

DRAFT INTERNATIONAL STANDARD

ISO/DIS 21448

ISO/TC 22/SC 32

Secretariat: JISC

Voting begins on:
2021-01-20

Voting terminates on:
2021-04-14

Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue

ICS: 43.040.10

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/DIS 21448](#)

<https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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.

This document is circulated as received from the committee secretariat.



Reference number
ISO/DIS 21448:2021(E)

© ISO 2021

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DIS 21448

<https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DIS 21448

[https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-
eb526ff1e98c/iso-dis-21448](https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448)

© 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
Web www.iso.org

Published in Switzerland.

Contents

Foreword	6
Introduction.....	7
1 Scope	10
2 Normative references	11
3 Terms and definitions.....	11
4 Overview and organization of SOTIF activities	18
4.1 General.....	18
4.2 SOTIF principles.....	18
4.3 Use of this document.....	23
4.4 Management of SOTIF activities and supporting processes.....	25
5 Specification and design	27
5.1 Objectives.....	27
5.2 Specification of the functionality and considerations for the design.....	27
5.3 Consideration on system design and architecture	28
5.4 Work Products.....	31
6 Identification and evaluation of hazards.....	31
6.1 Objectives.....	31
6.2 General.....	31
6.3 Hazard identification	31

6.4	Risk evaluation	33
6.5	Specification of acceptance criteria	34
6.6	Work Products.....	36
7	Identification and evaluation of potential functional insufficiencies and triggering conditions.....	36
7.1	Objectives.....	36
7.2	General.....	36
7.3	Analysis of potential functional insufficiencies and triggering conditions	36
7.4	Estimation of the acceptability of the response of the system to the triggering conditions.	42
7.5	Work Products.....	43
8	Functional modifications addressing SOTIF-related risks.....	43
8.1	Objectives.....	43
8.2	General.....	43
8.3	Measures to improve the SOTIF	44
8.4	Updating the input information for “Specification and design”	46
8.5	Work Products.....	47
9	Definition of the verification and validation strategy.....	47
9.1	Objectives.....	47
9.2	General.....	47
9.3	Specification of integration and testing	48
9.4	Work products.....	51
10	Evaluation of known hazardous scenarios (Area 2).....	51
10.1	Objectives.....	51
10.2	General.....	51
10.3	Sensing verification	51
10.4	Planning algorithm verification.....	52
10.5	Actuation verification	53
10.6	Integrated system verification.....	54
10.7	Acceptability of residual risk due to known hazardous scenarios	54
10.8	Work products.....	55
11	Evaluation of unknown hazardous scenarios (Area 3).....	55
11.1	Objectives.....	55
11.2	General.....	55
11.3	Evaluation of residual risk due to unknown scenarios.....	55

11.4	Acceptability of residual risk due to unknown hazardous scenarios	57
11.5	Work products.....	57
12	Criteria for SOTIF release	57
12.1	Objectives.....	57
12.2	General.....	58
12.3	Criteria for evaluating SOTIF for release	58
12.4	Criteria and methods for SOTIF evaluation.....	60
12.5	Work products.....	60
13	Operation phase activities	60
13.1	Objectives.....	60
13.2	General.....	60
13.3	Objects of observation.....	61
13.4	SOTIF issue evaluation and resolution process	62
13.5	Work Products.....	63
Annex A (informative)	General guidance on SOTIF	64
A.1	Examples of structuring the SOTIF argumentation with GSN	64
A.2	Explanations regarding the interaction between functional safety according to the ISO 26262 series and this document.....	83
A.3	Simplified SOTIF Application Examples.....	93
Annex B (informative)	Guidance on Scenario and system analyses	96
B.1	Method for deriving SOTIF misuse scenarios.....	96
B.2	Example construction of scenario factors for SOTIF safety analysis method	99
B.3	Examples of adaptation of safety analyses to identify and evaluate the potential triggering conditions and functional insufficiencies	105
B.4	Applying STPA in the Context of SOTIF for ADAS and Automated Vehicles	115
Annex C (informative)	Guidance on SOTIF verification and validation.....	120
C.1	Purpose of the Validation Strategy.....	120
C.2	Example for definition and validation of an acceptable false positive activation rate in AEB systems	121
C.3	Validation of SOTIF Applicable Systems	127
C.4	Perception system verification and validation.....	130
C.5	Guidance on scenario parameterization and sampling	140
C.6	Considerations for reducing validation testing.....	148
Annex D (informative)	Guidance on specific aspects of SOTIF.....	156
D.1	Guidance for driving policy specification.....	156

D.2	Implications for machine learning	166
D.3	SOTIF considerations for maps.....	172
D.4	SOTIF considerations for V2X	174

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/DIS 21448](https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448)

[https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-
eb526ff1e98c/iso-dis-21448](https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448)

1 Foreword

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

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 any
15 patent rights identified during the development of the document will be in the Introduction and/or on
16 the ISO list of patent declarations received. 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 Barriers
21 to Trade (TBT) see the following URL: [Foreword - Supplementary information](http://www.iso.org/foreword)

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

23 ISO 21448 consists of this document only.

24 Introduction

25 The safety of road vehicles during their operation phase is of paramount concern for the road vehicles
 26 industry. The number of advanced functionalities included in vehicles is increasing. These rely on sensing,
 27 processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E)
 28 systems.

29 An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by
 30 every hazard associated with the intended functionality and its implementation, especially those hazards
 31 not due to failures, but due to insufficiencies of specification or performance limitations.

32 For the achievement of functional safety (FuSa), ISO 26262-1 defines the functional safety as the absence
 33 of unreasonable risk due to hazards caused by malfunctioning behaviour of the E/E system. ISO 26262-3
 34 defines how to develop a Hazard Analysis and Risk Assessment (HARA) to determine vehicle level
 35 hazards. The HARA evaluates the potential risks due to malfunctioning behaviour of the item to
 36 determine top-level safety requirements, i.e. the safety goals, necessary to mitigate the risks. The other
 37 parts of the ISO 26262 series provide requirements and recommendations to avoid and control random
 38 hardware failures and systematic failures that could violate safety goals.

39 For some E/E systems, which rely on sensing the external or internal environment to build situational
 40 awareness, there can be potentially hazardous behaviour caused by the intended functionality, despite
 41 these systems being free from the faults addressed in the ISO 26262 series. Example causes of such
 42 potentially hazardous behaviour include:

- 43 – the inability of the function to correctly perceive the environment;
<https://standards.iteh.ai/catalog/standards/sist/51ac264d-83f4beb-afd1-12c16987c101/iso-21448>
- 44 – the lack of robustness of the function, system, or algorithm with respect to sensor input
 45 variations, heuristics used for fusion, or diverse environmental conditions;
- 46 – the unexpected behaviour due to decision making algorithm and/or divergent human
 47 expectations.

48 This also applies to functions, systems or algorithms that use machine learning. The absence of
 49 unreasonable risk due to these potentially hazardous behaviours related to these functional
 50 insufficiencies is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed
 51 by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

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

- 54 – the specification and design phase;

55 EXAMPLE Modification of vehicle functionality or of sensor performance requirements, driven by
 56 identified system limitations or by previously unknown hazardous scenarios.

- 57 – the verification phase;

58 EXAMPLE Technical Reviews, test cases with a high coverage of relevant scenarios, injection of
 59 potential triggering conditions, in the loop testing (e.g. SIL : Software in the loop / HIL : Hardware in the
 60 loop / MIL : Model in the loop) of selected SOTIF-relevant scenarios.

61 - the validation phase;

62 EXAMPLE Long-term vehicle test, simulation-based testing.

63 - the operation phase;

64 EXAMPLE Field monitoring of SOTIF incidents.

65 In many instances, triggering conditions are necessary to cause a potentially hazardous behaviour. In
66 addition, triggering conditions include reasonably foreseeable direct misuse. Therefore, a proper
67 understanding by the user of the functionality, its behaviour and its limitations (including the
68 human/machine interface) is essential to ensure safety.

69 In this document, potentially hazardous behaviour is considered for use cases when the vehicle is
70 correctly used and for use cases when it is incorrectly used in a reasonably foreseeable way (this excludes
71 intentional alterations made to the system's operation).

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

73 In addition, reasonably foreseeable misuse, which could lead directly to potentially hazardous behaviour,
74 is also considered as possible triggering conditions.

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

77 EXAMPLE By opening the door, the user unintentionally obstructs a sensor's field of view.

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

81 Ensuring compliance with local driving laws, policies, or road norms is out of scope of this document,
82 except in the case where not following laws and rules of the road could lead to safety hazards.

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

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

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

93 For a more detailed description of the articulation between ISO 26262 and this document, please refer to
94 Annex A.2.

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

96

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

Source	Cause of hazardous events	Within scope of
System	E/E System failures	ISO 26262
	Insufficiencies of specification, performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	This document
	Incorrect and inadequate Human-Machine Interface (HMI) design (inappropriate user situational awareness, e.g. user confusion, user overload, user inattentiveness)	This document European Statement of Principles on human-machine interface [1]
	system technologies EXAMPLE: Eye damage from a laser sensor	Specific standards
External factor	Reasonably foreseeable misuse	This document
	Attack exploiting vehicle security vulnerabilities	ISO/SAE 21434 or SAE J3061
	Impact from active infrastructure and/or vehicle to vehicle communication, and external systems	This document ISO 20077; ISO 26262
	Impact from vehicle surroundings (e.g. other users, passive infrastructure, weather, Electro-Magnetic Interference)	This document ISO 26262

97

ISO/DIS 21448
<https://standards.iteh.ai/catalog/standards/sist/51ac264d-8f3f-4beb-afd1-eb526ff1e98c/iso-dis-21448>

98 Road vehicles — Safety of the intended functionality

99 1 Scope

100 This document provides a general argumentation framework and guidance on measures to ensure the
101 safety of the intended functionality (SOTIF), i.e. the absence of unreasonable risk due to a hazard caused
102 by:

- 103 a. the insufficiencies of specification of the intended functionality at the vehicle level, or
- 104 b. the insufficiencies of specification or performance limitations in the implementation of E/E
105 elements in the system

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

107 These hazards can be triggered by specific conditions of a scenario, including reasonably foreseeable
108 misuse of the intended functionality or in combination with other functions at the vehicle level (e.g.
109 activation of the parking brake while the automated driving function is active).

110 NOTE Information provided by the infrastructure (e.g. Car2x communication, maps) is also part of the evaluation
111 of functional insufficiencies if it can have an impact on the SOTIF.

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

114 This document is applicable to an intended functionality where proper situational awareness is essential
115 to safety and where such situational awareness is derived from complex sensors and processing
116 algorithms, especially emergency intervention systems and systems having automation levels from 1 to
117 5.

118 This document is applicable to intended functionalities that include one or more electrical and/or
119 electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds.

120 This document does not apply to faults covered by the ISO 26262 series.

121 This document does not apply to hazards directly caused by the system technology (e.g. eye damage from
122 a laser sensor).

123 This document does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity,
124 flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by the
125 intended functionality of safety-related E/E systems.

126 This document does not apply to attacks exploiting vehicle security vulnerabilities.

127 This document considers local driving laws, policies, or road norms only as far as they can impact the
128 SOTIF, specifically where not following laws and rules of the road could lead to safety hazards. However,
129 this document does not address legal compliance to driving laws and/or policies.

130 Furthermore, functions of existing systems for which well-established and well-trusted design,
131 verification and validation (V&V) measures exist (e.g. Dynamic Stability Control (DSC) systems, airbag)
132 are exempt from the scope of this document.

133 EXAMPLE a system for which there is an existing standard sufficient to ensure safety

134 Some measures described in this document are applicable to newly designed functions or elements of
135 existing systems, if situational awareness derived from complex sensors and processing algorithms is
136 part of the design.

137 EXAMPLE Complex sensing and fusion of the road and cabin environment might replace current accelerometer (or
138 similar) based triggering mechanisms for airbags. SOTIF activities can be relevant, due to that change requiring
139 situational awareness.

140 Reasonably foreseeable misuse, which could lead directly to potentially hazardous behaviour, is in the
141 scope of this document as a possible triggering condition. This is defined as “reasonably foreseeable
142 direct misuse”.

143 Reasonably foreseeable misuse that prevents controllability by the driver of the system’s hazardous
144 behaviour, representing an unreasonable level of risk, is in scope of this document. This is defined as
145 “reasonably foreseeable indirect misuse”.

146 An intentional action that clearly violates the system’s intended use is considered feature abuse. This is
147 out of scope of this document.

148 EXAMPLE: Applying a substitute hand to fool a “hands on wheel” detection safety measure.

149 2 Normative references (standards.iteh.ai)

150 The following documents are referred to in the text in such a way that some or all of their content
151 constitutes requirements of this document. For dated references, only the edition cited applies. For
152 undated references, the latest edition of the referenced document (including any amendments) applies.

153 ISO 26262 – 1:2018, Road vehicles — Functional Safety Part 1: Vocabulary

154 3 Terms and definitions

155 For the purposes of this document, the terms and definitions given in ISO 26262-1:2018 and the following
156 apply.

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

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

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

160 3.1

161 acceptance criterion

162 criterion representing the absence of an unreasonable level of risk

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

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

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

171 3.2

172 action

173 single act or behaviour that is executed by any actor in a scene (3.26)

174 Note 1 to entry: The temporal sequence of actions/events (3.7) and scenes (3.26) specify a scenario (3.25).

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

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

178 3.3

179 driving policy

180 strategy and rules defining acceptable control actions (3.2) at vehicle level

181 3.4

182 dynamic driving task

183 DDT

184 real-time operational and tactical functions required to operate a vehicle in traffic

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

- 186 - Lateral vehicle motion control (operational);
- 187 - Longitudinal vehicle motion control (operational);
- 188 - Monitoring the driving environment (operational and tactical) and object and event (3.7) response
 189 execution (operational and tactical), see OEDR (3.20);
- 190 - Manoeuvre planning (tactical); and
- 191 - Enhancing conspicuity via lighting, signalling and gesturing, etc. (tactical).

192 [SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

193 3.5

194 DDT fallback

195 response by the driver or automation system to either perform the DDT (3.4) or transition to a minimal
 196 risk condition (3.16) after the occurrence of a failure(s) or detection of a functional insufficiency (3.8) or
 197 upon detection of a potentially hazardous behaviour

198 EXAMPLE ODD (3.21) exit or a sensor blocked by ice can lead to hazardous behaviour.

199 [SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

200 3.6

201 ego vehicle

202 vehicle fitted with functionality that is being analysed for SOTIF (3.24)

203

204 3.7

205 event

206 occurrence at a point in time

207 Note 1 to entry: The temporal sequence of actions/events (3.7) and scenes (3.26) specify a scenario (3.25).

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

209 EXAMPLE 2 Traffic light turning green at a given time

210 3.8

211 functional insufficiency

212 insufficiency of specification (3.12) or performance limitation (3.23)

213 Note 1 to entry: Functional insufficiencies include the insufficiencies of specification (3.12) of the intended
214 functionality (3.14) at the vehicle level, or the insufficiencies of specification (3.12) or performance limitations
215 (3.23) of the system elements.

216 Note 2 to entry: SOTIF (3.24) activities include the identification of functional insufficiencies and the evaluation of
217 their effects. Functional insufficiencies lead to hazardous behaviours by definition (see 3.12 and 3.23). The term
218 “potential functional insufficiency” can be used in the document when the ability to lead to hazardous behaviour is
219 not yet established.

220 3.9

221 functional modification

222 alteration of a functional specification

223 Note 1 to entry: Functional modification is not the same as the modification defined in ISO 26262.

224 3.10

225 fallback ready user

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

228 [SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

229 3.11

230 hazard

231 potential source of harm caused by the hazardous behaviour of the system

232 3.12

233 insufficiency of specification

234 specification, possibly incomplete, leading to hazardous behaviour in combination with one or more
235 triggering conditions (3.29)

236 EXAMPLE 1 A scenario (3.25) where the driving function in control of the ego vehicle (3.6) is not keeping a safe
237 distance to the vehicle in front can result from an insufficiency of specification.

238 EXAMPLE 2 System inability to handle uncommon road signs due to specification gaps

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

241 Note 2 to entry: SOTIF (3.24) activities include the identification of insufficiencies of specification and the
242 evaluation of their effects, possibly leading to hazardous behaviour. The term “potential insufficiency of
243 specification” can be used in the document when the ability to lead to hazardous behaviour is not yet established.

244 Note 3 to entry: Safety requirements derived from the specification, from the assumptions of other systems or
245 elements, or from systematic analyses (such as those included in Clause 6 or other analyses that elicit design and
246 implementation requirements for the SOTIF (3.24)) may be included in formal databases to support assurance of
247 verification. These requirements may not be designated as the “specification” in many organizations but are
248 necessary to ensure the SOTIF (3.24). The usage of the term “insufficiency (insufficiencies) of specification” in this
249 standard includes such derived requirements.