (long term tests, fleet tests) can take into account knowledge from  
817 prior vehicle programmes, driver controllability, or the criticality of selected test routes. In the case of  
818 the use of randomised input tests, the number of scenarios being simulated in which erroneous  
819 patterns are injected can be correlated with the test length and test content that is representative of the  
820 target market.  
821

822 Annexes B, C and D provide examples for the validation of SOTIF relevant systems.

823 **EXAMPLE** When evaluating an image recognition algorithm using simulation, a cumulated test length of  
824 X hours is selected, with Y different scenarios. The distribution of scenarios is adjusted according to the  
825 challenging scenarios and the distribution of driving use cases from traffic data. The susceptibility of the algorithm  
826 to real-life triggers is identified by analysis of the algorithm and its decision paths. Scenarios with the most  
827 sensitive algorithm characteristics are included with a distribution emphasizing the challenging scenarios and  
828 representing their statistical relevance. The probabilities of occurrence of the influencing parameters in real-life  
829 use cases can also be considered to determine the appropriate test length.

## 830 12 Methodology and criteria for SOTIF release

### 831 12.1 Objectives

832 A SOTIF release shall be performed to:

- 833 – review the SOTIF activities and
- 834 – evaluate the acceptability of the residual risk considering the findings of the SOTIF activities.

835 To support the achievement of the objectives of this clause, the following information is considered:

- 836 – functional and system specification as defined in Clause 5;
- 837 – verification and validation targets as defined in Clause 6;
- 838 – analysis of triggering events as defined in Clause 7;
- 839 – functional improvements as the result of Clause 8 activities;
- 840 – verification and validation strategy, as defined in Clause 9;
- 841 – results of verification as defined in Clause 10; and
- 842 – results of the validation of the SOTIF as defined in Clause 11

### 843 12.2 Methodology for evaluating SOTIF for release

844 The prerequisite information is reviewed taking the following into account:

- 845 1. Did the validation strategy take into account all the specified use cases within the scope of the  
846 intended functions?
  - 847 a) Did the testing cover identified triggering events?  
848 EXAMPLE narrow metallic structures for the radars falsely triggering braking.
  - 849 b) Was it tailored for differences from previous validations?
- 850 2. Does the intended functionality achieve a minimum fall-back risk condition[3], when necessary,  
851 providing a state without unreasonable risk to the occupants or other road users:
  - 852 a) Using only the specified driver intervention;
  - 853 b) Taking into account reasonably foreseeable misuse; and
  - 854 c) Warning to the vehicle occupants and/ or the other road users of the malfunctioning  
855 vehicle.
- 856 3. Was sufficient verification and validation completed and acceptance criteria met, to have  
857 confidence that the risk is not unreasonable?
  - 858 a) Has the intended function been exercised sufficiently to evaluate both nominal  
859 behaviour and potential unwanted behaviour?
  - 860 b) Was no unintended behaviour observed with the possibility to lead to a hazardous  
861 event?
- 862 4. In case of an unintended behaviour with the possibility to lead to a hazardous event, was  
863 evidence provided to argue the absence of unreasonable risk?

864 EXAMPLE See Annexes B, C and D.

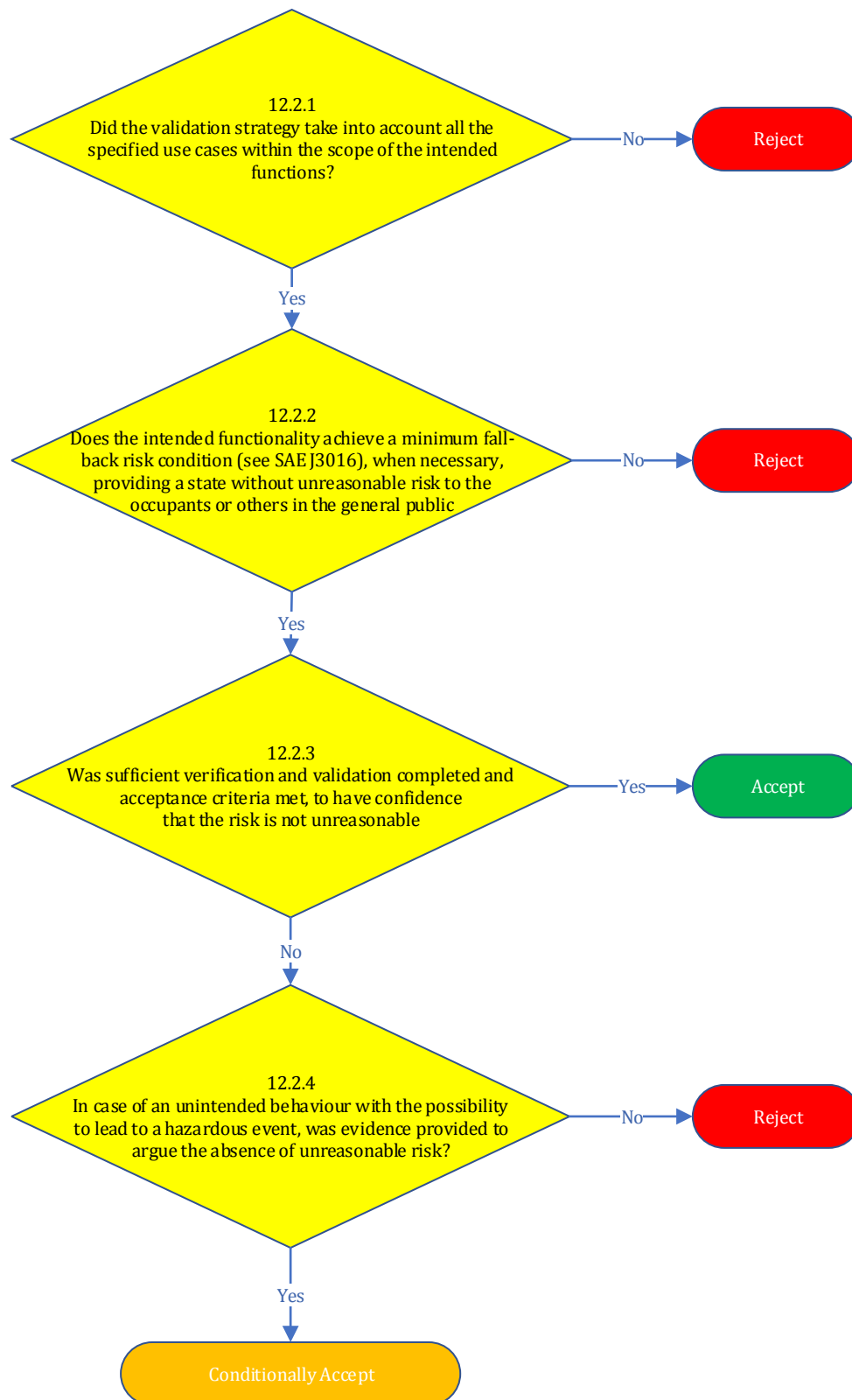
865 NOTE The examination of the results of the SOTIF activities can be considered in the ISO26262 functional  
866 safety assessment.

867 **12.3 Criteria for SOTIF release**


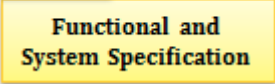
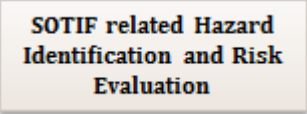

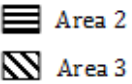


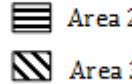
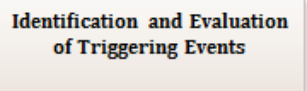
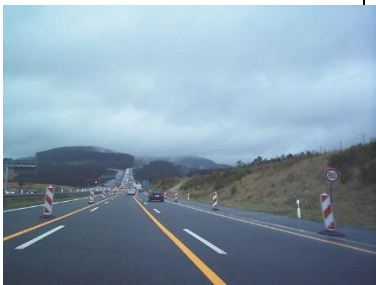

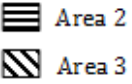


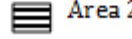
868 Based on evidence of the methodology from 12.2.3 above, a recommendation of “acceptance”,  
869 “conditional acceptance”, or “rejection” for release may be determined using the following criteria:

- 870 a) For “acceptance”, points 1, 2, and 3 of chapter 12.2 are satisfied.  
871 b) For “conditional acceptance”, points 1, 2, and 4 of chapter 12.2 are satisfied. The condition is  
872 satisfied when the risk is shown not to be unreasonable by the specified date.  
873 c) Neither 12.3a nor 12.3b are satisfied, the SOTIF release status is “rejection”.



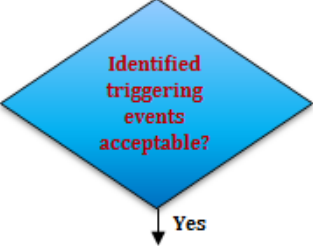



874 See Figure 14 for a flowchart of the SOTIF release decision logic.

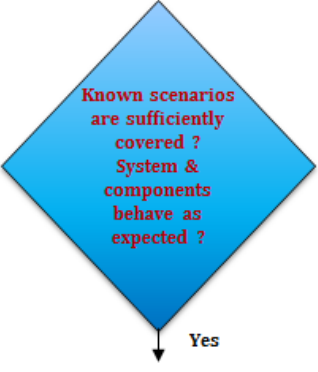

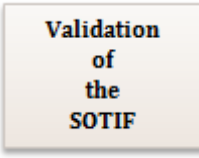



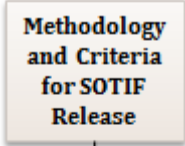




**Figure 14: Evaluation of Criteria for SOTIF release**

Elements of flow diagram	Example 1: Lane Keeping Support (LKS)	Example 2: Automatic Emergency Braking (AEB)	Area of SOTIF diagram
 	<p>This function uses a video camera to detect the lane markings ahead of the vehicle. If it detects that the vehicle is getting too close to the side of its lane, Lane Keeping Support (LKS) will take action by applying a corresponding steering torque.</p>	<p>This function uses a radar sensor to scan the distance to the obstacle (e.g. vehicle) in front. If it detects an imminent collision, Automatic Emergency Braking (AEB) will be triggered.</p>	NA
	<p>Traffic situation: driving on the highway with LKS active. The driver might rely on the function and drive hands-off.</p> <p>Potential hazard: Unwanted steering activation could lead to a collision with oncoming traffic or with other obstacles.</p>	<p>Traffic situation: driving on roads with heavy traffic (e.g. suburban road).</p> <p>Potential hazard: Unwanted emergency braking could lead to a rear end collision with the following vehicle.</p>	 
	<p>No control of the hazard because the driver might rely on the function and be driving hands-off and be unable to take over in time.</p>	<p>No control of the hazard by the driver. Control of hazard by the following driver depends on the distance between the two vehicles.</p>	 
	<p>Crossing lane marking (e.g. before construction zone) [6]</p> 	<p>Special road conditions (e.g. manhole cover, tunnels, beverage can) can give a radar echo, which could be interpreted as a potential obstacle.</p>	 
	<p>“No”: the SOTIF related risk is not accepted. The controllability of the function by the driver must be ensured.</p>	<p>The severity of the rear end collision caused by unwanted emergency braking must be reduced.</p>	 



<b>Functional Modification to reduce SOTIF risk</b>	<p>Functional improvement: Implemented detection of driver not holding steering wheel.</p>	<p>Limit the duration and/or strength of the braking intervention.</p>	
<b>Functional and System Specification</b>	<p>This function uses a video camera to detect the lane markings ahead of the vehicle. If it detects that the vehicle is getting too close to the side of its lane, LKS will take action.</p> <p><i>Additional specification: Driver warning in case of hands-off, detected based on capacitive sensing, to ensure hands-on driving maintained.</i></p>	<p>This function uses a radar sensor in order to scan the distance to the vehicle in the front. If it detects an imminent collision, Automatic Emergency Braking (AEB) will be triggered.</p> <p><i>Additional specification: Limitation of the braking intervention to minimise or prevent damage in case of unwanted emergency braking.</i></p>	
	<p>“Yes”: the SOTIF related risk is accepted. No further improvements.</p>	<p>No further improvements.</p>	
<b>Definition of the Verification and Validation strategy</b>	<p>Definition of test cases for evaluating the LKS function in known and unknown unsafe scenarios based on Clause 9, Table 4.</p>	<p>Definition of test cases for evaluating the AEB function in known and unknown unsafe scenarios based on Clause 9, Table 4.</p>	
<b>Verification of the SOTIF</b>	<p>Verification of hands-off detection at system integration level, based on Clause 10, Table 8 (e.g. capacitive-measurement on HIL, robustness tests)</p> <p>Additionally, studies with test persons e.g. using a driving simulator</p>	<p>Known scenarios which could lead to unwanted emergency braking (e.g. manhole, beverage can) are considered in each new project and verified on a test track and/or in simulation and/or during an endurance run.</p> <p>Result: All known scenarios are removed except the detection and reaction to a moving beverage can.</p>	

	<p>“Yes”. Increasing driver awareness due to the warnings resulting from hands-off detection. Evidence of sufficient controllability by studies with test persons.</p>	<p>Assumption that the probability of the occurrence of a moving beverage can in front of the vehicle is very low and so acceptable.</p>	
	<p>Long-term endurance run based on a knowledge-based driving catalogue to prove controllability in further (unknown) scenarios.</p> <p>Result from endurance run: false hands-on detection only possible with intentional steering wheel alterations. This is considered as abuse.</p>	<p>Vehicle level testing on selected test cases (derived from technical analysis and error guessing).</p> <p>Endurance run for the function that is representative of the target market and that obtains statistical evidence about remaining unknown scenarios</p>	
	<p>“Yes”. Target level for endurance run complies with the state of the art and GAMAB principle (description of GAMAB see Clause 6.5)</p>	<p>Target level for endurance run complies with the state of the art and GAMAB principle (description of GAMAB see Clause 6.5).</p> <p>Reduction in the amount of endurance runs possible by using experience and results from preceding projects. Justification of the reusability of test evidence is necessary.</p>	
 	<p>“Yes”. Verification of hands-off detection done by testing. No further unknown unsafe scenarios identified during endurance run.</p> <p>Residual risk acceptable.</p>	<p>Achievement of the verification and validation target values is demonstrated.</p> <p>Residual risk acceptable.</p>	

## 879 **Annex B (Informative): Example for definition and validation of an acceptable** 880 **false alarm rate in AEB systems**

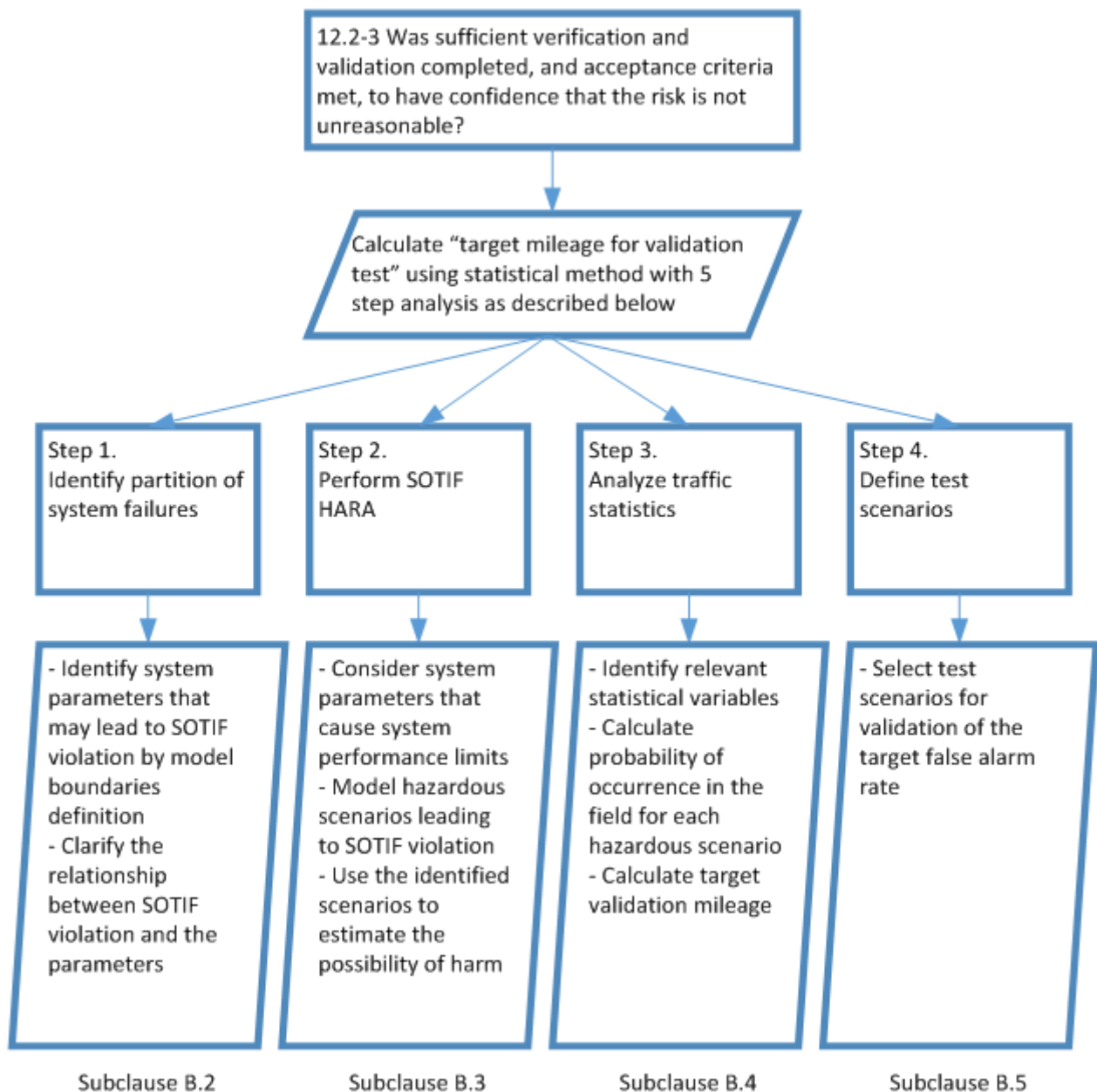
### 881 **B.1 Objective and Structure of this Annex**

882 The objective of this Annex is to show an example of evaluating SOTIF for release (see Clauses 12.2 and  
883 12.3). This example demonstrates a method for the validation of an Automatic Emergency Braking  
884 system (AEB) based on published traffic accident statistics. Test driving was chosen as the validation  
885 method. The target mileage was calculated using statistical methods and a 4-step analysis. The steps are  
886 described in the individual sub-clauses of this Annex (see also Fig. B.1). The list of steps is given below  
887 and for each step its partial objective is formulated:

- 888 1. Partition of system failures  
889     ○ For the target system, identify parameters that can lead to a hazardous event caused by  
890         suboptimal model boundary definitions  
891     ○ Clarify the relationship between the SOTIF hazardous event and the combination of these  
892         parameters
- 893 2. Modelling of hazardous events  
894     ○ Consider representative parameters that cause system performance limitations  
895     ○ Model the scenarios of hazardous events  
896     ○ Use the derived scenarios to assess the influence of the selected parameters on the  
897         probability of harm
- 898 3. Analysis of traffic statistics  
899     ○ Identify statistical variables relevant to the scenarios derived on the previous step  
900     ○ Calculate the probability of occurrence for each hazardous scenario  
901     ○ Calculate target validation mileage using statistical simulation based on the models of  
902         hazardous scenarios
- 903 4. Define test scenarios  
904     ○ Select target validation test scenarios according to the mission profile that relate to the false  
905         alarm rate

906 NOTE 1 This Annex is related to Area 3 “Unknown unsafe scenarios” (see Figure 7). Actions to reduce the risk in  
907 Area 2 “Known unsafe scenarios” (Clause 7) and to complete the verification of the SOTIF (Clause 10) are assumed  
908 to be executed prior to production vehicle deployment and are not covered by this Annex.

909 NOTE 2 This Annex is based on the presentation [7]



**Figure B.1. Overview of Annex B**

## **B.2 Partition of system failures**

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 identification of the driving scenario might activate emergency braking bringing the vehicle to a complete stop when not needed.

Some ADAS algorithms (e.g. Bayesian estimators, neural networks) for object recognition are affected by failures caused by performance limitations – a group of failures different to those defined within ISO 26262:2018.

920 In the case of AEB systems as well as other ADAS functions, the causes of hazardous events can be  
921 classified in three categories:

- 922 1. Hardware failures (both random and systematic) responsible for safety goal violation can be  
923 controlled by the application of ISO 26262-5
- 924 2. Systematic software failures responsible for safety goal violation can be controlled by the  
925 application of ISO 26262-6
- 926 3. Unintended behaviour due to performance limitations

927 Unintended behaviour due to performance limitations can contribute to safety violations. The scenarios  
928 of those violations can be identified in the ISO 26262 HARA (e.g. crash due to an as unintended AEB  
929 actuation). The safety analyses according to ISO 26262, however, tend to focus on design failures  
930 (points 1 and 2 from the list above). ISO/PAS 21448 can consider other sources of hazards such as  
931 reasonably foreseeable misuse as a triggering event for the potentially hazardous behaviour of the  
932 system.

933 The AEB system behaviour can be modelled at a very high level through three parameters:

- 934 ○ Probability of existence,  $P_E$ : how confident we are that an object is in front of us
- 935 ○ Probability of collision,  $P_C$ : how likely it is that we are going to collide with the object in front
- 936 ○ Time to collide,  $TTC$ : time left before collision

937 The system commands AEB activation when the conjunction of the following conditions holds:  
938 probability of existence exceeds a given threshold, probability of collision exceeds a given threshold,  
939 AND time to collide ( $TTC$ ) is below a certain threshold ( $\overline{TTC}$ ). Mathematically, this can be written in the  
940 following way:

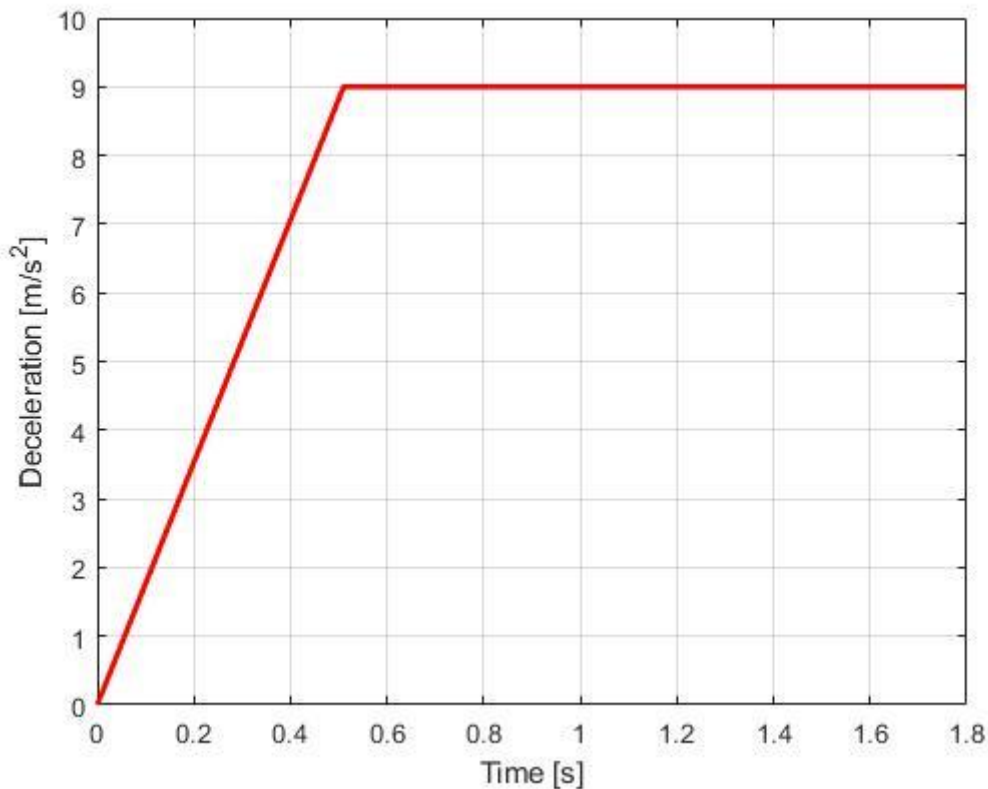
$$\begin{cases} TTC < \overline{TTC} \\ P_C > \overline{P_C} \\ P_E > \overline{P_E} \end{cases} \Rightarrow AEB \text{ activation}$$

941 The relationship between a safety violation and the combination of these parameters is not linear.  
942 Besides the parameters listed in the system above, it can depend on multiple external factors.

### 943 **B.3 Modelling of the hazardous event**

944 Considering a system able to perform AEB with the deceleration profile shown in Figure B.2 and within  
945 the following performance limitations:

- 946 – AEB system commands braking with maximum negative acceleration of 0.9 g in response to a  
947 moving object
- 948 – Brake rise time is subject to a brake system pre-fill and limited to 15 m/s<sup>3</sup>
- 949 – AEB feature is available between 5 and 80 km/h
- 950 – A maximum speed reduction of 50 km/h is allowed
- 951 – Safety mechanisms in the sensor and the braking systems will prevent AEB commanding  
952 deceleration outside the designated speed range



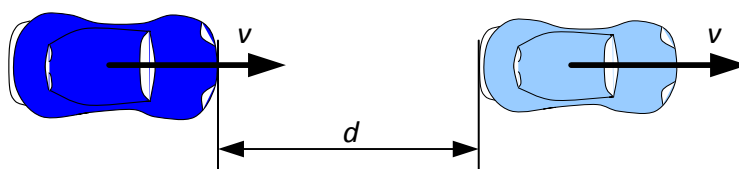
**Figure B.2. Deceleration profile for AEB.**

The Safety Goal and relevant hazardous scenario were identified in the HARA performed according to ISO 26262.

**Safety Goal:** Unintended AEB braking within design intent for longer than 340 ms is to be avoided

**Hazardous scenario:** AEB event lasting longer than 340 ms at a time when an attentive driver would not perceive the need of an AEB actuation.

Possible SOTIF-relevant causes for the realization of the hazardous scenario include a rear-end crash after the AEB is activated by an algorithm error caused by a suboptimal model boundary definition. The Hazard of unintended deceleration can be modelled as a straight road car-following scenario for first order effects (see Figure B.3) [8].



**Figure B.3. Car-following scenario used in the hazardous event model**

The scenario is based on the following assumptions:

- Both cars are travelling at the same speed  $v$
- The headway  $d$  has known probability distribution.
- 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 B.2.

- The following driver perceives the hazardous situation and reacts by braking. The reaction time has a known probability distribution.

The Monte Carlo simulation based on the defined distance between cars in traffic and response time distributions was used to identify the outcome of various brake events. Some of them can result in a collision. The outcome largely depends on the speed of the vehicles when the unintended AEB activation occurs.

The simulation model delivers the percentage of unintended AEB activation cases that result in a collision. The simulation takes the start speed  $v$  and interval of differential speed at collision  $\delta v$  as inputs, while the percentage of the simulations that result in a collision where start speed was of  $v$  and speed difference at the time of collision falls into  $\delta v$  is considered as the output. The dependency produced by the model is formally described by the equation (B.1):

$$P_{collision} = P(v, \delta v) \quad (B.1)$$

## B.4 Analysis of traffic statistics

According to ISO 26262-1:2018, a HARA can identify the mishap(s) associated with an ADAS function. It is assumed for AEB that the most common mishap related to AEB functionality is associated with injuries arising as a consequence of rear-end collision between two cars in a car-following scenario (see Figure B.3). An analysis was performed in order to identify the maximum tolerable (accepted) occurrence rate of rear-end collisions. A rate below the existing occurrence rate is considered as accepted by the general public. Traffic statistics provided by national road safety authorities can offer an overview of the existing rate at which the mishap happens in the field, classified by the posted speed in the locality of the accident. The data providers include NHTSA for the US, ONISR for France, ITARDA for Japan, BASt for Germany. Besides statistical overviews of road safety, ONISR also provides a database listing precise characterization of all accidents in France that resulted in injury or death of people (BAAC). Data with similar granularity can be obtained from the GIDAS study (Germany).

Traffic statistics can provide the following data:

- Number of passenger cars in the field ( $N$ )
- Average distance travelled by each passenger car per year ( $K$ )
- Number of rear end collision in the field per year within the range of defined posted speed  $v$  ( $A_v$ )

Based on this information, average distance travelled between collisions in each speed range can be calculated, see Formula (B.2). An assurance coefficient  $C_a$  is adopted to avoid under-estimation of the target validation mileage distance (e.g. accidents due to justified braking). The confidence of the model used to determine the probability of collision can be conservative enough not to warrant any further consideration of statistical confidence, e.g. much more conservative than a 70% confidence interval. However, further statistical confidence can be added, if relevant by using the  $C_a$  factor.

$$C_{KT_v} = \frac{NK}{A_v} C_a \quad (B.2)$$

The goal of the analysis is that the end user of the vehicle cannot be exposed to a risk of a rear end collision which is higher than the one normally accepted using a vehicle not equipped with an AEB system. It is assumed that the use of AEB cannot increase the risk of accidents of types other than rear end collision.

The value  $C_{KT_v}$  represents the target false alarm rate for the system in each posted speed limit interval.

1010 NOTE The target presented above is only a probabilistic theoretical objective to explain risk that can be  
 1011 tolerated in the decision to release the product to the market. Therefore, even if this probability is achieved, when  
 1012 a false alarm occurs in the actual market, the judgment of whether countermeasures are necessary requires  
 1013 another consideration.

1014 Merging the dependencies taken from the traffic statistics analyses (B.2) with the results of the  
 1015 simulation as given by equation (B.1) and taking all feasible values of  $\delta v$  (i.e.  $|\delta v| < |v|$ ) into account, it  
 1016 is possible to identify (in relation to the performance described in section B.3) the number of kilometres  
 1017 of data ( $D_{km}$ ) that need to be collected/analysed at each posted speed limit in order to validate that the  
 1018 system behaviour is robust enough w.r.t. the SOTIF requirements:

$$D_{km} = P(v) C_{KT\_v} = \frac{K}{A_v C_a} \sum_{\delta v} P(v, \delta v) \quad (B.3)$$

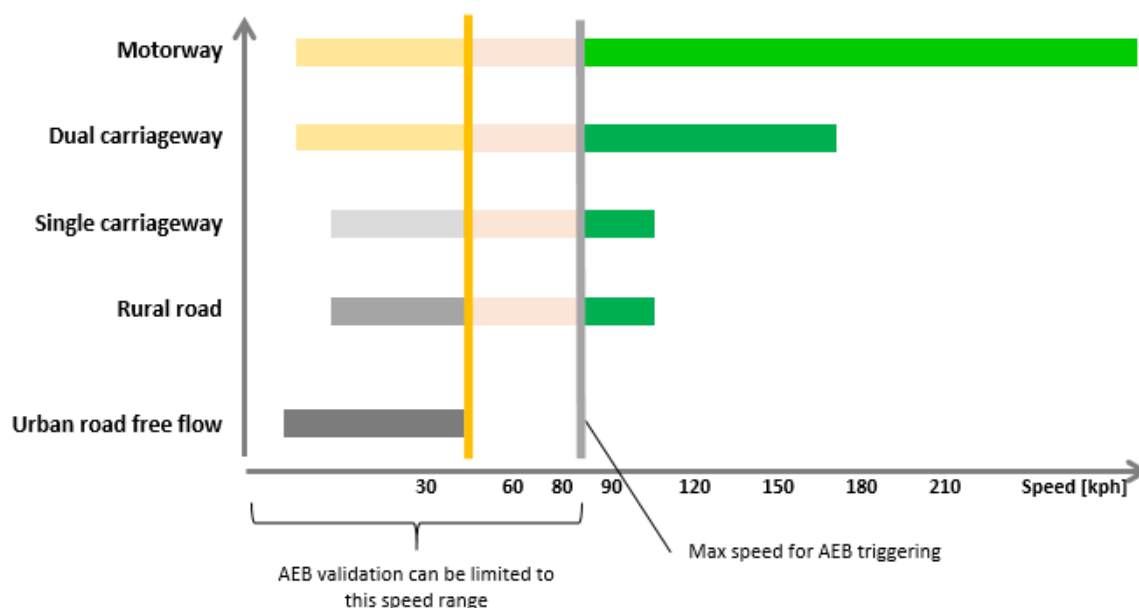
1019 NOTE 1 If a “grey box” approach is used, and the architecture includes independent elements with independent  
 1020 logic such that some statistical independence can be shown, then this architecture can be evaluated taking this  
 1021 independence into account. Reduction in validation requirements for each independent element can result. Any  
 1022 statistical dependency must be considered, e.g. as in the Beta Factor in IEC 61508.

1023 NOTE 2 For all calculations and inferences performed based on statistical data, it is required to utilize appropriate  
 1024 methods and confidence levels that are standard for the industry.

## 1025 B.5 Definition of the amount of data collection

1026 The vehicle mission profile can be used to address the data collection and validation strategy as well as  
 1027 available data from recognized international standards. As an example, Figure B.4 shows the speed  
 1028 intervals observable on roads of different kinds. Colour coding shows the probability of rear-end  
 1029 collision as a result of an erroneous AEB activation. The information on “risky” speed ranges can be  
 1030 used to address the data collection for the AEB system.

1031 NOTE A potential AEB activation at a speed of more than 80 km/h violates the limitations of the item. This can,  
 1032 for example, be implemented by an external measure as suggested in ISO 26262.



1033

1034 **Figure B.4 Target validation mileage per posted speed limit**



1035 Depending on the vehicle mission profile and the required performance, the data collection can include  
 1036 a comprehensive variety of driving conditions in terms of weather, time of day, and speed. As an  
 1037 example:

- 1038     ○ Speed: the host vehicle speed can be relevant for the feature in scope. For this example, no  
 1039 speeds above 80 km/h are considered
- 1040     ○ Weather condition: the AEB system can be tested according to a representative set of weather  
 1041 conditions. This includes dry, fog, snow, rain, overcast etc.
- 1042     ○ Time of day: depending on the type of sensor, data collection can include different times of day,  
 1043 such as night, dusk, etc.

1044 In addition, the data collection can include relevant driving situations derived from analysis of sensor  
 1045 limitations and feature specific limitations.

1046 An example of data collection specification for the feature that is the subject of this example is given in  
 1047 Table B.1. The specification may be based on real-life profiles for weather, speed and other parameters.  
 1048 An alternative approach suggests choosing the parameters related to the increased probability of a  
 1049 traffic accident of interest (e.g. rear end collision for the considered example). The relationship between  
 1050 external parameters and probability of accidents of specific types may be found via statistical analysis.

1051 Table B.1 Example of data collection specification

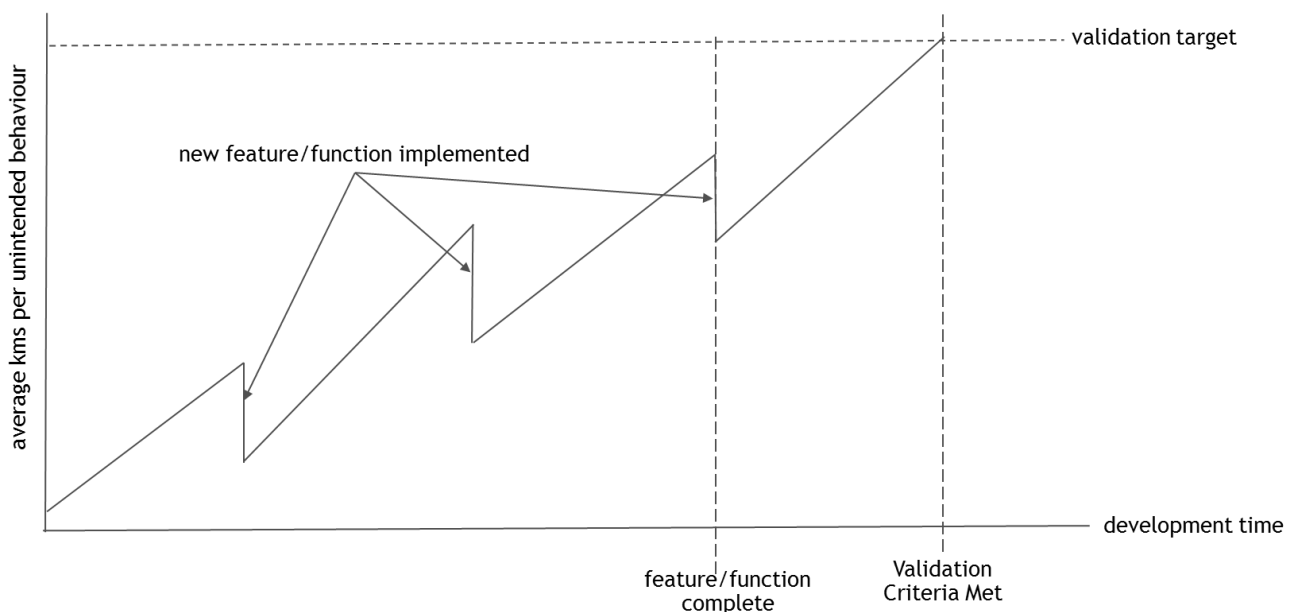
Time of day		
Type		Percentage
Day		50%
Night		35%
Dusk		15%
Vehicle Speed		
Speed [mi/h]	Speed [km/h]	Percentage
0-25	0-40	60%
26-50	41-80	40%
>50	>80	0%
Weather condition		
Type		Percentage
Dry / Clear sky		65%
Rain		7%
Fog		5%
Snow		5%
Overcast		10%
Heavy rain		5%

## Annex C (informative): Validation of SOTIF Applicable Systems

Technical limitations of the system can be a significant source of problems for SOTIF. This Annex addresses the validation activities for Figure 9 area 3. Concepts for deriving the validation targets are presented.

For SOTIF, 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 may contain some structured testing, dedicated analysis and simulation but the key aspect, especially for area 3, is to have sufficient testing under sufficiently random operating conditions to expose unknown unsafe scenarios.

Typical vehicle software development for SOTIF applicable systems is expected to have a history trajectory of average hours or kilometres per unintended behaviour as schematically shown in Figure C.1. As the software is tested and unintended behaviours are removed, the average kilometres between unintended behaviours is expected to rise. However, as new features/functions are introduced or enabled, the average hours or kilometres per unintended 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.



1068

1069 **Figure C.1 Expected profile of unintended behaviour rate during development**

1070 For example, prior to testing, the item owner specifies the following:

- 1071 1. Validation target (stopping rule)
- 1072 2. Weighting between testing modes, real-world tests, HIL, SIL, etc.
- 1073 3. Definition of validation unintended behaviours, criterion for restarting distance counter

1074 The process of validating SOTIF applicable systems starts with the selection of a validation target (see  
1075 Clause 6.5). The target can be calculated based on the system use case (e.g. assisted parking, automatic  
1076 emergency braking, lane keeping, autonomous parallel parking, low speed autonomous car park shuttle,  
1077 highway autopilot, autonomous taxi), crash statistics for the use case and a safety margin.

1078 **EXAMPLE** For a particular use case, human drivers experience an average of  $x$  kilometres between incidents. For  
1079 safety reasons an additional margin  $y$  is specified. The validation target for the SOTIF applicable system selected is  
1080  $x * y$  average kilometres between unintended behaviours or a target incident rate of  $\lambda = 1 / (x * y)$ . The stopping

1081 rule assumes that the incidents have a Poisson distribution. The system can be shown to have an incident rate  
1082 greater than or equal to  $\lambda$  with a confidence  $\alpha$ , if there is  $\tau$  quantity of driving with no unintended behaviours,  
1083 where  $\tau$  is given in equation (C.1) [9]:

1084 
$$\tau = -\ln(1 - \alpha) / \lambda \quad (C.1)$$

1085 NOTE  $\tau$  can be in units of time or distance depending on the units of incident rate.

1086 NOTE 2 For  $\alpha = 0.63$ ,  $\tau = 1/\lambda$ .

1087 In practice,  $\tau$ , the number of validation kilometres or hours to be driven can be quite large and therefore  
1088 not practical in some cases. The real-world driving requirement can be lessened by using expert  
1089 knowledge with similar systems and MIL, SIL and HIL simulated kilometres. An acceptable split  
1090 between real-world and simulated kilometres can be specified. Real-world and simulated validation test  
1091 conditions are varied as much as possible (e.g. different weather conditions, time of day, road  
1092 conditions, traffic conditions, pedestrian conditions, etc.) to try and uncover rare operating situations.

1093 Especially for ADAS functions it is also possible to reduce the validation target  $x*y$  by considering the  
1094 exposure to hazardous situations. Depending on the function it is possible to calculate the exposure  
1095 quantitatively by using data from on-road data collection.

1096 The criteria that characterise unintended behaviour, are specified. Care is taken if one encounters an  
1097 issue early in testing. In this case, [9] demonstrates that the additional amount of testing might be  
1098 greater than  $\tau$  (i.e. greater than restarting at zero kilometres with the original metric) for the same  
1099 confidence level.

## 1100 **Annex D (informative): Automotive perception systems verification and** 1101 **validation**

1102 The verification and validation of automotive perception systems is difficult. This annex describes  
1103 example practices for the verification and validation of these systems.

1104 Assumption:

- 1105 • Test drives might not cover every drivable road.

1106 Drivers normally drive a small number of routes repeatedly but in different environmental conditions.

1107 Example considerations for developing perception systems verification test plans (not comprehensive):

- 1108 1. Continuous data collection, in different markets, weather and illumination conditions. The data  
1109 represents the real-world user profile (kilometre distribution over different types of roads,  
1110 weather, illumination etc.)
- 1111 2. Specific data collection, in conditions which are normally rare and less represented in normal  
1112 driving but that might impact perception:
  - 1113 a. Vision perception – data at dusk or dawn
  - 1114 b. Lidar system – Adverse weather
  - 1115 c. Radar system – Rain and splash conditions on salt spread roads
  - 1116 d. All systems – Entering, exiting or within a tunnel
- 1117 3. Specific data collection, in uncommon scenarios that might increase the likelihood of a safety  
1118 violation:
  - 1119 a. Driving on roads with sparse traffic and no lead cars can increase the probability of  
1120 failure of in-path target selection and detection of ghost targets.
  - 1121 b. Overtaking a line of trucks with long shadows covering the passing lane(s).
  - 1122 c. Snow sprayed when passing by a snowplough can lead to a sudden blindness of one or  
1123 more perception systems.
- 1124 4. Specific data collection, based on system limitations:
  - 1125 a. Based on radar braking in metal bridges:
    - 1126 i. Specific data collection in such bridges will be made, including repetitions in  
1127 different driving condition (host and target cars)
    - 1128 ii. Test track set-up will be created to emulate the triggering event, and the  
1129 robustness of the solutions will be tested in this setup.
  - 1130 b. Based on vision system – High beam control function does not turn on in the absence of  
1131 oncoming traffic:
    - 1132 i. Driving on dark roads with sparse traffic.
- 1133 5. Various drivers and driving habits need to be taken into account, including the equivalent of  
1134 “double blind testing” (for example, tell drivers that they need to test the sound system quality  
1135 in perception test cars)
- 1136 6. Dedicated testing in extreme conditions:
  - 1137 a. Weather:
    - 1138 i. Winter testing
    - 1139 ii. Hot test
  - 1140 b. Infrastructure quality:
    - 1141 i. Dual-lane motorway
    - 1142 ii. Roads with poor maintenance and poor road markings
  - 1143 c. Traffic and driving dynamics:
    - 1144 i. Boston vs San Francisco.
    - 1145 ii. Bangkok.
    - 1146 iii. Seoul rush hour.
    - 1147 iv. Naples.
    - 1148 v. New York.

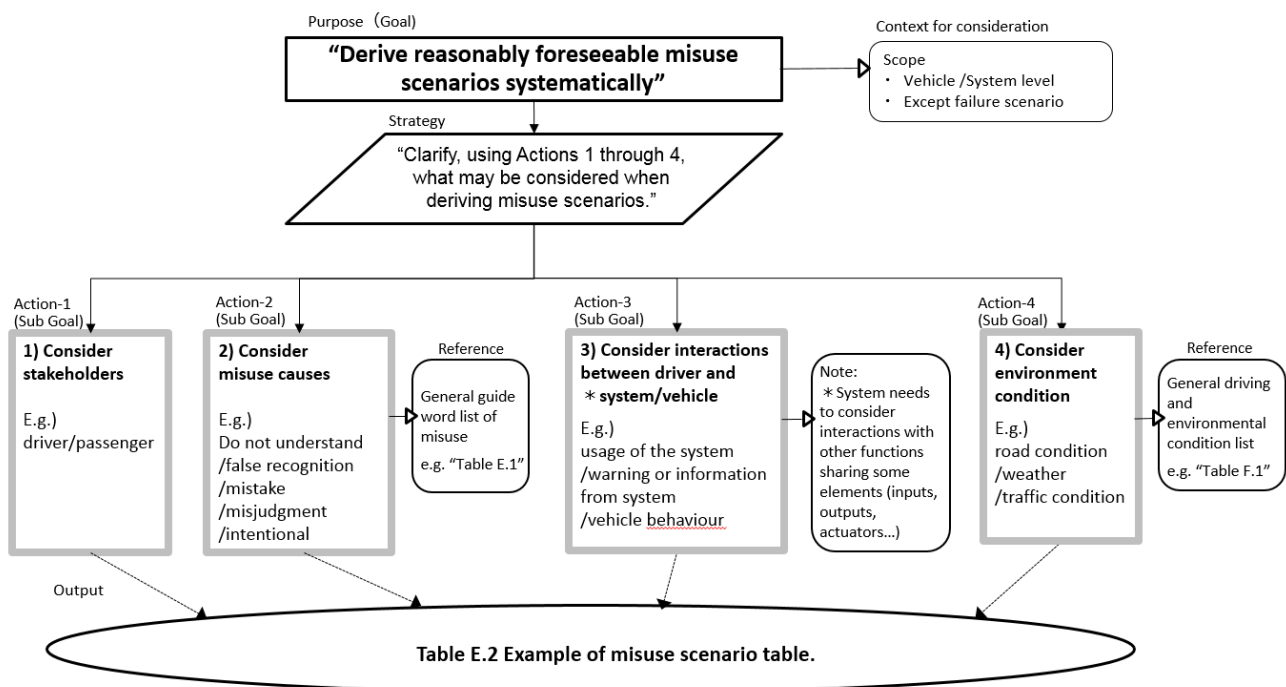
- d. Near road clutter
  - i. Las Vegas at night produces a large number of light sources as opposed to a normal road scenario.
- e. Urban environment:
  - i. VRU (Vulnerable Road Users) rich environment.
- 7. Production tolerances testing – it is expected that there will be ranges within mass production, therefore data is collected with variable performance sensing modules:
  - a. Camera – testing over expected focus range.
  - b. Radar – testing with different antenna sensitivity.
- 8. Active systems – testing the interaction between systems:
  - a. Need to rule out the effect of one perception system affecting other perception systems (as an example radars jamming each other on different cars or on the same car)
    - i. On a test track.
    - ii. In the real world (staged and unstaged testing).
- 9. Testing on multiple versions:
  - a. Different stages of the code expose system behaviour and possible weaknesses.
  - b. Derive better robustness from process repetition.
  - c. Prevent problems from re-emerging later on.
- 10. Feature based testing
  - a. Allows large data set analysis based on discovery of hazardous behaviour.
  - b. Use of larger feature scope allows mileage multiplication and rare events identification (e.g. using higher Time To Collision for AEB, ignore driver intent in features).
- 11. Measurement of standalone perception system performance
  - a. Measure the angular separation capabilities (in azimuth and elevation)
  - b. Measure the range separation capabilities
  - c. Measure the object measurement accuracy

There is much benefit in having an ability to incorporate use cases and lessons learned from system generation into new versions and configurations. Having such an ability (for example, knowing that the code will run data also from past configurations) allows some data re-use between development programs.

1180 **E.1 Overview**

1181 For systems that are SOTIF relevant, it is important to consider potential reasonably foreseeable misuse  
 1182 when performing the safety analysis. Misuse scenarios can be derived from various sources, such as:  
 1183 lessons learnt, expert knowledge, brainstorming by designers, etc. This Annex gives an example  
 1184 methodology for systematically deriving misuse scenarios to support the SOTIF safety analysis. The  
 1185 concept overview of this example methodology is given in Figure E.1 and an example of a misuse  
 1186 scenario is outlined. The approach to the human factors analysis is described in the HFACS document  
 1187 [10].

1188



1189 **Figure E.1. Systematic derivation of SOTIF misuse scenarios.**  
 1190

1191 Points to consider and an example misuse scenario table are described in section E.2.

1192 **E.2 Flow of safety analysis method for misuse.**

1193 The points that can be considered when deriving the misuse scenarios are described below:

1194 1) Stakeholders

1195 Consider who performs the misuse that leads to the hazard (e.g. driver, passenger)

1196 2) Misuse causes

1197 When considering the misuse causes, general “Guide words,” derived from the typical human  
 1198 misuse process (Recognition, Judgment, and Action) can be useful.

1199 Examples of possible guide words are described in Table E.1.

1200 **Table E.1** — Guide words for human error

Process	Guide word	Example
Recognition	1. Do not understand	Cannot operate correctly due to complicated usage.
	2. False recognition	Cannot recognize correctly due to overloaded information.
Judgment	3. Judgment error/ misjudgment	Misjudgment due to wrong impression or misunderstanding.
Action	4. Slip/Mistake	Mistake due to loss of concentration (distraction, snooze, etc.).
	5. Intentional	Violation of traffic regulations or social rules.
	6. Unable	Hard to operate

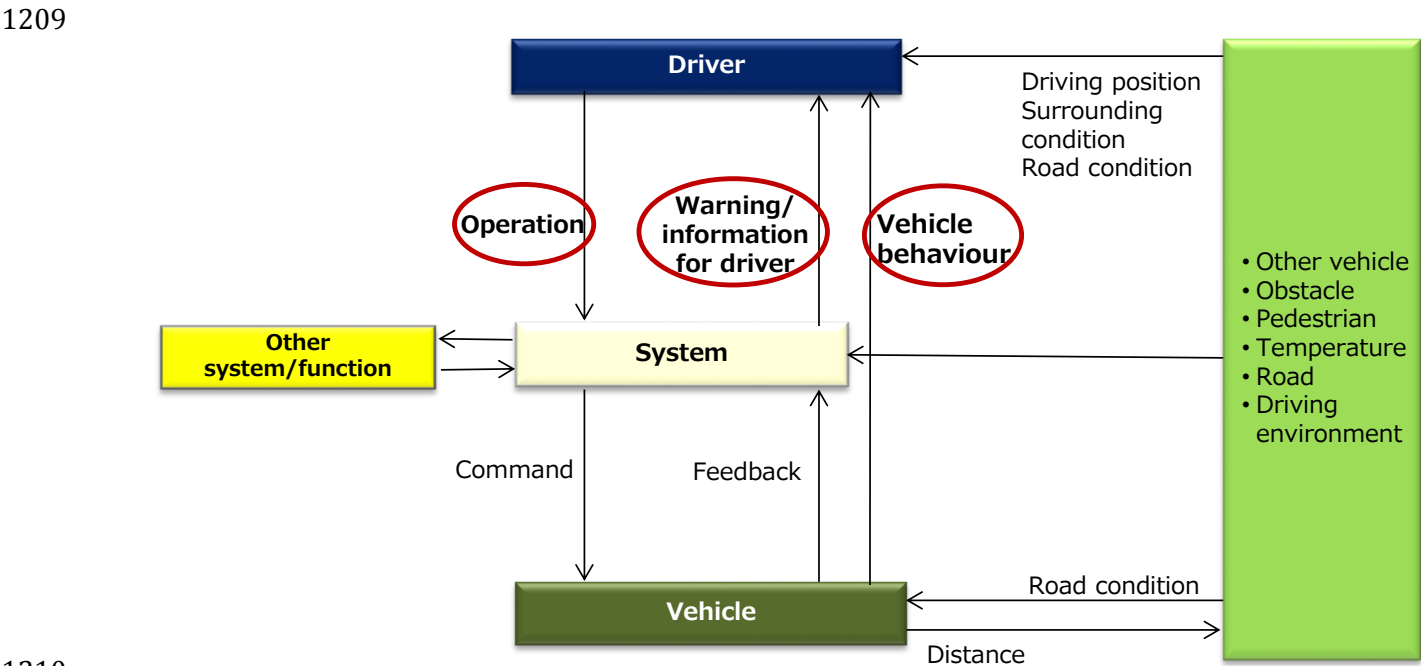
1201

1202 3) Interactions between the driver and system/vehicle

1203 A possible cause of misuse might be miscommunication between the Driver and the  
1204 System/Vehicle interfaces. (See Figure E.2)

1205 For example, the following interface subjects can be derived.

- 1206 • System operation by the driver (Usage): Interface “from Driver to System/Vehicle”
- 1207 • Warning notification from the system: Interface “from System/Vehicle to Driver”
- 1208 • System/vehicle behaviour: Interface “from System/Vehicle to Driver”



1211 **Figure E.2.** An example of interactions between driver and system/vehicle

1212 NOTE The boxes and arrows in Figure E.2 have the following meaning:

- 1213 - Boxes: external factors interacting with the system (possibility),
- 1214 - Arrow: interaction (possibility)

1215 4) Consideration of the environment in use case scenarios

1216 The impact of the environment, including road conditions, can be considered when deriving the  
1217 misuse scenario.

1218 EXAMPLE Some environmental conditions for consideration in use cases scenarios are described in  
 1219 Annex F.2.2 Table F.1.

1220 NOTE Table F.1 can be used both for the performance limit scenario analysis and for misuse scenario analysis.

1221 When the misuse scenario is derived considering points 1) to 4) in Annex E, a scenario table, such  
 1222 as Table E.2, can be used.

1223 **Table E.2** — Example of misuse scenario table based on guide word approach similar to HAZOP.

Performance limitation scenario	1) Stakeholders	2) Misuse causes		3) interactions between driver and system/vehicle	Misuse scenario 4) consider condition of environment
		process	Guide words		
“While operating autonomously on a highway, the vehicle cannot estimate the location of the lane boundary due to a performance limitation. The vehicle starts to leave the lane and the driver is notified to take control.”	Driver ...	Recognition	1.Do not understand	Operation(Usage)	...
				Vehicle behaviour	...
			2.False recognition	Warning/information	“Driver does not take over control of the vehicle and vehicle departs lane because driver does not know meaning of the warning”
				Operation(Usage)	...
		Judgment	3.Judgment error/ misjudgement	Vehicle behaviour	...
				Warning/information	...
		Action	4.Slip/Mistake	...	...
			5. Intentional “driver vacated seat”	...	...
			6.Unable “Driver not paying attention Driver asleep”	...	...
			...	...	...
...	...	...	...	...	...

1224 NOTE 1 Methods such as HAZOP and STPA analysis can be useful in deriving misuse scenarios. STPA (Systems  
 1225 Theoretic Process Analysis) is a hazard analysis method which considers the hazard factor in interacting function  
 1226 units.

1227 NOTE 2 This Annex E method is not intended to be a comprehensive analysis of all combinations. The methods  
 1228 outlined in Annex E are intended as an example that can be used to initiate the derivation of the analyses required  
 1229 for a specific SOTIF development. Only factors that influence hazardous events are selected for the analysis.  
 1230 Factors that have no influence on hazardous events can be recorded as not applicable.



1231

1232

Annex F (informative) Example construction of scenario for SOTIF safety analysis method

1233

1234

This annex gives an example methodology for developing scenario to support the safety analysis of Clause 7.

1235

1236

1237

The following steps are taken to identify and evaluate potential triggering events affecting system performance caused by various conditions, such as: parts characteristics, process, phenomenon, and environment condition.

- 1238
- 1239
- 1240
1.

Break down a strategy into three parts: recognition, judgment, and vehicle performance.
2.

Construct performance limiting scenarios with influencing factors for each part from triggering condition.

1241

Table F.1 Example Scenario of Factors

Factor	
climate	fine
	cloudy
	rainy
	sleet
	snow (accumulation of snow)
	hail
	fog
time of day	early morning
	daytime
	evening
	night time
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
	tollgate
	merging
	branching
	pothole
road condition	dry
	wet
	low $\mu$ path
	crossover road
	water trough
	gravel road
ego vehicle operation	vehicle is accelerating
	vehicle is decelerating
	vehicle is driving at constant speed
	vehicle is stopping
	drive at high speed
	drive at low speed
	vehicle is making a turn
	vehicle is making a sudden traversing

	passing
	right or left turn
vehicle around <ul style="list-style-type: none"> <li>• preceding vehicle</li> <li>• to side vehicle</li> <li>• oncoming vehicle</li> </ul> including <ul style="list-style-type: none"> <li>• motorcycle</li> <li>• bicycle</li> </ul>	preceding vehicle makes sudden deceleration
	preceding vehicle makes deceleration
	preceding vehicle makes acceleration
	preceding vehicle makes sudden acceleration
	interrupting vehicle
	trailing vehicle in stop and go traffic
	there is vehicle to right of ego vehicle going in same direction
	there is vehicle to left of ego vehicle going in same direction
	there is an oncoming vehicle
	high beam of oncoming vehicle
	passing by a motorcycle
	bicycle
Other road participants	pedestrian is walking across
	truck
	three-wheeled motorcycle
	peculiar vehicle
objects off-roadway (surroundings)	sidewall
	sign (upside)
	sign (side)
	pole
	tunnel
	multi-story parking space
	beneath a viaduct
	kerb
	guardrail
	pylon
	pots dots, cats eye
	vehicle stopping on the side of the road
	animal jumping out
	railway crossing
	construction site
	marked crosswalk
	water alongside road

1242 EXAMPLE Use case construction: climate = rainy, time of day = daytime, shape of road = straight, road conditions =  
 1243 wet, ego vehicle operation= vehicle is stopping, other vehicles = oncoming and on right side, pedestrian = none,  
 1244 objects off-roadway = none

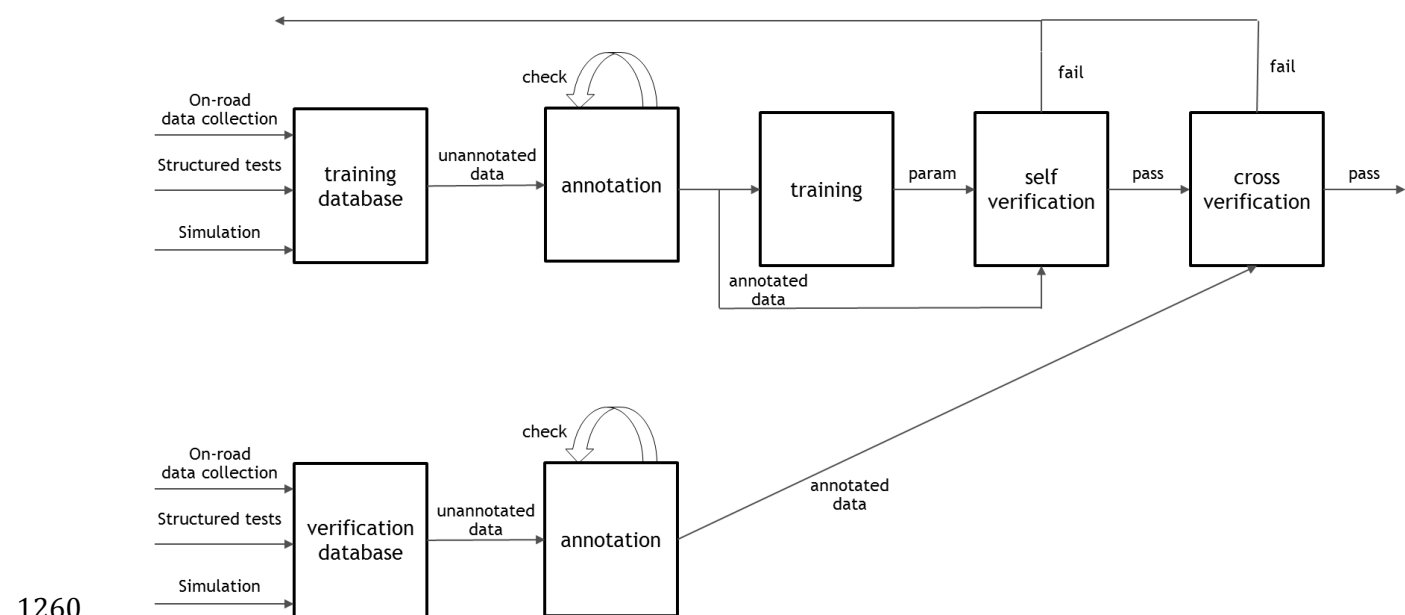
1245 NOTE Table F.1 is not comprehensive. Other factors can be considered when constructing use cases such as  
 1246 local driving customs and infrastructure.

## 1247 Annex G (informative): Implications for Off-line Training

1248 Autonomous vehicle technology typically involves some type of machine learning, especially for object  
 1249 detection and classification. Machine learning training has the potential to introduce systematic faults.  
 1250 As this process can be of critical importance to the safe operation of the vehicle, this can lead to the  
 1251 need for the data collection and learning system to be developed according to safety standards, with  
 1252 attention given to reducing hazards such as unintended bias or distortion in the collected data [11].

1253 Off-line training can involve several steps some of which may be considered as tools. ISO 26262-  
 1254 8:2018 Clause 11 deals with the qualification of software tools where an erroneous output of the tool  
 1255 can introduce or fail to detect errors in a safety-related item or element being developed. An argument  
 1256 built around this consideration can be a good basis to justify of tools used to support algorithms which  
 1257 rely on machine learning. However, off-line training can involve several steps and tools and can need  
 1258 additional attention.

1259 An example training process is shown in Figure G.1.



1260  
 1261 **Figure G.1 Off-line Machine Learning Process Flow**

1262 The top row of Figure G.1, starts with the collection of a training data base that is collected using a  
 1263 mixture of structured testing (e.g. tests designed and implemented on a test track), simulation and on-  
 1264 road random data collection. The data is then annotated for specific features to be learnt (e.g. road  
 1265 boundaries, cars, motorcycles, emergency vehicles). Since annotation is typically a manual process,  
 1266 there can be a check of the annotations; this is represented by the 'circle back' in the figure above.

1267 The annotated data is then used to determine parameters (e.g. neural net weights) via training. The  
 1268 trained system is then verified with the training data using pass/fail criteria, such as acceptable false  
 1269 positive and false negative rates. If the self-verification fails, the process can be restarted after more  
 1270 data is collected and/or training is modified.

1271 Self-verification might be insufficient since it is difficult to ensure that the learning system has trained  
 1272 on the essential characteristics of the training data instead of coincidental correlations [11]. One  
 1273 approach to address this problem is to verify the learning using a separately collected and annotated  
 1274 database (bottom row of Figure G.1). The cross-verification step evaluates the performance of the

1275 trained system to respond to the data contained in the verification database in a safe manner. Suitable  
1276 pass-fail criteria are selected before accepting the trained parameters.

1277 Many training limitation issues can be uncovered by verification and validation activities. However, it is  
1278 recommended that techniques such as a PFMEA (Process Failure Modes and Effects Analysis) can be  
1279 used to analyse and eliminate possible sources of bias and limitation within the off-line training process.  
1280 Example issues to be considered include coverage and diversity of:

- 1281 • Data Collection
  - 1282 ○ Vehicles and drivers
  - 1283 ○ Routes and driving conditions
  - 1284 ○ Structured tests
- 1285 • Annotation
- 1286 • Annotation Check

- 1288 [1] ULBRICH, S., MENZEL, T., RESCHKA, A., SCHULDT, F. and MAUER, M. "Defining and Substantiating the  
1289 Terms Scene, Situation, and Scenario for Automated Driving", 2015 IEEE 18th International  
1290 Conference on Intelligent Transportation Systems (ITSC), <https://doi.org/10.1109/ITSC.2015.164>
- 1291 [2] WATZENIG, D. and HORN, M. (editors), "Automated Driving - Safer and More Efficient Future Driving",  
1292 Springer International, 2017, p. 456. <http://rd.springer.com/book/10.1007/978-3-319-31895-0>
- 1293 [3] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor  
1294 Vehicles, SAE Recommended Practice J3016:SEPT2016, <[http://standards.sae.org/j3016\\_201609/](http://standards.sae.org/j3016_201609/)>.
- 1295 [4] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3";  
1296 <[http://www.acea.be/uploads/publications/20090831\\_Code\\_of\\_Practice\\_ADAS.pdf](http://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf)>
- 1297 [5] KUHN, D. S., KACKER, R. N. and LEI, Y., "Combinatorial testing", NIST report, June 25, 2012,  
1298 <https://www.nist.gov/publications/combinatorial-testing>
- 1299 [6] Source: Wikipedia:  
1300 [https://de.wikipedia.org/wiki/Fahrbahnmarkierung#/media/File:Roadworks\\_Germany\\_A9\\_2.jpg](https://de.wikipedia.org/wiki/Fahrbahnmarkierung#/media/File:Roadworks_Germany_A9_2.jpg)
- 1301 [7] FABRIS,S., PRIDDY, J. and HARRIS, F., "Method for Hazard Severity Assessment for the Case of  
1302 Unintended Deceleration", presented at 2012 VDA Auto SYS conference in Berlin.
- 1303 [8] FABRIS,S., PRIDDY, J. and HARRIS, F., "Method for hazard severity assessment for the case of  
1304 undemanded deceleration.", Presented at VDA Automotive SYS Conference, Berlin, June 19/20, 2012.
- 1305 [9] LITTLEWOOD B. and WRIGHT, D., "Some Conservative Stopping Rules for the Operational Testing of  
1306 Safety-Critical Software", IEEE Trans. SW Engng., 23(11), 673-683, Nov. 1997
- 1307 [10] SHAPPELL, S.A. and WIEGMANN, D.A., The Human Factors Analysis and Classification-System –  
1308 HFACS, February 2000 Final Report. This document is available to the public through the National  
1309 Technical Information Service, Springfield, Virginia 22161.
- 1310 [11] KOOPMAN, P. and WAGNER, M., "Autonomous Vehicle Safety: An Interdisciplinary Challenge," IEEE  
1311 Intelligent Transportation Systems Magazine, Special Issue on SSIV, 2017, in press Vol. 9 #1, Spring  
1312 2017, pp. 90-96.