ISO 21448:2022-06 (E)

Road vehicles - Safety of the intended functionality

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 2

4 Overview and organization of SOTIF activities 11
4.1 General 11
4.2 SOTIF principles 11
4.2.1 SOTIF-related hazardous event model 11
4.2.2 The four scenario areas 12
4.2.3 Sense-Plan-Act model 15
4.3 Use of this document 16
4.3.1 Flow chart and structure of this document 16
4.3.2 Normative clauses 19
4.3.3 Interpretation of tables 19
4.4 Management of SOTIF activities and supporting processes 19
4.4.1 Quality management, systems engineering and functional safety 19
4.4.2 Distributed SOTIF development activities 20
4.4.3 SOTIF-related element out of context 20

5 Specificationanddesign 21
5.1 Objectives 21
5.2 Specification of the functionality and considerations for the design 21
5.3 System design and architecture considerations 22
5.4 Performance insufficiencies and countermeasures considerations 23
5.5 Work products 25

6 Identificationandevaluationofhazards 25
6.1 Objectives 25
6.2 General 26
6.3 Hazard identification 26
6.4 Risk evaluation 29
6.5 Specification of acceptance criteria for the residual risk 30
6.6 Work products 31

7 Identificationandevaluationofpotentialfunctionalinsufficienciesandpotential triggering conditions 31
7.1 Objectives 31
7.2 General 31
7.3 Analysis of potential functional insufficiencies and triggering conditions 32
7.3.1 General 32
7.3.2 Potential functional insufficiencies and triggering conditions related to planning algorithms 35
7.3.3 Potential functional insufficiencies and triggering conditions related to sensors and actuators 35
7.3.4 Analysis of reasonably foreseeable direct or indirect misuse 36
7.4 Estimation of the acceptability of the system's response to the triggering conditions 37

7.5 Work products ... 38

8 FunctionalmodificationsaddressingSOTIF-relatedrisks ... 38
8.1 Objectives ... 38
8.2 General ... 38
8.3 Measures to improve the SOTIF ... 38
8.3.1 Introduction ... 38
8.3.2 System modification ... 39
8.3.3 Functional restrictions ... 40
8.3.4 Handing over authority ... 41
8.3.5 Addressing reasonably foreseeable misuse ... 41
8.3.6 Considerations to support the implementation of SOTIF measures ... 42
8.4 Updating the input information for "Specification and design" ... 42
8.5 Work products ... 42

9 Definitionoftheverificationandvalidationstrategy ... 42
9.1 Objectives ... 42
9.2 General ... 42
9.3 Specification of integration and testing ... 43
9.4 Work products ... 45

10 Evaluationofknownscenarios ... 46
10.1 Objectives ... 46
10.2 General ... 46
10.3 Sensing verification ... 46
10.4 Planning algorithm verification ... 47
10.5 Actuation verification ... 48
10.6 Integrated system verification ... 48
10.7 Evaluation of the residual risk due to known hazardous scenarios ... 49
10.8 Work products ... 50

11 Evaluationofunknownscenarios ... 50
11.1 Objectives ... 50
11.2 General ... 50
11.3 Evaluation of residual risk due to unknown hazardous scenarios ... 50
11.4 Work products ... 52
11.4.1 Validation results for unknown hazardous scenarios fulfilling objective 11.1 ... 52
11.4.2 Evaluation of the residual risk fulfilling objective 11.1 ... 52

12 Evaluation of the achievement of the SOTIF ... 52
12.1 Objectives ... 52
12.2 General ... 53
12.3 Methods and criteria for evaluating the SOTIF ... 53
12.4 Recommendation for SOTIF release ... 54
12.5 Work products ... 54

13 Operation phase activities ... 55
13.1 Objectives ... 55
13.2 General ... 55
13.3 Topics for observation ... 56
13.4 SOTIF issue evaluation and resolution process ... 57
13.5 Work products ... 57

Annex A (informative) General guidance on SOTIF ... 58

Annex B (informative) Guidance on scenario and system analyses ... 95

Annex C (informative)GuidanceonSOTIFverificationandvalidation ... 125

Annex D (informative)GuidanceonspecificaspectsofSOTIF ... 159

Bibliography **179**