



DPC: 25/30488169 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 15 July 2025

Origin: International

Latest date for receipt of comments: 07 September 2025

Project No. 2024/00610

Responsible committee: AUE/15 Safety related to vehicles

Interested committees:

Title: Draft BS ISO 19725 Road vehicles - Steer-by-wire Systems - System Safety Guidelines.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 07 September 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 19725

Road vehicles — Steer-by-wire Systems — System Safety Guidelines

Véhicules routiers — Systèmes de direction électronique — Lignes directrices sur la sécurité du système

ICS: 43.040.99

ISO/TC 22/SC 33

Secretariat: **DIN**

Voting begins on:
2025-07-15

Voting terminates on:
2025-10-07

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS 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.

Reference number
ISO/DIS 19725:2025(en)

Full document details: 25/30488169 DC

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 List of symbols	4
5 Derivation of the safety goals	4
5.1 System boundary	4
5.2 SbW malfunctioning behaviours	7
5.3 Safety goals	8
5.3.1 General	8
5.3.2 Safety goal SG1: Self-steering shall be prevented while driving	9
5.3.3 Safety goal SG2: Loss of steerability shall be prevented while driving	10
5.3.4 Safety goal SG3: Loss of feedback torque to the driver shall be prevented while driving	11
5.3.5 Safety goal SG4: Unintentional blocking of the steering wheel shall be prevented while driving	12
5.3.6 Safety goal SG5: Unintended loss of synchronization between the SbW actuators shall be prevented while driving	13
6 System availability requirements	14
6.1 Availability requirements	14
6.2 Availability requirements after fault	15
6.3 Availability requirements for mechanical system parts	16
7 Controllability in the event of a first fault	16
7.1 Introduction and general information on controllability	16
7.2 Failure pattern	17
7.2.1 General	17
7.2.2 Malfunction behaviours	17
7.2.3 Failure source	17
7.2.4 Failure type	17
7.2.5 Failure characteristics with the associated physical values	18
7.2.6 Failure pattern with loss of actively generated feedback torque - supplementary instruction	23
7.3 Failure pattern matrix	24
7.4 Assessment of controllability in case of a fault	25
7.4.1 Failure pattern-driving maneuver combinations	26
7.4.2 Controllability thresholds	27
7.4.3 Subjective controllability assessment and related objective vehicle dynamics characteristics	27
7.5 Driving maneuvers and test execution for the assessment of controllability in the event of a fault	28
8 Minimum requirements for operation behavior after a fault	29
8.1 Introduction and general description of the degradation concept	29
8.2 Degradations and transitions	30
8.2.1 Normal operation N	30
8.2.2 Transition x-2 and Degradation 2	30
8.2.3 Transition 2-3 and Degradation 3	31
8.2.4 Transition x-emergency braking	31
8.2.5 Transition N-1 and Degradation 1	31
8.2.6 Transition x-3	31
8.3 General requirements of the degradation concept	32
8.3.1 Controllability during degradations and transitions	32

8.3.2	Electrical power supply system.....	32
8.3.3	Shortened transitions.....	32
8.3.4	Requirements for the vehicle lateral acceleration.....	32
8.3.5	Unrestricted continued driving before an automated speed reduction.....	33
8.3.6	Overriding the automated speed reduction and speed limiter.....	33
8.3.7	Braking during the automated speed reduction.....	34
8.4	Differentiation of vehicle systems.....	34
8.5	Minimum requirements for degradations and transitions.....	34
8.5.1	General.....	34
8.5.2	System integrity and speed limitations.....	35
8.5.3	Requirements for ASIL capability.....	41
8.5.4	Time-limited usage.....	42
8.5.5	Re-transitioning and its conditions.....	44
8.5.6	Requirements for the warning concept.....	47
8.5.7	Minimum requirements for lateral control and controllability of the vehicle.....	48
8.6	Maneuver sequences and their requirements.....	49
8.6.1	General explanations.....	49
8.6.2	Goals of the maneuver sequences and associated maneuver.....	49
8.6.3	General requirements.....	51
Annex A (informative) Driving manouvers for assessment of controllability.....		53
Annex B (informative) Tests to verify vehicle lateral control and controllability in the degradations and transitions.....		64
Annex C (informative) Development responsibility.....		90
Annex D (informative) Experience values from test series during the preparation of the standard.....		95
Annex E (informative) Explanation of degradation concept.....		98
Bibliography.....		104

Foreword

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

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, Subcommittee SC 33 "Vehicle dynamics, chassis components and driving automation systems testing".

A list of all parts in the ISO 19725 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Steer-by-Wire (SbW) systems represent the next generation of technology in vehicle steering. They enable new interior concepts and pave the way for further innovations in vehicle technology. In the context of automated driving, mechanical decoupling between the steering wheel and the steered wheels is becoming increasingly important. To date, there is no experience of widespread use of this technology in the market for large-series passenger cars.

Compared to conventional steering systems, SbW technology results in additional requirements for the safety concept of the vehicle for safe operation.

This document represents a description of a minimal set of safety aspects developed by vehicle manufacturers and system suppliers.

This document considers:

- the description and system boundary of an SbW system,
- basic safety goals,
- general availability requirements,
- requirements for controllability in the event of a first fault, and
- requirements for the operational behavior after a fault event.

Road vehicles — Steer-by-wire Systems — System Safety Guidelines

1 Scope

This document describes necessary but not sufficient safety requirements for the use of SbW systems in passenger cars and light commercial vehicles for series application.

This document does not replace the full application of the ISO 26262 [\[1\]](#) series of standards and their implementation in safety-related measures.

This document defines requirements for manual driving where the driver holds the steering wheel.

NOTE Misuse of hands-free driving is not considered.

This document does not contain requirements for the use of automated lateral vehicle control functions.

The requirements consider systems consisting of an Road wheel Actuator (RWA), Hand Wheel Actuator (HWA), and a steering wheel for driver input. Deviating concepts need to be analyzed by the user for transferability.

2 Normative references

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

ISO 4138:2021, *Passenger cars — Steady-state circular driving behaviour — Open-loop test methods*

ISO 15037-1:2019, *Road vehicles — Vehicle dynamics test methods — Part 1: General conditions for passenger cars*

ISO 17361:2017, *Intelligent transport systems — Lane departure warning systems — Performance requirements and test procedures*

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

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

ISO 26262-3:2018, *Road vehicles — Functional safety — Part 3: Concept phase*

ISO 26262-5:2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

3 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

degradation / degradation stage / DEG

operating conditions of the vehicle within the framework of the *degradation concept* ([3.2](#))

Note 1 to entry: Due to the operating condition of the steering system or supporting systems, a degradation condition can lead to restrictions in the use of the vehicle, e.g. speed limitations. Normal operation N is treated as degradation condition in this document.

3.2

degradation concept

all operating states of the vehicle, including the operating states of the steering system and the supporting vehicle systems after initial and subsequent faults

Note 1 to entry: Operating states include both transition and degradation states after faults, as well as the fault-free normal operation N.

3.3

drive cycle

time span from start to end of a trip

Note 1 to entry: In this document, the term is used in the context of re-transitioning between degradation states.

3.4

expert driver

person who has above-average vehicle dynamics knowledge, skills, ability to assess controllability, capability to conduct the vehicle tests and has regular driving experience

3.5

feedback torque

torque on the steering wheel

Note 1 to entry: An actively generated feedback torque occurs when at least one drive unit of the HWA is active. A passively generated feedback torque occurs when no drive unit of the HWA is active and the driver performs a steering wheel rotation. The feedback torque is used, among other things, to represent the steering feel.

3.6

Hand Wheel Actuator (HWA)

component(s) sensing the steering wheel angle and providing a *feedback torque* ([3.5](#))

3.7

immobilization

process in which a stationary vehicle is secured against rolling away

3.8

lane

lateral limited area for the movement of the vehicle, within which the driving task is to be accomplished

3.9

maneuver

specified road test

3.10

vehicle lateral maneuverability

ability of the vehicle to convert the steering wheel angle request of the driver into a minimal lateral motion reaction while driving below 10 km/h

3.11

maneuver sequence (MS)

specific sequence of maneuvers

3.12

normal driver

person who does not have special skills to drive a vehicle

Note 1 to entry: Used to distinguish from expert driver.

3.13

normal operation (N)

condition of the steering system and the supporting vehicle systems without safety-critical faults

Note 1 to entry: Minor, non-safety critical deviations within the nominal application range are permissible. The deviation of the behavior of the steering system and the vehicle relative to the nominal behavior is within the range expected by the driver.

3.14

passive fallback level (of the HWA)

Operating condition at which no active feedback torque is generated

Note 1 to entry: A passive fallback of an HWA could be mechanical base friction or a damping (e.g. electromagnetic, magneto-resistive, back EMF).

3.15

positive diagnostic re-check

diagnostic measure that confirms a previously detected fault is no longer present

3.16

Road wheel Actuator (RWA)

component(s) for actuating the required road wheel angle on the front axle

3.17

steerability

ability of the SbW system to convert the steering wheel angle request of the driver into a design-intended steering movement of the road wheels of the vehicle

3.18

system integrity

characteristics of the SbW system including ASIL capability to meet functional and availability requirements

Note 1 to entry: Functional requirements concern e.g. steering performance, feedback torque and synchronicity. Availability requirements concern e.g. redundancies to maintain steering capability.

Note 2 to entry: Degradation of steering performance or loss of redundancy may reduce the ASIL capability .

3.19

test configuration

combination of the configuration of the test vehicle (see Annex B, [B.2.2](#)) and the configurations of the respective vehicle systems (see Annex B, [B.2.3](#)) for the tests to demonstrate steerability or vehicle lateral control and controllability in the degradations and transitions

3.20

transition (TR)

change between degradation states

Note 1 to entry: A transition represents a time-limited state of a steering system and vehicle. Due to the system state of the steering system or supporting systems, a transition could lead to restrictions in the use of the vehicle, e.g. speed limits.

3.21

vehicle lateral control

ability of the vehicle to convert the steering wheel angle request of the driver into an expected vehicle trajectory according to the available friction coefficient between the tire and the road surface

Note 1 to entry: A trajectory change is also realized by other vehicle systems (e.g. brake, drivetrain, powertrain etc.) beyond the SbW system.

3.22**warning concept**

technical measures to warn the driver and the environment in case of faults

3.23**warning symbol**

standardized symbol for feedback to the driver of a failure or a degradation state of the SbW system

4 List of symbols**Table 1 — List of used symbols**

Vehicle lateral acceleration	a_y	m/s ²
Vehicle longitudinal acceleration	a_x	m/s ²
Distance	a	m
Vehicle width	B	m
Lane width	b	m
Wheelbase	L	m
Pylons distance	d	m
Circle radius	R/R_i	m
Track length	S	m
Vehicle speed	v_x	km/h
Vehicle speed at the beginning of the maneuver	$v_{x \text{ Start}}$	km/h
Vehicle speed at the end of the maneuver	$v_{x \text{ End}}$	km/h
Disturbance yaw rate	Δ	°/s
Disturbance lateral acceleration	Δa_y	m/s ²
Failure duration	t_{Failure}	s

5 Derivation of the safety goals**5.1 System boundary**

SbW is a steering system in which the driver's steering intention is detected by a sensor system and transmitted exclusively electrically to the actuator system to apply the road wheel angle. The steering feel is represented to the driver by means of an HWA.

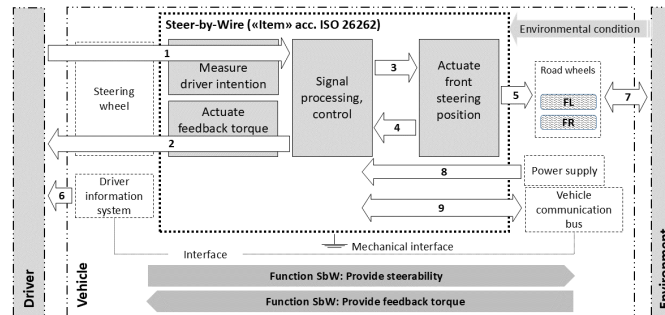
Compared with conventional steering systems (e.g. electromechanical steering, superimposed steering), there is no mechanical connection between the steering wheel and the steered wheels in an SbW system. This conceptual difference results in additional safety requirements and safety-related availability requirements for the steering system in the vehicle.

For an SbW system, steerability or vehicle lateral control shall be maintained during driving despite an electrical fault in the SbW system or in other supporting systems in the vehicle (e.g. vehicle power supply system, vehicle communication).

Figure 1 shows an example of the item SbW according to ISO 26262-1:2018 with the system boundaries of the item, the interfaces to the vehicle as well as functional elements. In addition, the control chains of the two main functions of an SbW system are also shown:

— Provide steerability and

— Provide feedback torque.



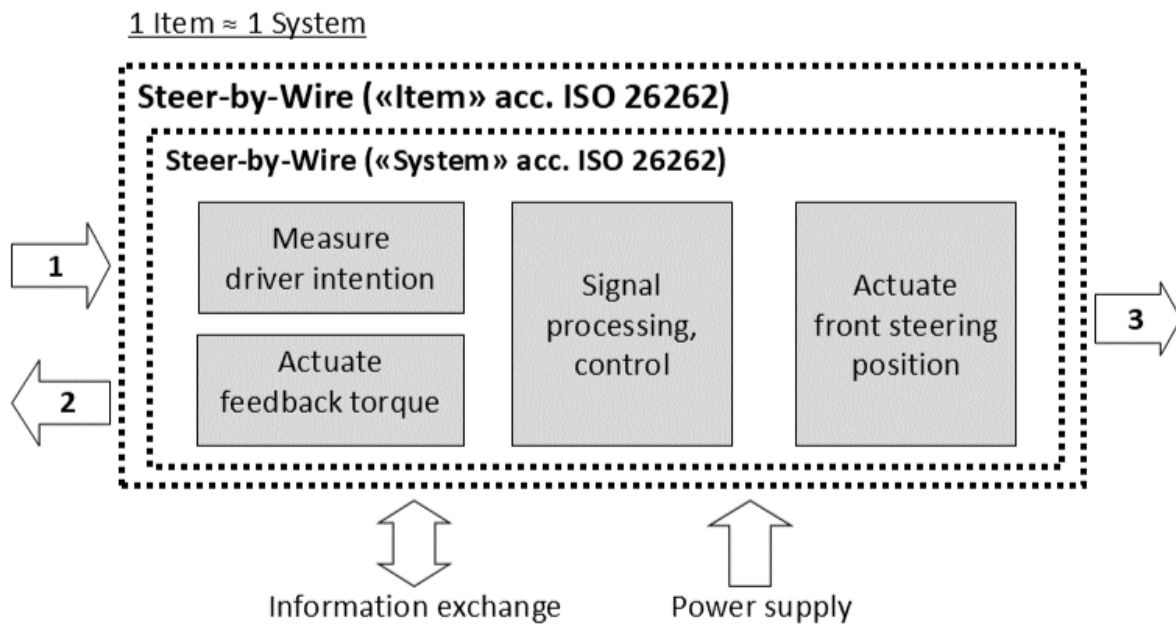
Key

- 1 Measurement of the driver's intention by measurement of the steering wheel angle
- 2 Actuation of feedback torque via feedback torque actuator and steering wheel (steering feel including haptic warning)
- 3 Target road wheel angle
- 4 Measured variables of actuators
- 5 Road wheel angle (transmission through the mechanical linkage via tie rod and steering linkage to the front wheels)
- 6 Visual or audible information and warnings from the SbW system
- 7 Interaction between wheels and road
- 8 Power supply
- 9 Information exchange

Figure 1 — Definition of item for SbW

An SbW system with the specified functions is defined as one item according to the definition in ISO 26262-1:2018 and ISO 26262-5:2018.

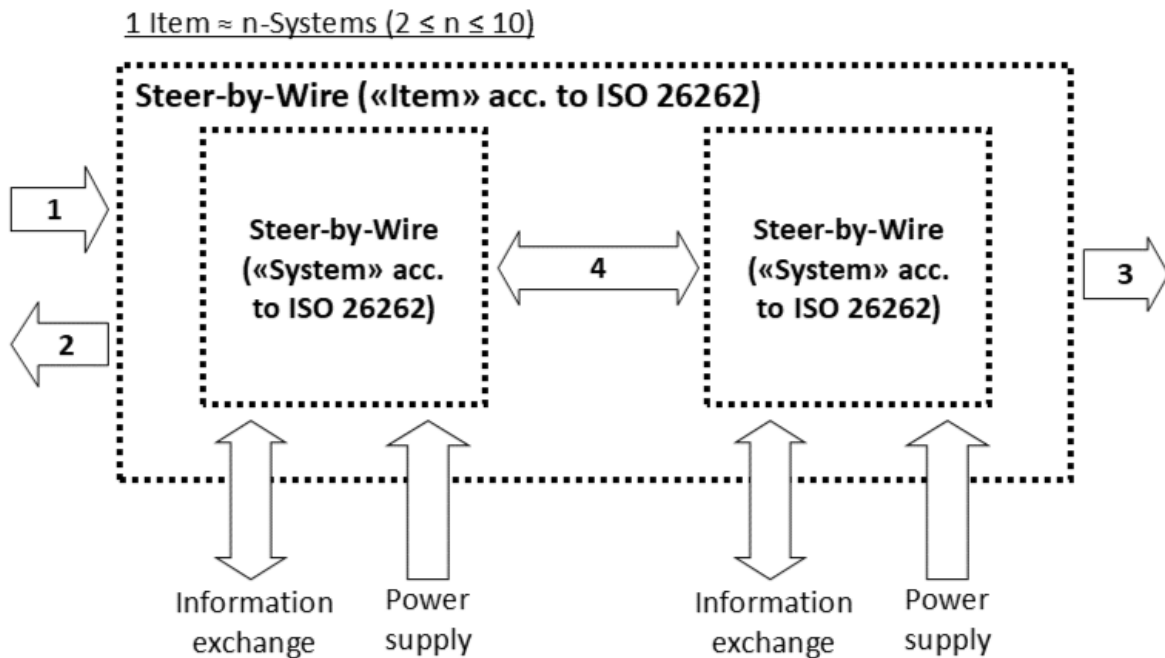
The item SbW can either be defined as one system or as a combination of several systems according to ISO 26262-1:2018 and ISO 26262-5:2018, see [Figure 2](#) and [Figure 3](#).



Key

- 1 Steering wheel angle input
- 2 Feedback torque (steering feel including warning)
- 3 Road wheel angle

Figure 2 — Option 1: Definition of system(s) SbW according to ISO 26262 [\[1\]](#)

**Key**

- 1 Steering wheel input
- 2 Feedback torque (steering feel including haptic warning)
- 3 Road wheel angle
- 4 Information exchange between systems

NOTE The definition "1 item = n systems ($2 \leq n \leq 10$)" follows the requirements of ISO 26262 [\[1\]](#).

Figure 3 — Option 2: Definition of system(s) SbW according to ISO 26262[\[1\]](#)

An example breakdown in physical system architecture(s) for both variants and for the share of development responsibilities between OEM and supplier is given in [Annex C](#).

5.2 SbW malfunctioning behaviours

Based on the functions of the SbW system listed in [5.1](#):

- Provide steerability and
- Provide feedback torque

the following SbW malfunctioning behaviours are considered:

- Self-Steering,
- Loss of steerability,
- Loss of feedback torque,
- Blocking of the steering system and
- Loss of synchronization between steering wheel angle and road wheel angle.

The malfunctioning behaviours are defined from driver's perspective, that means they represent a faulty behaviour as it can be experienced by the driver:

- "Self-steering" can occur if the road wheels are unintentionally moved
 - due to a fault in the function "Provide steerability" (e.g. faults in the measurement, signal processing, actuation) or
 - due to a fault in the function "Provide feedback torque" (e.g. faults in the measurement, signal processing, actuation) leading to an unintended movement of the steering wheel
- "Loss of steerability" can occur if the driver's intention is not actuated at the road wheels
- "Loss of feedback torque" can occur if no or insufficient torque is applied to the steering wheel
- "Blocking of the steering system" can occur if the forces to rotate the steering wheel are too high for the driver
- "Loss of synchronization between steering wheel angle and road wheel angle" can occur if the road wheel angle and steering wheel angle are misaligned, e.g. due to
 - delayed road wheel angle actuation
 - misalignment at vehicle wake-up

In addition to the above listed malfunctions, a complete analysis of all E/E malfunctions according to ISO 26262-3:2018 as well as mechanical failures shall be conducted for a specific SbW System.

5.3 Safety goals

5.3.1 General

The following safety goals and their criticality ratings are derived from the SbW malfunctioning behaviours listed in [5.2](#):

- SG1: Self-steering shall be prevented while driving.
- SG2: Loss of steerability shall be prevented while driving.
- SG3: Loss of feedback torque to the driver shall be prevented while driving.
- SG4: Unintentional blocking of the steering wheel shall be prevented while driving.
- SG5: Unintended loss of synchronization between the SbW actuators shall be prevented while driving.

The following [Table 2](#) shows the allocation of the SbW malfunctioning behaviours to the safety goals:

Table 2 — Allocation of SbW malfunctions to safety goals

Function of SbW system	SbW malfunction	Safety Goals
Provide steerability	Self-Steering (RWA)	SG1
	Loss of steerability Blocking of the steering system (RWA)	SG2
	Loss of synchronization between steering wheel angle and road wheel angle	SG5

Table 2 (continued)

Function of SbW system	SbW malfunction	Safety Goals
Provide feedback torque	Self-Steering (HWA)	SG1
	Loss of feedback torque	SG3
	Blocking of the steering system (HWA)	SG4

NOTE 1 In the context of the safety goals, "while driving" means that the vehicle is in a state where the driver has lateral and longitudinal control of the vehicle. The criticality (ASIL rating) of a safety goal violation is speed dependent. At very low speeds (e.g. 10 km/h with a corresponding warning concept), the risk is much lower than at higher speeds due to the significantly reduced kinetic energy.

NOTE 2 This document evaluates the criticality of the safety goals for E/E faults with Automotive Safety Integrity Level (ASIL) according to ISO 26262 [\[1\]](#).

NOTE 3 The SbW malfunction "blocking of the steering system" as per chapter [5.2](#) can be caused by blocking of the HWA (SG4) or blocking of the RWA (SG2)

The listed safety goals are not derived from a complete hazard analysis and risk assessment according to ISO 26262 [\[1\]](#) but are based on the generic failure modes. Therefore, the listed safety goals represent only a minimum set of safety goals.

This document does not relieve the user from performing a complete HARA according to ISO 26262-3:2018 for a specific SbW system.

5.3.2 Safety goal SG1: Self-steering shall be prevented while driving

5.3.2.1 Explanation

Self-steering is an unintended steering angle change (RWA and/or HWA) caused by a unintended force of the RWA or an unintended torque of the HWA. The safety goal is classified as ASIL D.

EXAMPLE Possible causes for an unintended RWA force or an unintended feedback torque including failures in the entire control path: sensors, communication, control and actuators. The type of unintended actuator control can follow different failure patterns, e.g. wrong amplitude, overshoot, wrong direction, superimposed, oscillating.

5.3.2.2 Acceptance criteria

Faults in an SbW system which may lead to the violation of the safety goal shall be mitigated in a suitable manner. It has to be ensured that the vehicle can be kept in the lane. (see [Clause 7](#)).

5.3.2.3 Safe state vehicle

The safe state on vehicle level for the function "Provide steerability" is reached when the vehicle speed is reduced to ≤ 10 km/h with a corresponding warning.

The safe state on vehicle level for the function "Provide feedback torque" is reached when general controllability (C0 controllability) is given or when the vehicle speed is reduced to ≤ 10 km/h with appropriate warning.

NOTE UN Regulation No. 79 [\[2\]](#) refers to the threshold of ≤ 10 km/h in the event of a fault. Depending on driving situations, furthermore the degradation concept defines the transition of the vehicle into vehicle standstill within the vehicle safe state.

When transitioning the vehicle to the safe state, the requirements of the degradation concept shall be met (see [Clause 8](#)).

The safe state at vehicle level can only be reached and ensured by considering systems outside the SbW system or considering the driver.

5.3.2.4 Safe state SbW system

The safe state on SbW system level for the function "Provide steerability" is to continue the operation of the function until the safe state is reached at the vehicle level. Faulty components shall be isolated or deactivated. Remaining required redundancies are to be activated or maintained.

The safe state on SbW system level for the function "Provide feedback torque" is to continue the operation of the function until the safe state at the vehicle level is reached or internal SbW mechanism exists where the functionality of the active feedback torque is no longer required for safety reasons. Faulty components shall be isolated or deactivated. Remaining required redundancies shall be activated or kept active or alternative mitigation measures must be applied.

EXAMPLE Example mitigation measures may be increased mechanical friction or damping.

In order to prevent violation of other safety goals, following additional measures shall be considered:

- Remaining redundant control and power supply channels shall be activated or kept active.
- Minimum steering performance according to the degradation concept shall be ensured.

5.3.3 Safety goal SG2: Loss of steerability shall be prevented while driving

5.3.3.1 Explanation

Loss of the steerability is a failure in the SbW system that leads to the loss of the function "Provide steerability" and cannot be sufficiently compensated by other systems for vehicle lateral control. The safety goal is classified as ASIL D.

EXAMPLE Possible failure causes for a failure of the steerability include the entire control path: sensors, communication, control, actuators, power supply, as well as mechanical components.

5.3.3.2 Acceptance criteria

In the event of faults in an SbW system which may lead to the violation of the safety goal shall be mitigated in a suitable manner. It shall be ensured that the vehicle can be kept in the lane. (see [Clause 7](#)). The minimum steering performance shall be ensured in accordance with the degradation concept (see [Clause 8](#)).

5.3.3.3 Safe state vehicle

The safe state on vehicle level is reached when the vehicle speed is reduced to $\leq 10\text{km/h}$ with appropriate warning.

NOTE 1 UN Regulation No. 79 [\[2\]](#) refers to the threshold of $\leq 10\text{ km/h}$ in the event of a fault. Depending on driving situations, furthermore the degradation concept defines the transition of the vehicle into vehicle standstill within the vehicle safe state. The safe state with corresponding driver warning is a sufficient risk mitigation according to ISO 26262 [\[1\]](#). The residual risk of a loss of steerability at vehicle speeds $\leq 10\text{km/h}$ with corresponding driver warning does not lead to an ASIL classification.

A minimum vehicle lateral maneuverability shall be ensured while continuing driving within the safe state. If steerability or vehicle lateral control is completely lost, an automated deceleration to standstill shall be executed as long as the automated deceleration is still operational (see [Clause 8](#)).

NOTE 2 Previous experiences indicate that drivers try to control the vehicle by more steering angle input, instead of immediately braking. The reaction of the driver to brake the vehicle to standstill can be delayed.

When transitioning the vehicle to the safe state, the requirements of the degradation concept shall be met (see [Clause 8](#)).

The safe state at vehicle level can only be reached and ensured by considering systems outside the SbW system or considering the driver.

5.3.3.4 Safe state SbW system

The safe state on SbW system level for the function "Provide steerability" is to continue the operation of the function until the safe state is reached at the vehicle level. Faulty components shall be isolated or deactivated. Remaining required redundancies shall be activated or maintained.

5.3.4 Safety goal SG3: Loss of feedback torque to the driver shall be prevented while driving

5.3.4.1 Explanation

Loss of feedback torque is a fault in the SbW system that results in a loss of the function "Provide feedback torque". The safety goal is classified as minimum ASIL B. The criticality for loss of feedback torque may vary depending on system design and characteristics of the transfer function (e.g. differences in friction, steering ratio).

EXAMPLE Possible failure causes for a loss of the feedback torque include the entire control path: sensors, communication, control, actuators, power supply, as well as mechanical components. The effect of faults can lead to a partial loss or even to a complete loss of the feedback torque.

5.3.4.2 Acceptance criteria

Two aspects regarding controllability shall be considered in case of faults leading to loss of feedback torque.

Faults in an SbW system that may lead to the violation of the safety goal shall be mitigated in an appropriate manner. It shall be ensured that the vehicle can be kept in the lane. (see [Clause 7](#)).

In addition, the remaining substitute functions (for example, redundancy, friction, damping) shall ensure controllability of the vehicle to continue driving (see [Clause 8](#)).

5.3.4.3 Safe state vehicle

The safe state on vehicle level is reached when general controllability (C0 controllability) is given or when the vehicle speed is reduced to ≤ 10 km/h with appropriate warning.

NOTE UN Regulation No. 79 [\[2\]](#) refers to the threshold of ≤ 10 km/h in the event of a fault. Depending on driving situations, furthermore the degradation concept defines the transition of the vehicle into vehicle standstill within the vehicle safe state. When transitioning the vehicle to the safe state, the requirements of the degradation concept shall be met (see [Clause 8](#)).

If the safe state cannot be achieved with general controllability, the safe state can only be reached and ensured at the vehicle level by considering systems outside the SbW system or considering the driver

5.3.4.4 Safe state SbW system

The safe state on SbW system level for the function "Provide feedback torque" is to continue the operation of the function until the safe state at the vehicle level is reached or internal SbW mechanism exists where the functionality of the active feedback torque is no longer required for safety reasons. Faulty components shall be isolated or deactivated. Remaining required redundancies shall be activated or kept active or alternative mitigation measures must be applied.

EXAMPLE Example mitigation measures may be increased mechanical friction or damping.

5.3.5 Safety goal SG4: Unintentional blocking of the steering wheel shall be prevented while driving

5.3.5.1 Explanation

An unintentional excessive feedback torque acting against the driver's steering wheel rotation (high steering resistance up to blocking of the HWA) shall be prevented. This includes both, electromechanically and mechanically caused high steering resistance up to blocking. The safety goal is classified as ASIL D.

EXAMPLE 1 Possible electromechanical faults causing excessive feedback torque include the entire control path: sensors, communication, control, actuators. Examples include simulation of the unintended dynamic end stop due to an incorrect steering angle or an unintended phase short-circuit in the HWA.

EXAMPLE 2 Possible mechanical causes for excessive feedback torque include the mechanical components, e.g., wrong mechanical end stop position leading to blocking or increased friction leading to high steering resistance.

NOTE SG4 differs from SG1. Fault leading to violation of SG4 will not lead to any active steering wheel rotation. The steering wheel rotation by the driver is inhibited or limited.

5.3.5.2 Acceptance criteria

Two aspects regarding controllability shall be considered in case of faults leading to unintentionally blocking of the steering wheel.

Faults in an SbW system that may lead to the violation of the safety goal shall be mitigated in a suitable manner. It shall be ensured that the vehicle can be kept in the lane. (see [Clause 7](#)).

In addition, the remaining substitute functions (for example redundancy, friction, damping) shall ensure controllability of the vehicle to continue driving (see [Clause 8](#)).

5.3.5.3 Safe state vehicle

The safe state on vehicle level is reached when general controllability (C0 controllability) is given or when the vehicle speed is reduced to ≤ 10 km/h with appropriate warning.

NOTE UN Regulation No. 79 [\[2\]](#) refers to the threshold of ≤ 10 km/h in the event of a fault. Depending on driving situations, furthermore the degradation concept defines the transition of the vehicle into vehicle standstill within the vehicle safe state.

When transitioning the vehicle to the safe state, the requirements of the degradation concept shall be met (see [Clause 8](#)).

If the safe state cannot be achieved by general controllability, the safe state can only be reached and ensured at the vehicle level by considering systems outside the SbW system or considering the driver.

5.3.5.4 Safe state SbW system

The safe state on SbW system level for the function "Provide feedback torque" is to continue the operation of the function until the safe state at the vehicle level is reached, or an internal SbW mechanism exists whereby the functionality of the active feedback torque is no longer required for safety reasons. Faulty components shall be isolated or deactivated. Remaining required redundancies shall be activated or kept active or alternative mitigation measures must be applied.

EXAMPLE Example mitigation measures may be increased mechanical friction or damping.

5.3.6 Safety goal SG5: Unintended loss of synchronization between the SbW actuators shall be prevented while driving

5.3.6.1 Explanation

An unintended and uncontrollable steering angle change or unintended and uncontrollable steering angle deviation due to a loss of synchronization between steering wheel angle and road wheel angle shall be prevented. The criticality of a loss of synchronization depends on the specific driving situation and the impact of the asynchronism. The safety goal is classified as ASIL D, because a high asynchronism while driving could potentially lead to loss of controllability or subsequently to further hazards like self-steering or blocking.

The user of this document can perform a detailed situation and functional analysis while performing the HARA for a specific SbW system and differentiate the malfunctioning behaviour into several safety goals with a corresponding ASIL rating. In this case the independency shall be demonstrated.

NOTE 1 If an SbW control concept includes functions to control the intended increase and decrease of asynchronism, those functions can potentially reduce the vehicle controllability.

EXAMPLE Causes that can lead to loss of synchronization include:

- Steering performance limitations of the RWA leading to delays at high steering dynamics,
- Communication or control faults leading to delays or latencies,
- Position bias between HWA and RWA due to sensor faults or mechanical offset,
- HWA and RWA position are not synchronized before vehicle launch,
- Blocking of the RWA due to external influences like road wheel hits high curb or stuck in deep ruts and
- Motion of the RWA due to high external forces.

NOTE 2 Relation between SG5 and SG1: a self-steering of the RWA, which might also lead to a loss of synchronization, is already covered by SG1.

Relation between SG5 and SG2: although SG5 is violated, a reduced level of steerability is provided, but the loss of synchronization can still result in uncontrollable trajectory deviations.

5.3.6.2 Acceptance criteria for SG5

During the development of an SbW system, it must be ensured that a potential loss of synchronization and their compensations are controllable. Faults in an SbW system that may lead to the violation of the safety goal shall be mitigated in a suitable manner. It must be ensured that the vehicle can be kept in the lane.

In case of an asynchronous position between RWA and HWA at start-up, the position between the two actuators shall be synchronized before driving, or other safety mechanism shall ensure the controllability when the vehicle is launched.

NOTE 1 The criticality while launching the vehicle with an asynchronous position between RWA and HWA depends on the results of the HARA for specific SbW design and may result in a lower ASIL than ASIL D.

The user of this document shall identify faults leading to loss of synchronization of a specific SbW system. Those faults shall be controllable by the driver and mitigated if required. It is recommended that the user of this document prepares a test catalog that considers the "worst case driving situations" (e.g., deep ruts, curbs, performance limitations, switching between steering modes).

NOTE 2 Loss of synchronization is not considered in the assessment of controllability in the event of a first fault in [Clause 7](#). A potential malfunction leading to aynchronism depends on a specific SbW system design and therefore a generic failure pattern is not defined in this document.

If an SbW control concept includes functions to control the intended increase and decrease of asynchronism, the control strategies shall not violate other safety goals and shall be controllable by the driver.

A partial consideration of aynchronism in the SbW steering system is given in [Clause 8](#). That clause defines the minimum requirements for steering performance and vehicle controllability to continue driving after a fault, depending on the actual state of degradation.

5.3.6.3 Safe state vehicle

The safe state on vehicle level is reached when the vehicle speed is reduced to $\leq 10\text{km/h}$ with appropriate warning.

NOTE UN Regulation No. 79 [\[2\]](#) refers to the threshold of $\leq 10\text{ km/h}$ in the event of a fault. Depending on driving situations, furthermore the degradation concept defines the transition of the vehicle into vehicle standstill within the vehicle safe state.

When transitioning the vehicle to the safe state, the requirements of the degradation concept shall be met (see [Clause 8](#)).

The safe state at vehicle level can only be reached and ensured by considering systems outside the SbW system or considering by the driver.

5.3.6.4 Safe state SbW system

The safe state on SbW system level for the function "Provide steerability" is to continue the operation of the function until the safe state is reached at the vehicle level. Faulty components shall be isolated or deactivated. Remaining required redundancies shall be activated or kept active or alternative mitigation measures (e.g., control strategies to mitigate loss of synchronization and maintain controllability) must be applied.

6 System availability requirements

6.1 Availability requirements

In the context of a fail-operational SbW system, two types of availability can be distinguished.

Concerning the "safety-related availability", the system availability is meant to allow the driver to reach the vehicle safe state in case of a fault.

In contrast, the "general availability" addresses the system availability which enhances the driver's ability to continue driving in case of faults not reducing ASIL capability, which is further described in [8.2.5](#)

For the derivation of the availability the following requirements, among others, shall be met:

- Safety-related availability requirements shall be derived from the safety goals of the HARA.

NOTE 1 Classification examples may include "fail safe" and "fail operational".

- Sufficient safety-relevant availability shall be available to achieve the safe states of the safety goals. This can be achieved via E/E redundancy, as shown in the example architectures in the [Clause C.3](#) described.

NOTE 2 In this document, this requirement relates to safety goals SG2 and SG3.

NOTE 3 The example architectures in the [Clause C.3](#) assume sufficient integrity of the E/E elements and their required diagnostics.

- The required energy shall be ensured to reach the safe state considering the degradation concept. The energy demand of the relevant vehicle systems during the transition to the safe state shall be considered.

- The system integrity (e.g., steering performance, feedback torque) required for steerability or lateral vehicle control and controllability in the degradations and transitions to the safe state shall be ensured as described in [Clause 8](#).

When considering the safety-relevant availability of the SbW system, the availability of supporting systems (e.g. vehicle power supply system, vehicle communication) is not specified in this document.

NOTE 4 The availability requirements for supporting systems need to be aligned with the availability requirements of the SbW system.

Regarding availability at vehicle level, alternative options for vehicle lateral control are permissible and may offer further potential.

NOTE 5 Alternative options for vehicle lateral control include unilateral brake intervention or rear wheel steering.

6.2 Availability requirements after fault

In the event of a fault that reduces the ASIL capability of the SbW system, the steerability and controllability of the vehicle shall be maintained to offer the driver sufficient time to transition the vehicle to a safe state (see [Clause 5](#)).

The available time for continued driving should allow the driver to safely stop in the sense of safely leaving the driving situation and reaching a safe parking position.

The following aspects shall be considered to determine the time for continued driving:

- Possible environmental conditions shall be considered which are relevant for a safe stop or for reaching a safe parking position when determining the minimum time for continued driving. In particular, the maximum lengths of bridges, tunnels, construction sites and the distances between highway exits shall be considered.

NOTE 1 Justified exceptions are permitted (e.g. in the case of low state of charge in the energy storage device).

- The requirements for "Emergency Operation" according to ISO 26262 [\[1\]](#) shall be applied when determining the maximum permissible time for continued driving.
- A safety factor for determining the maximum permissible time for continued driving shall be defined.
- A safety factor of the order of 10 is recommended.
- The maximum permissible upper limit of the time for continued driving is the shortest "Emergency Operation Tolerance Time Interval" (EOTTI, see ISO 26262-1:2018) with consideration of the defined safety factor.

NOTE 2 By defining the safety factor, the analyses and measures of ISO 26262 [\[1\]](#) are to be considered with respect to defects of the same type (e.g., component aging, systematic quality issues during manufacturing) as well as systematic defects. The recommended order of 10 is typically used in ISO 26262 [\[1\]](#) to differentiate between criticality levels.

In [Figure 4](#) the minimum target time for continued driving and example environmental conditions with times and driving distances are shown. In addition, the maximum possible time for continued driving is shown.

The time for continued driving should enable the driver to reach a suitable parking position. Earlier stopping by the driver shall be always possible.

The targeted time to continue driving may be limited by the availability of the supporting systems (e.g., power supply). This shall be considered when defining the continued driving time.

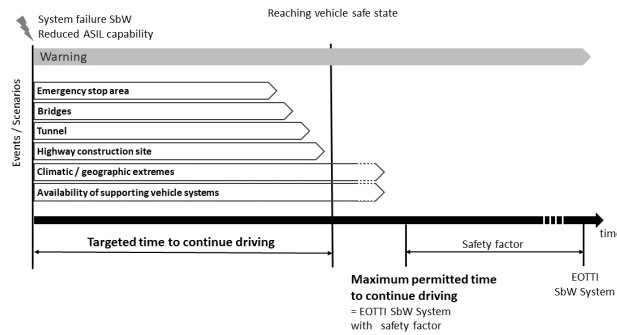


Figure 4 — Continuation time with reduced ASIL capability

EXAMPLE Examples for distances are:

- Emergency Stop Area: Japan 1,5 km
- Bridges: Lake Pontchartrain USA 42 km, Qingdao Jiaozhou Bay Bridge China 19 km
- Tunnel: Laredal Tunnel Norway 24,5 km, Gotthard Tunnel Switzerland 17 km
- Highway Construction Site: length 20 km with speed of 60 km/h resulting in 20 min driving

NOTE 3 Extreme climatic and geographic conditions (heat, cold, desert) may be considered when defining the continued driving time.

6.3 Availability requirements for mechanical system parts

Mechanical failures can cause critical hazards in SbW systems. The same methodologies as for conventional steering systems can be used to validate the system design and verify the mechanics.

NOTE 1 Methodologies to validate system design include robustness and reliability analyses.

NOTE 2 Mechanical subcomponents in the SbW system may require modified safety ratings compared to conventional steering systems.

7 Controllability in the event of a first fault

7.1 Introduction and general information on controllability

This clause defines the requirements for evaluating the controllability of the vehicle in the event of a first fault by executing vehicle tests. The vehicle tests deliver key inputs for the development of the safety mechanisms for the SbW system according to ISO 26262 [1].

The requirements consider the safety goals described in 5.3 and represent a minimum set of requirements for the controllability assessment.

Based on a specific SbW item and the corresponding completed HARA according ISO 26262-3:2018, the user of this document shall extend the controllability assessment for additional safety goals and safety requirements.

The vehicle tests to evaluate the controllability can be used as a base for verification and validation of the safety goals. The user of this document shall ensure completeness for the specific SbW design and related safety mechanisms.

7.2 Failure pattern

7.2.1 General

The failure patterns explained below are to be examined during the development of an SbW system, to evaluate system faults and their impact at vehicle-environment level or vehicle-driver level with respect to the controllability of the vehicle. A total of 11 failure patterns are considered (see [Table 3](#)).

NOTE Each of the following failure patterns will potentially result in the violation of a safety goal without an appropriate safety mechanism.

A failure pattern in the context of controllability assessment is composed of the malfunctioning behaviour, the failure source, the failure type, and the failure characteristic with the associated physical values (e.g. failure amplitude, duration or frequency). The failure characteristics consist of input values and controllability thresholds. The physical values are varied during the vehicle tests to determine the controllability threshold.

7.2.2 Malfunction behaviours

The safety goals from [5.3](#) are based on the following malfunctioning behaviours:

- Self-Steering,
- Loss of steerability,
- Loss of feedback torque,
- Blocking of the steering system and
- Loss of synchronization between steering wheel angle and road wheel angle.

The loss of synchronization between steering wheel angle and road wheel angle is not considered in the context of controllability in the event of a first fault since a generic failure pattern cannot be defined. Considerations on the assessment of controllability in the case of continued driving in the event of a fault are given in [Clause 8](#).

7.2.3 Failure source

For the assessment of the controllability of the vehicle at the malfunctioning behaviours from [7.2.2](#) the RWA and HWA are considered as failure sources. The effects of faults on the SbW system, such as faults in the power supply or in the communication network, are also considered as failure sources which are assigned to the RWA and HWA.

7.2.4 Failure type

7.2.4.1 Reversible failure

Reversible failures are failures whose fault effects shall be timely limited by the system's own safety mechanisms to ensure controllability.

The controllability threshold shall be determined depending on the applied malfunctioning behaviour, the failure source and the failure characteristics.

NOTE Safety mechanisms maintain the functionality, e.g. isolate or deactivate the faulty component(s) and activate or keep active the remaining redundancies.

EXAMPLE Reversible failure: Mitigation of selfsteering at the HWA by deactivating the faulty channel and switching to the remaining active or passive feedback torque.

7.2.4.2 Irreversible failure

Irreversible failures are failures where the system's safety mechanisms cannot promptly limit the failure effects, causing them to persist for a longer period.

The controllability threshold shall be determined depending on the applied malfunctioning behaviour, the failure source and the failure characteristics, whereby the fault duration shall be ≥ 2 s.

NOTE 1 Irreversible failures might not be detected by safety mechanisms.

EXAMPLE Irreversible failure: Selfsteering effect at the HWA due to constant torque offset caused by sensor bias.

NOTE 2 The impact of the failure on the vehicle behavior depends on the fault duration and the failure mode. The fault duration of ≥ 2 s was defined because shorter times are not sufficient to fully expose the fault and after this time the driver has adapted to the effect of a fault. The fault duration of ≥ 2 s is based on controllability assessments by expert drivers and confirmed in a subject study [\[3\]](#).

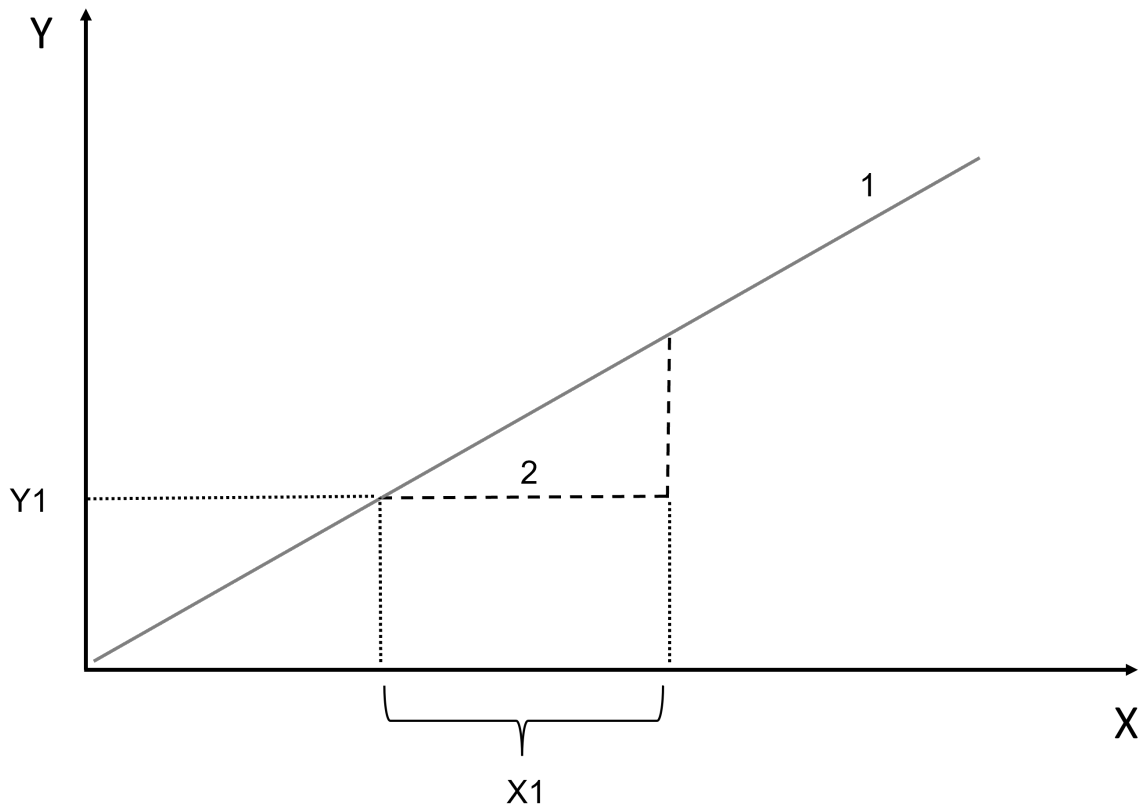
7.2.5 Failure characteristics with the associated physical values

7.2.5.1 Blocking

In the case of blocking (see [Figure 5](#)), a torque acts against the steering motion or steering wheel rotation, so that a steering motion or steering wheel rotation is prevented. In the case of blocking, only a reversible failure type is considered.

The frozen steering wheel angle is the input value of the controllability assessment for the blocking at the HWA. The frozen road wheel angle is the input value of the controllability assessment for the blocking at the RWA. The controllability threshold is the allowable fault duration.

In case of blocking, the actual value of the steering wheel angle or road wheel angle shall be kept constant over the duration of the fault, representing the input value.

**Key**

X	Time
Y	Angle
X1	Fault duration
Y1	Frozen steering wheel angle (HWA) / Frozen road wheel angle (RWA)
1	Reference without failure
2	Failure

Figure 5 — Schematic diagram of the failure characteristic "blocking"

7.2.5.2 Oscillation

Oscillation (see [Figure 6](#)) describes an oscillating torque curve at the HWA or an oscillating road wheel angle curve at the RWA. In the case of oscillation, only an irreversible failure type is considered.

NOTE 1 Oscillation was chosen as a substitutional failure characteristic to represent stochastic faults. It's only consider irreversible here due to oscillation usually appears to be longer than 2 s.

The characteristic of the oscillation shall be a rectangular shape.

NOTE 2 To investigate the driver-vehicle system behaviour, the oscillation shape is defined as:

- constant frequency
- symmetric amplitude
- pulse width is half of the period
- rectangular

A rectangular oscillation represents the most severe shape due to its step-like character. By choosing different oscillation shapes, different failure effects might occur.

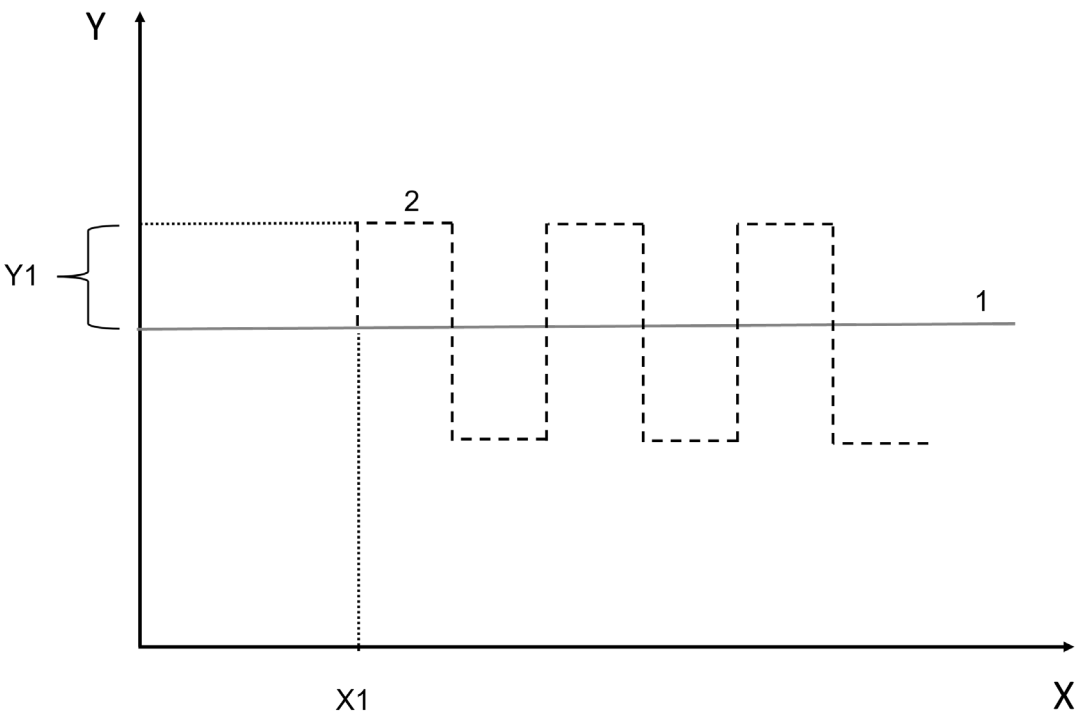
The fault duration of $t_{\text{fault}} \geq 2 \text{ s}$ and the failure frequency are the input values of the controllability assessment for the oscillation.

The frequency of the oscillation shall be pre-determined by vehicle test, to correspond approximately to the first resonance frequency of the driver-vehicle system.

NOTE 3 There are oscillation frequencies where the driver amplifies the effect of a failure. Typical oscillation frequencies are $\leq 1,5 \text{ Hz}$. The experience values listed in [Table D.1](#) are based on these oscillation frequencies. Usually, higher frequencies are not amplified by the driver.

The controllability threshold is the feedback torque amplitude at the HWA or the road wheel angle amplitude at the RWA.

In the case of oscillation, the actual value of the feedback torque or the road wheel angle shall be additively superimposed with the input value of the failure patterns.



Key

X	Time
Y	HWA torque / RWA angle
X1	Point of fault injection
Y1	Steering wheel torque amplitude (HWA) / Road wheel angle amplitude (RWA)
1	Reference without failure
2	Failure

Figure 6 — Schematic diagram of the failure characteristic "oscillation"

7.2.5.3 Step

The step describes a step-like change in the feedback torque by the HWA or a step-like change in the road wheel angle by the RWA. In the case of a step change, both reversible (see [Figure 7](#)) and irreversible (see

Figure 8) failure types are considered. To realize the step-like change, the maximum possible dynamics of the respective actuator shall be requested.

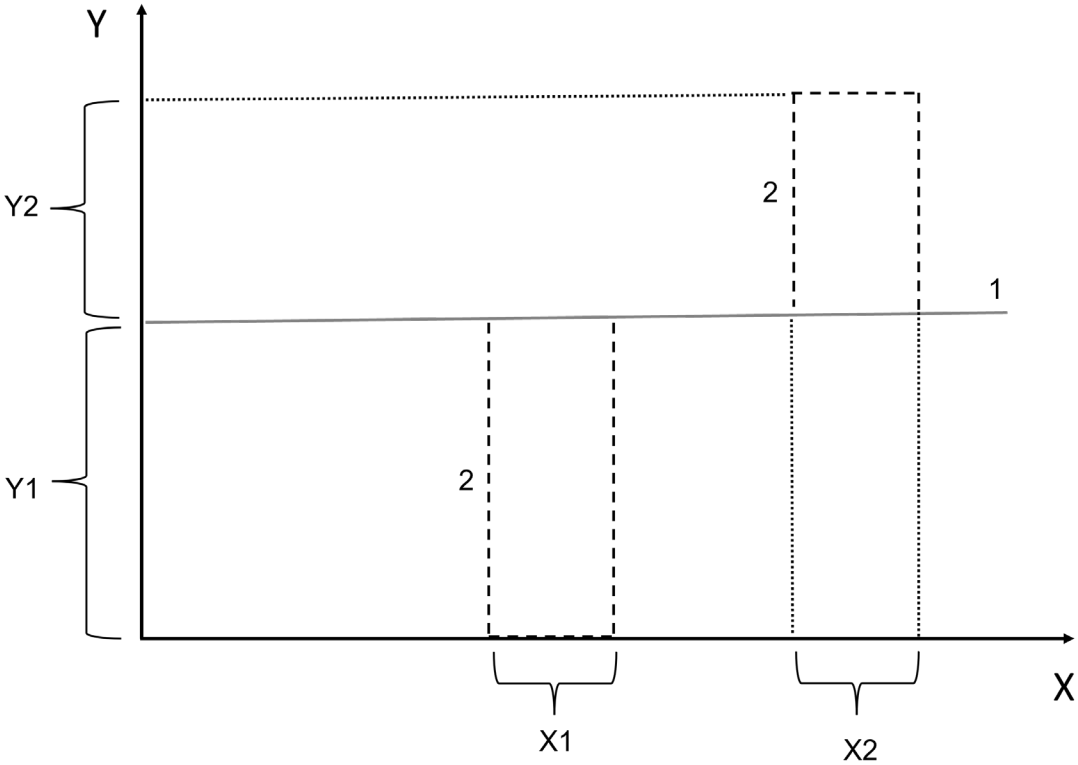
Reversible step

The maximum possible feedback torque demand is the input value of the controllability assessment for the reversible step at the HWA.

The maximum possible road wheel angle demand is the input value of the controllability assessment for the reversible step at the RWA. Another possible failure characteristic of the reversible step is the sudden loss of torque at the RWA. In this case the input value is a motor torque of 0 Nm for the reversible step at the RWA.

The controllability threshold of the reversible step is the permissible fault duration.

In the case of a reversible step change, the actual value of the feedback torque or the road wheel angle shall be replaced by the input value of the failure patterns.



Key

X	Time
Y	HWA torque / RWA torque or angle
X1	Fault duration
X2	Fault duration
Y1	Loss of RWA motor torque
Y2	Maximum steering wheel torque amplitude (HWA) / Maximum road wheel angle or torque amplitude (RWA)
1	Reference without failure
2	Failure

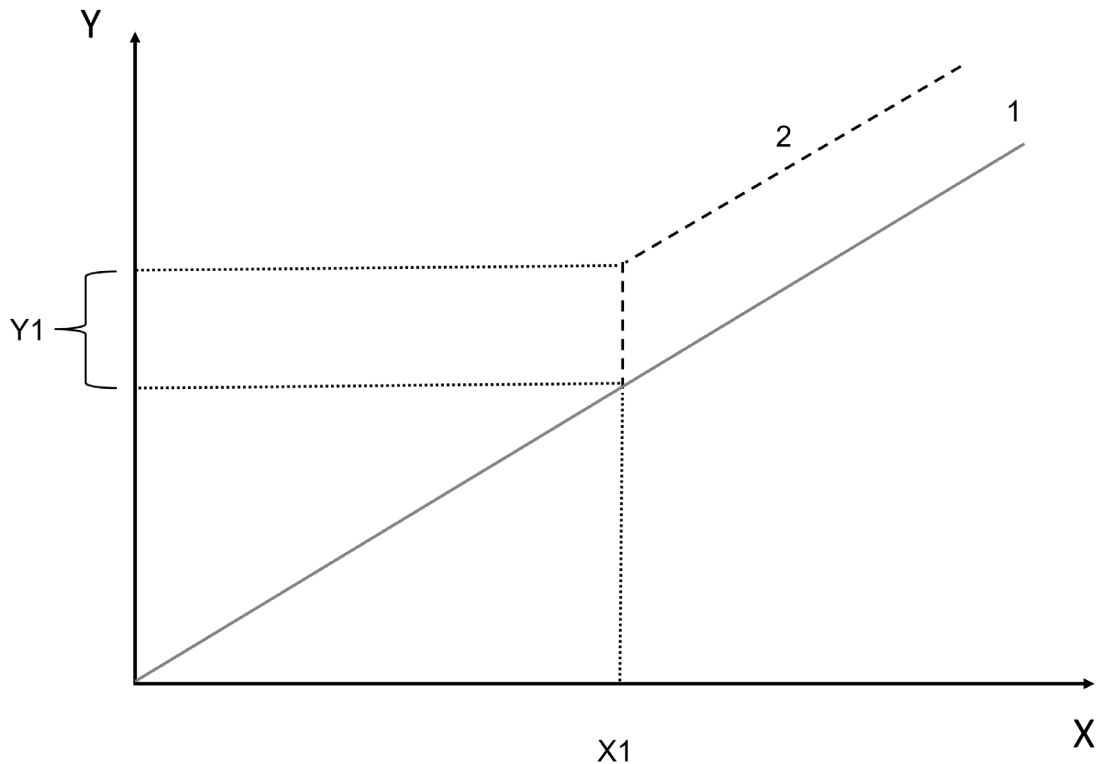
Figure 7 — Schematic diagram of the failure characteristic "reversible step"

Irreversible step

The fault duration of $t_{\text{fault}} \geq 2 \text{ s}$ is the input value of the controllability assessment for the irreversible step at the HWA or RWA.

The controllability threshold for an irreversible step at the HWA is the maximum controllable feedback torque request. The controllability threshold for an irreversible step at the RWA is the road wheel angle demand.

In the case of an irreversible step change, the actual value of the feedback torque or the road wheel angle shall be additively superimposed with the input value of the failure patterns.



Key

X	Time
Y	HWA torque / RWA angle
X1	Point of fault injection
Y1	Steering wheel torque amplitude (HWA) / Road wheel angle amplitude (RWA)
1	Reference without failure
2	Failure

Figure 8 — Schematic diagram of the failure characteristic "irreversible step"

7.2.5.4 Resistance

Steering resistance (see [Figure 9](#)), also known as steering effort, is a passively generated torque that counteracts the steering wheel rotation as a function of the steering wheel angular velocity. In the case of high steering resistance an irreversible failure type at the HWA is considered.

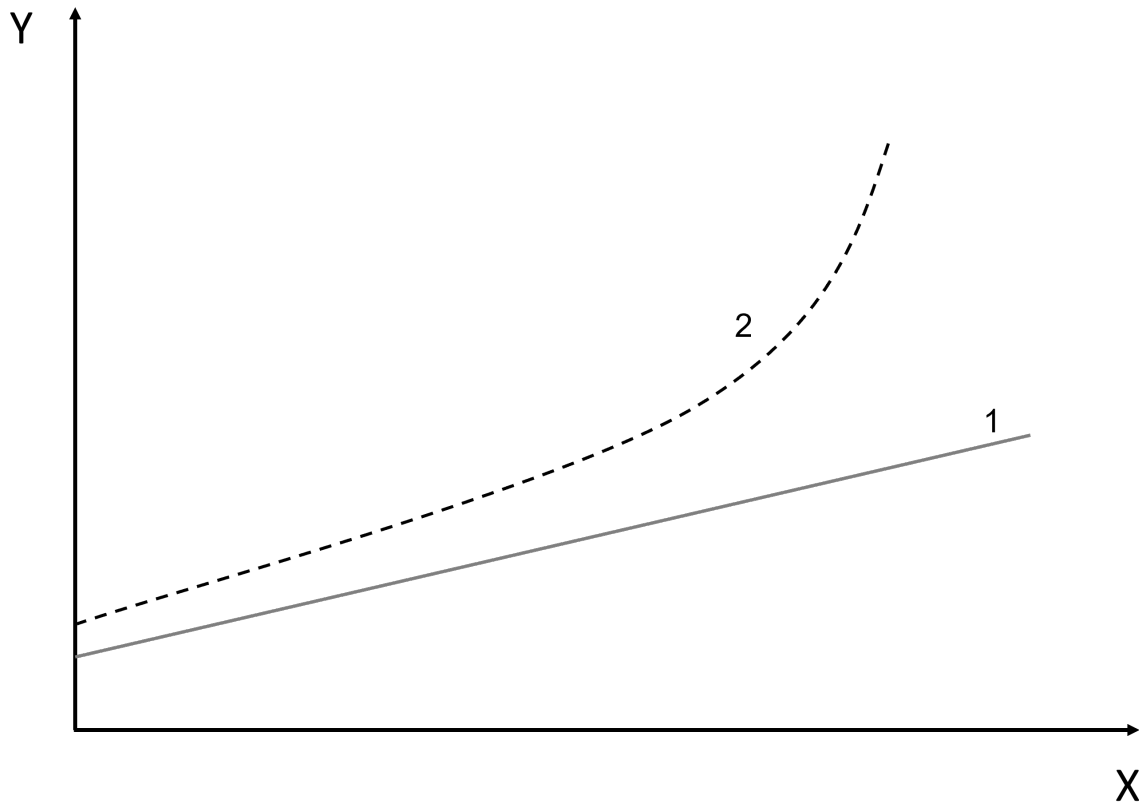
The fault duration of $t_{\text{fault}} \geq 2 \text{ s}$ is the input value of the controllability assessment for the high steering resistance at the HWA.

NOTE High steering resistance usually appears to be longer than 2 s, hence only irreversible failure types are considered. The worst case of high steering resistance as a reversible failure type is covered by the blocking failure characteristic.

The controllability threshold is the maximum controllable steering resistance (passive feedback torque) as a function of the steering wheel angular velocity.

In the case of high steering resistance, the actual value of the feedback torque shall be replaced by the input value of the failure pattern.

EXAMPLE High steering resistance is caused by an electrical defect in the HWA or by mechanical friction.



Key

X	Steering wheel angular velocity
Y	HWA torque
1	Reference without failure
2	Failure

Figure 9 — Schematic diagram of the failure characteristic "resistance"

7.2.6 Failure pattern with loss of actively generated feedback torque - supplementary instruction

The loss of the actively generated feedback torque of the HWA does not necessarily lead to a loss of controllability of the vehicle. Inherent passively generated feedback torque due to friction or damping in the HWA can maintain the controllability in the event of such a failure pattern (see 7.4).

However, this failure pattern shall be considered much more critical for a non-redundant HWA when the loss of the actively generated feedback torque follows an unintended self-steer (see Table 3, failure pattern 11). As a result the drive unit of the HWA is transferred to a passively generated feedback torque as the safe state. The failure pattern 11 is composed of:

- Phase 1: self-steering according to failure pattern 7, immediately followed by
- Phase 2: loss of the actively generated feedback torque.

As in failure pattern 7, the input value in phase 1 is the maximum feedback torque amplitude in the malfunctioning behaviour of self-steering. The controllability threshold in the malfunctioning behaviour self-steering is the fault duration.

Additionally the physical interactions between the two phases of failure pattern 11 shall be considered. Insufficient passively generated feedback torque generally can lead to lower controllability threshold of the fault duration in phase 1. If, for example, the fault duration cannot be limited further for technical reasons, additional measures shall ensure the controllability of the vehicle.

In the closed control loop driver-vehicle environment, an external fault is first followed by the driver's perception of the failure and then by the driver's compensation for the failure. In the case of failure pattern 11, the driver compensates not only for the direct consequences of a feedback torque step in the form of a deviation in the steering wheel angle, but also for a simultaneous change in the usual correlation between feedback torque change and steering angle change. The aim of the additional measures is to use passively generated feedback torque, for example in the form of friction or damping in the HWA, to reduce the demands on the driver's compensatory abilities and thereby ensure the controllability of the vehicle in the case of the failure pattern 11.

7.3 Failure pattern matrix

11 failure patterns were selected which are of particular importance regarding the controllability of the vehicle, combining malfunctioning behaviours, failure sources, failure type and the failure characteristics. The following [Table 3](#) lists the 11 failure patterns.

The controllability of the vehicle with these fault patterns shall be evaluated as described in [7.4](#).

Table 3 — Failure pattern matrix

Failure pattern	Malfunctioning behaviour	Safety Goal(s)	Failure source	Failure type	Failure characteristics	Input value	Control-lability threshold ^d
1	Blocking of the steering system	SG 4	HWA	irreversible	Resistance ^a	$t_{\text{Fault}} \geq 2 \text{ s}$	feedback torque against the steering wheel rotation by the driver as a function of the steering wheel angular velocity
2	Blocking of the steering system	SG 4	HWA	reversible	Blocking ^a	Frozen steering wheel angle	t_{Fault}
3	Loss of steerability	SG 2	RWA	reversible	Blocking ^a	Frozen road wheel angle	t_{Fault}
4	Loss of steerability	SG 2	RWA	reversible	Step ^b	Motor torque	t_{Fault}
5	Self-steering	SG 1	HWA	irreversible	Step ^c	$t_{\text{Fault}} \geq 2 \text{ s}$	feedback torque amplitude
6	Self-steering	SG 1	HWA	irreversible	Oscillation ^c	$t_{\text{Fault}} \geq 2 \text{ s}$	feedback torque amplitude, failure frequency

Table 3 (continued)

Failure pattern	Malfunctioning behaviour	Safety Goal(s)	Failure source	Failure type	Failure characteristics	Input value	Control-ability threshold ^d
7	Self-steering	SG 1	HWA	reversible	Step ^a	Max. feed-back torque amplitude (active) with max dynamics	t _{Fault}
8	Self-steering	SG 1	RWA	irreversible	Step ^c	t _{Fault} ≥ 2 s	Road wheel angle amplitude
9	Self-steering	SG 1	RWA	irreversible	Oscillation ^c	t _{Fault} ≥ 2 s	Road wheel angle amplitude, failure frequency
10	Self-steering	SG 1	RWA	reversible	Step ^a	Max. road wheel angle - amplitude (active) with max dynamics	t _{Fault}
11	Self-steering with subsequent loss of actively generated feedback torque	SG 1 and SG 3	HWA	Phase 1: Self steering	Step ^a	Phase 1: Self steering	
				reversible		Max. feed-back torque amplitude (active) with max dynamics	t _{Fault}
				Phase 2: Loss of active feedback torque		Phase 2: Loss of active feed-back torque	
				Not applicable ^e		t _{Fault} ≥ 2 s	Min. passively generated feedback torque
^a actual value during normal operation is replaced by input value ^b actual value during normal operation is replaced by input value 0 Nm ^c actual value during normal operation is additively superimposed with input value ^d the physical value is variied as an input during the vehicle tests to determine the controllability threshold ^e Phase 2 is the reaction to the malfunction behavior							

7.4 Assessment of controllability in case of a fault

The assessment of controllability in case of a fault delivers a key input to develop the safety mechanisms for the SbW system according ISO 26262 [\[1\]](#).

The controllability of the vehicle under the effect of an SbW-System fault (see [7.3](#)) shall be evaluated using specified driving maneuvers (see [7.5](#)).

The assessment of controllability must be conducted in a closed loop driver-vehicle setup within the corresponding environment, thus the driver's reaction to the failure pattern during the driving maneuver is considered.

The assessment of controllability shall be based on the assessment levels C0 (generally controllable), C1 (simply controllable), C2 (normally controllable) and C3 (difficult to control or uncontrollable) according to ISO 26262-3:2018.

NOTE In addition to the probability of occurrence and the possible extent of damage, the ASIL classification of safety-critical functions takes controllability in the event of potential faults into account as a classification criterion. In addition, controllability is used as an evaluation criterion for the effectiveness of safety mechanisms to mitigate fault effects (see ISO 26262 [11](#)).

7.4.1 Failure pattern-driving maneuver combinations

Failure pattern-driving maneuver combinations of particular relevance with regard to the controllability of the vehicle in the event of a fault shall be used for controllability assessments.

The following [Table 4](#) shows the selected failure pattern (see [7.3](#)) and the selected maneuvers (see [7.5](#)) as an overview of those combinations.

Table 4 — Combinations of selected failure patterns with driving maneuvers

Failure pattern	Malfunctioning behaviours	Failure source	Failure type	Failure characteristics	Maneuver		
					Straight ahead	Circular driving	Slalom
1	Blocking of the steering system	HWA	irreversible	Resistance	-	-	X
2	Blocking of the steering system	HWA	reversible	Blocking ^a	-	-	X
3	Loss of steerability	RWA	reversible	Blocking ^a	-	-	X
4	Loss of steerability	RWA	reversible	Step ^b	-	X	X
5	Self-steering	HWA	irreversible	Step ^c	X	-	X
6	Self-steering	HWA	irreversible	Oscillation ^c	X	X	-
7	Self-steering	HWA	reversible	Step ^a	X	X	-
8	Self-steering	RWA	irreversible	Step ^c	X	X	-
9	Self-steering	RWA	irreversible	Oscillation ^c	X	X	-
10	Self-steering	RWA	reversible	Step ^a	X	-	-
11	Self-steering with subsequent loss of actively generated feedback torque	HWA	reversible	Step ^a	X ^d	X	-

^a actual value during normal operation is replaced by input value

^b actual value during normal operation is replaced by input value 0 Nm

^c actual value during normal operation is additively superimposed with input value

^d test at 120 km/h and a lane width of 3,25 m