ISO/TR 4804:2020 (E)

Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 General approach and overview

4.1 Introduction and motivation
4.2 Overview of this document
4.3 Structure and development examples used in this document
4.4 Safety vision
4.4.1 Background
4.4.2 Positive risk balance and avoidance of unreasonable risk
4.4.3 Principles of safety and cybersecurity for automated driving
4.4.3.1 PSC_01: Cybersecurity
4.4.3.2 PSC_02: Data recording
4.4.3.3 PSC_03: Passive safety
4.4.3.4 PSC_04: Safety assessment
4.4.3.5 PSC_05: Safe operation
4.4.3.6 PSC_06: Safety layer
4.4.3.7 PSC_07: Behaviour in traffic
4.4.3.8 PSC_08: Operational design domain handling
4.4.3.9 PSC_09: Role of user
4.4.3.10 PSC_10: Driver initiated takeover
4.4.3.11 PSC_11: Vehicle initiated takeover request
4.4.3.12 PSC_12: Interdependency between driver and automated driving system

5 Systematically developing dependability to support safety by design

5.1 General
5.2 Deriving capabilities of automated driving from dependability domains
5.2.1 Applying the related safety standards
5.2.2 ISO/PAS 21448 - Safety of the intended functionality
5.2.3 ISO 26262 series - Functional safety
5.2.4 ISO/SAE 21434 - Automotive cybersecurity
5.2.5 Capabilities of automated driving
5.2.5.1 Initial derivation of capabilities
5.2.5.2 Overview of the capabilities
5.2.6 Minimal risk conditions and minimal risk manoeuvres
5.3 Elements for implementing the capabilities
5.3.1 Implementing the capabilities
5.3.1.1 FS_1: Determine location
5.3.1.2 FS_2: Perceive relevant static and dynamic objects
5.3.1.3 FS_3: Predict the future behaviour of relevant objects
5.3.1.4 FS_4: Create a collision-free and lawful driving plan
5.3.1.5 FS_5: Correctly execute and actuate the driving plan
5.3.1.6 FS_6: Communicate and interact with other road users
5.3.1.7 FS_7: Determine if specified nominal performance is not achieved
5.3.1.8 FD_1: Ensure controllability for the driver
5.3.1.9 FD_2: Detect when degradation is not available

5.3.1.10 FD_3: Ensure safe mode transitions and operating mode awareness
5.3.1.11 FD_4: React to insufficient nominal performance and other failures via degradation
5.3.1.12 FD_5: Reduce system performance in the presence of failure for the fail-degraded mode

5.3.1.13 FD_6: Perform ODD functional adaptation within reduced system constraints
5.3.2 Elements
5.3.2.1 Environment perception sensors
5.3.2.2 A-priori perception sensors
5.3.2.2.1 HD map
5.3.2.2.2 Global navigation satellite system (GNSS)
5.3.2.3 V2X
5.3.2.4 Sensor fusion
5.3.2.5 Interpretation and prediction
5.3.2.6 Localization
5.3.2.7 ADS mode manager
5.3.2.8 Egomotion
5.3.2.9 Drive planning
5.3.2.10 Traffic rules
5.3.2.11 Motion control
5.3.2.12 Motion actuators
5.3.2.12.1 Steering system
5.3.2.12.2 Braking system
5.3.2.12.3 Powertrain
5.3.2.13 Secondary actuators
5.3.2.14 Human-machine interaction
5.3.2.15 User state determination
5.3.2.16 Vehicle state
5.3.2.17 Monitors (all modes)
5.3.2.18 Processing unit
5.3.2.19 Power supply
5.3.2.20 Communication network
5.3.3 Generic logical architecture

6 Verification and validation

6.1 General
6.2 The scope and main steps of verification and validation for automated driving systems
6.3 Key challenges for verification and validation of SAE L3 and SAE L4 automated driving systems
6.3.1 Challenge 1: Statistical demonstration of avoidance of unreasonable risk and a positive risk balance without driver interaction
6.3.2 Challenge 2: System safety with driver interaction (especially in takeover manoeuvres)
6.3.3 Challenge 3: Consideration of scenarios currently not known
6.3.4 Challenge 4: Validation of various system configurations and variants
6.3.5 Challenge 5: Validation of (sub)systems that are based on machine learning
6.4 Verification and validation approach for automated driving systems
6.4.1 Defining test goals and objectives (why and how well)
6.4.2 Test design techniques (how)
6.4.3 Test platforms (where)
6.4.4 Test strategies in response to the key challenges
6.4.4.1 Solution for challenge 1: Statistical demonstration of system safety and positive safety impact without driver/ operator interaction of ego-vehicle
6.4.4.2 Solution for challenge 2: Assessment of human driving performance (especially in takeover manoeuvres)
6.4.4.3 Solution for challenge 3: Consideration of scenarios currently not known in traffic
6.4.4.4 Solution for challenge 4: Validation of various system configurations and variants
6.4.4.5 Solution for challenge 5: Validation of (sub)systems that are based on machine learning

6.5 Quantity and quality of testing
6.5.1 Equivalence classes and scenario-based testing
6.6 Simulation
6.6.1 Types of simulation
6.6.2 Simulation scenario generation
6.6.3 Validating simulation
6.6.4 Further applications of simulation

6.7 Verification and validation of elements
6.7.1 A-priori information and perception (map)
6.7.2 Localization (including GNSS)
6.7.3 Environment perception sensors, V2X and sensor fusion
6.7.4 Interpretation and prediction, drive planning and traffic rules
6.7.5 Motion control
6.7.6 Monitor, ADS mode manager (including the vehicle state)
6.7.7 Human machine interaction and user state monitor
6.8 Field operation (monitoring, configuration, updates)
6.8.1 Testing traceability
6.8.2 Robust configuration and change management process
6.8.3 Regression prevention
6.8.4 Cybersecurity monitoring and updates
6.8.5 Continuous monitoring and corrective enforcement

Annex A (informative) Development examples

A.1 General
A.2 SAE level 3 traffic jam chauffeur system (TJCS)
A.3 SAE level 3 motorway chauffeur system (MCS)
A.4 SAE level 4 urban chauffeur system (UCS)
A.5 SAE level 4 automated valet parking systems (AVPS)
A.6 Selection of the discussed elements
A.6.1 Sensing elements for FS_1 localization
A.6.1.1 Traffic jam chauffeur system L3
A.6.1.2 Motorway chauffeur system L3
A.6.1.3 Urban chauffeur system L4
A.6.1.4 Automated valet parking systems L4
A.6.2 Sensing elements for FS_2 perceive relevant objects
A.6.2.1 Traffic jam chauffeur system L3
A.6.2.2 Motorway chauffeur system L3
A.6.2.3 Urban chauffeur system L4
A.6.2.4 Automated valet parking systems L4
A.6.3 Interpretation and prediction in FS_3 predict future movements
A.6.3.1 Traffic jam chauffeur system L3
A.6.3.2 Motorway chauffeur system L3
A.6.3.3 Urban chauffeur system L4
A.6.3.4 Automated valet parking systems L4
A.6.4 Acting elements in FS_5 execute driving plan and FD_6 perform ODD functional adaptation
A.6.4.1 Traffic jam chauffeur system L3
A.6.4.2 Motorway chauffeur system L3
A.6.4.3 Urban chauffeur system L4
A.6.4.4 Automated valet parking systems L4
A.6.5 ADS mode manager in FS_7 detect nominal performance and FD_4 react to insufficient performance
A.6.5.1 Traffic jam chauffeur system L3
A.6.5.2 Motorway chauffeur system L3
A.6.5.3 Urban chauffeur system L4
A.6.5.4 Automated valet parking systems L4
A.6.6 User state determination in FD_1 ensure controllability for driver
A.6.6.1 Traffic jam chauffeur system L3
A.6.6.2 Motorway chauffeur system L3
A.6.6.3 Urban chauffeur system L4
A.6.6.4 Automated valet parking systems L4
A.6.7 HMI in FD_1 ensure controllability for operator and FD_6 perform ODD functional adaptation
A.6.7.1 Traffic jam chauffeur system L3
A.6.7.2 Motorway chauffeur system L3
A.6.7.3 Urban chauffeur system L4
A.6.7.4 Automated valet parking systems L4
A.6.8 Monitors in FS_7 and FD_2
A.6.8.1 Traffic jam chauffeur system L3
A.6.8.2 Motorway chauffeur system L3
A.6.8.3 Urban chauffeur system L4

A.6.8.4 Automated valet parking systems L4

Annex B (informative) Using deep neural networks to implement safety-related elements for automated driving systems

B.1 General
B.2 Motivation and introduction: machine learning in automated driving
B.3 Define (what and why)
B.4 Specify (how)
B.4.1 Defining and selecting the data
B.4.1.1 Dataset labelling
B.4.2 Architecture design for DNNs
B.4.2.1 DNN-based software architecture level
B.4.2.2 DNN-only architecture level
B.5 Develop and evaluate
B.6 Deploy and monitor
B.6.1 General
B.6.2 The input data
B.6.3 The model behaviour
B.7 DNN safety artefacts

Annex C (informative) Principles of safety and cybersecurity for automated driving

Annex D (informative) List of proposed standards

Page count: 111