
**Road vehicles — Functional safety —
Part 7:
Production, operation, service and
decommissioning**

Véhicules routiers — Sécurité fonctionnelle —

Partie 7: Production, utilisation, maintenance et démantèlement

STANDARDSISO.COM : Click to view the full PDF of ISO 26262-7:2018



STANDARDSISO.COM : Click to view the full PDF of ISO 26262 7:2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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

Contents

Page

Foreword	iv
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Requirements for compliance	2
4.1 Purpose	2
4.2 General requirements	2
4.3 Interpretations of tables	3
4.4 ASIL-dependent requirements and recommendations	3
4.5 Adaptation for motorcycles	3
4.6 Adaptation for trucks, buses, trailers and semi-trailers	3
5 Planning for production, operation, service and decommissioning	4
5.1 Objectives	4
5.2 General	4
5.3 Inputs to this clause	4
5.3.1 Prerequisites	4
5.3.2 Further supporting information	4
5.4 Requirements and recommendations	5
5.4.1 Production planning	5
5.4.2 Pre-production	6
5.4.3 Planning of operation, service and decommissioning	6
5.5 Work products	8
6 Production	8
6.1 Objectives	8
6.2 General	8
6.3 Inputs to this clause	9
6.3.1 Prerequisites	9
6.4 Requirements and recommendations	9
6.4.1 Production	9
6.5 Work products	10
7 Operation, service and decommissioning	10
7.1 Objectives	10
7.2 General	10
7.3 Inputs to this clause	10
7.3.1 Prerequisites	10
7.3.2 Further supporting information	11
7.4 Requirements and recommendations	11
7.4.1 Operation, service and decommissioning	11
7.5 Work products	11
Annex A (informative) Overview on and document flow of production, operation, service and decommissioning	12
Bibliography	14

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 the 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 voluntary nature of standards, 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, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

This edition of ISO 26262 series of standards cancels and replaces the edition ISO 26262:2011 series of standards, which has been technically revised and includes the following main changes:

- requirements for trucks, buses, trailers and semi-trailers;
- extension of the vocabulary;
- more detailed objectives;
- objective oriented confirmation measures;
- management of safety anomalies;
- references to cyber-security;
- updated target values for hardware architecture metrics;
- guidance on model based development and software safety analysis;
- evaluation of hardware elements;
- additional guidance on dependent failure analysis;
- guidance on fault tolerance, safety related special characteristics and software tools;
- guidance for semiconductors;
- requirements for motorcycles;
- general restructuring of all parts for improved clarity.

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.

A list of all parts in the ISO 26262 series can be found on the ISO website.

STANDARDSISO.COM : Click to view the full PDF of ISO 26262-7:2018

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles.

This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

Safety is one of the key issues in the development of road vehicles. Development and integration of automotive functionalities strengthen the need for functional safety and the need to provide evidence that functional safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures, these being considered within the scope of functional safety. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes.

To achieve functional safety, the ISO 26262 series of standards:

- a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;
- b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASILs)];
- c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;
- d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and
- e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with functional safety of E/E systems that is achieved through safety measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and the management processes.

Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

[Figure 1](#) shows the overall structure of the ISO 26262 series of standards. The ISO 26262 series of standards is based upon a V-model as a reference process model for the different phases of product development. Within the figure:

- the shaded “V”s represent the interconnection among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;
- for motorcycles:
 - ISO 26262-12:2018, Clause 8 supports ISO 26262-3;
 - ISO 26262-12:2018, Clauses 9 and 10 support ISO 26262-4; and
- the specific clauses are indicated in the following manner: “m-n”, where “m” represents the number of the particular part and “n” indicates the number of the clause within that part.

EXAMPLE “2-6” represents ISO 26262-2:2018, Clause 6.

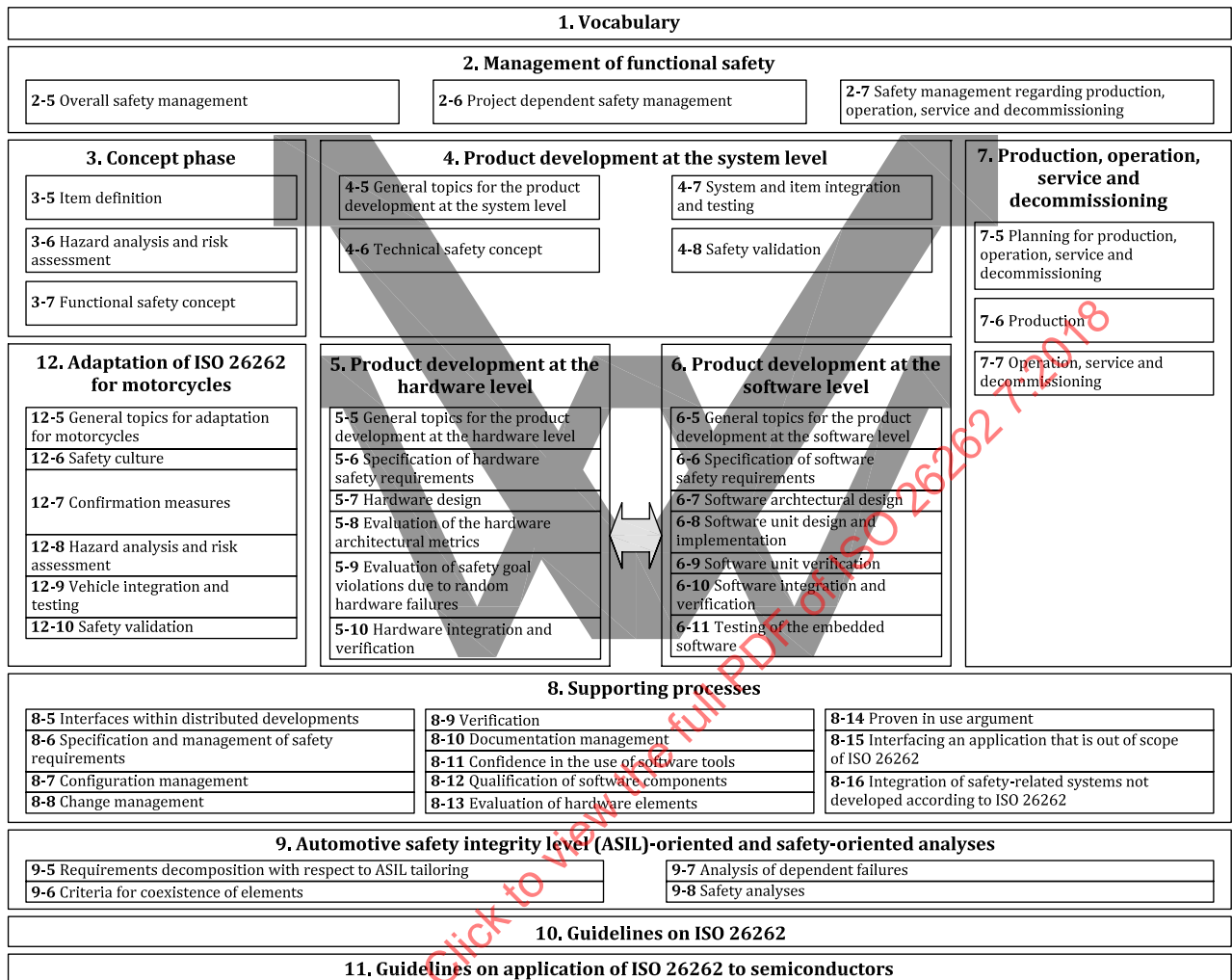


Figure 1 — Overview of the ISO 26262 series of standards

STANDARDSISO.COM : Click to view the full PDF of ISO 26262-7:2018

Road vehicles — Functional safety —

Part 7:

Production, operation, service and decommissioning

1 Scope

This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed according to this document and systems developed according to this document by tailoring the safety lifecycle.

This document addresses possible hazards caused by malfunctioning behaviour of safety-related E/E systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of safety-related E/E systems.

This document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document does not address the nominal performance of E/E systems.

This document specifies the requirements for production, operation, service and decommissioning, including related planning activities.

[Annex A](#) provides an overview on objectives, prerequisites and work products of this document.

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

ISO 26262-2:2018, *Road vehicles — Functional safety — Part 2: Management of functional safety*

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

ISO 26262-4:2018, *Road vehicles — Functional safety — Part 4: Product development at the system level*

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

ISO 26262-8:2018, *Road vehicles — Functional safety — Part 8: Supporting processes*

ISO 26262-9:2018, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

3 Terms and definitions

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1 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 <https://www.iso.org/obp>

4 Requirements for compliance

4.1 Purpose

This clause describes how:

- a) to achieve compliance with the ISO 26262 series of standards;
- b) to interpret the tables used in the ISO 26262 series of standards; and
- c) to interpret the applicability of each clause, depending on the relevant ASIL(s).

4.2 General requirements

When claiming compliance with the ISO 26262 series of standards, each requirement shall be met, unless one of the following applies:

- a) tailoring of the safety activities in accordance with ISO 26262-2 has been performed that shows that the requirement does not apply; or
- b) a rationale is available that the non-compliance is acceptable and the rationale has been evaluated in accordance with ISO 26262-2.

Informative content, including notes and examples, is only for guidance in understanding, or for clarification of the associated requirement, and shall not be interpreted as a requirement itself or as complete or exhaustive.

The results of safety activities are given as work products. “Prerequisites” are information which shall be available as work products of a previous phase. Given that certain requirements of a clause are ASIL-dependent or may be tailored, certain work products may not be needed as prerequisites.

“Further supporting information” is information that can be considered, but which in some cases is not required by the ISO 26262 series of standards as a work product of a previous phase and which may be made available by external sources that are different from the persons or organizations responsible for the functional safety activities.

4.3 Interpretations of tables

Tables are normative or informative depending on their context. The different methods listed in a table contribute to the level of confidence in achieving compliance with the corresponding requirement. Each method in a table is either:

- a) a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3), or
- b) an alternative entry (marked by a number followed by a letter in the leftmost column, e.g. 2a, 2b, 2c).

For consecutive entries, all listed highly recommended and recommended methods in accordance with the ASIL apply. It is allowed to substitute a highly recommended or recommended method by others not listed in the table, in this case, a rationale shall be given describing why these comply with the corresponding requirement. If a rationale can be given to comply with the corresponding requirement without choosing all entries, a further rationale for omitted methods is not necessary.

For alternative entries, an appropriate combination of methods shall be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation should be preferred. A rationale shall be given that the selected combination of methods or even a selected single method complies with the corresponding requirement.

NOTE A rationale based on the methods listed in the table is sufficient. However, this does not imply a bias for or against methods not listed in the table.

For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:

- “++” indicates that the method is highly recommended for the identified ASIL;
- “+” indicates that the method is recommended for the identified ASIL; and
- “o” indicates that the method has no recommendation for or against its usage for the identified ASIL.

4.4 ASIL-dependent requirements and recommendations

The requirements or recommendations of each sub-clause shall be met for ASIL A, B, C and D, if not stated otherwise. These requirements and recommendations refer to the ASIL of the safety goal. If ASIL decomposition has been performed at an earlier stage of development, in accordance with ISO 26262-9:2018, Clause 5, the ASIL resulting from the decomposition shall be met.

If an ASIL is given in parentheses in the ISO 26262 series of standards, the corresponding sub-clause shall be considered as a recommendation rather than a requirement for this ASIL. This has no link with the parenthesis notation related to ASIL decomposition.

4.5 Adaptation for motorcycles

For items or elements of motorcycles for which requirements of ISO 26262-12 are applicable, the requirements of ISO 26262-12 supersede the corresponding requirements in this document. Requirements of ISO 26262-2 that are superseded by ISO 26262-12 are defined in Part 12.

4.6 Adaptation for trucks, buses, trailers and semi-trailers

Content that is intended to be unique for trucks, buses, trailers and semi-trailers (T&B) is indicated as such.

5 Planning for production, operation, service and decommissioning

5.1 Objectives

The objectives of this clause are:

- a) to develop and maintain a production process for safety-related elements or items that are intended to be installed in road vehicles; and

NOTE This objective can be achieved by an organization's compliance to IATF 16949 or equivalent, depending on the organization's position in the safety supply chain and the complexity of the safety-related element being produced.

- b) to develop the necessary information concerning operation, service (maintenance and repair) and decommissioning for users who interface with the safety-related items or elements in order to ensure that functional safety is achieved throughout the lifecycle of the vehicle.

5.2 General

The requirements and recommendations of this clause apply to the planning of production, operation, service and decommissioning of items and elements including their installation in the vehicle.

To achieve functional safety, it is necessary to comply with safety-related special characteristics of items or elements during their production. These special characteristics are identified during the development phases. Examples of such safety-related special characteristics are specific process parameters (e.g. temperature range for reflow or fastening torque), material characteristics, production tolerances and configuration of elements.

This clause includes requirements to ensure that functional safety is achieved during the production process by including these safety-related special characteristics in production planning and control.

This clause also includes requirements related to developing service information and user information (including the user manual); the planning, execution and monitoring of maintenance work; repair instructions; decommissioning instructions; and instructions and information for rescue services.

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

- specification of requirements related to production, operation, service and decommissioning in accordance with ISO 26262-4:2018, 6.5.5, and ISO 26262-5:2018, 7.5.4;
- specification of dedicated measures for hardware in accordance with ISO 26262-5:2018, 9.5.2; and
- warning and degradation strategy, included in the functional safety concept in accordance with ISO 26262-3:2018, 7.5.1.

5.3.2 Further supporting information

The following information can be considered:

- production plan (from an external source);
- production control plan (from an external source); and
- relevant aspects of the technical specifications or designs at the system, software or hardware level.

5.4 Requirements and recommendations

5.4.1 Production planning

5.4.1.1 The production process shall be planned for the item and its elements by considering the following:

- a) the requirements for production;

EXAMPLE 1 Assembly instructions (e.g. calibration and setup of a sensor).

EXAMPLE 2 IPC (Institute of Printed Circuits) standard requirements.

- b) safety related special characteristics;

EXAMPLE 3 Tolerance for the selection of elements.

EXAMPLE 4 End of line calibration of inclination sensor.

- c) the conditions for the handling and management of elements;

EXAMPLE 5 Allowed storage time for a hardware element.

EXAMPLE 6 Correct programming of the ECU software.

- d) the configurations defined during product development;

- e) the lessons learned from previously released production plans;

- f) the suitability of the production process, equipment, tools and test equipment concerning the safety-related special characteristics; and

- g) the competence of the personnel.

5.4.1.2 The production plan shall describe the production steps, sequence and methods required to ensure that functional safety of the item or elements is achieved. It shall include:

- a) the production process flow and instructions;

NOTE The production process can also include rework of elements.

EXAMPLE 1 Instruction for rework of defect solder joints for components with three or fewer pins.

- b) the production tools and equipment;

- c) the implementation of the traceability measures; and

EXAMPLE 2 Labelling of elements.

- d) the implementation of dedicated measures in accordance with ISO 26262-5:2018, 9.5.2, if applicable.

5.4.1.3 A procedure shall be defined to ensure that the correct version of the embedded software and its associated calibration data is programmed onto the ECUs as part of the production process.

EXAMPLE 1 The use of a checksum, so that the checksum of the loaded executable and calibration data is compared to the correct checksum for the particular vehicle configuration.

EXAMPLE 2 Read back of the part number from the software loaded into the ECUs and comparison with the target part number for that specific vehicle from the bill of materials; as well as read back and comparison of the loaded calibration data with the calibration data for that specific vehicle from the bill of materials.

5.4.1.4 Reasonably foreseeable production process failures and their effects on functional safety shall be identified and the appropriate measures implemented to address the relevant process failures.

EXAMPLE Process Failure Modes and Effects Analysis (PFMEA).

5.4.1.5 When developing the production control plan, the control descriptions (with their criteria) for the item or elements and the safety-related special characteristics shall be considered.

5.4.1.6 The sequence and methods of the control steps shall be described in the production control plan, as well as the necessary test equipment, tools and test criteria.

5.4.1.7 Safety requirements identified during the planning for production shall be directed to the persons responsible for the system, hardware and software development as appropriate in accordance with ISO 26262-2:2018, Clause 6.

EXAMPLE Adding a mistake-proofing feature (poka-yoke) in a connector to ensure it is plugged into the ECU correctly during assembly.

5.4.1.8 Changes to the production, operation, service and decommissioning, impacting the item or its elements, shall be managed in accordance with the requirements in ISO 26262-8:2018, Clause 8.

5.4.2 Pre-production

5.4.2.1 The pre-production process and its control measures should be representative of the target series production process.

NOTE Pre-production is production of items or elements before release for production.

5.4.2.2 Differences between the pre-production process and the target series production process can be analysed in order to determine if the capability of the production process can be obtained during the pre-production stage.

NOTE 1 If the pre-production process is the same as the target series production process, the capability of the production process according to [6.4.1.3](#) can be obtained during pre-production.

NOTE 2 Differences can include the production rate, the sequence and methods of the production or control steps, test equipment, and tools.

5.4.3 Planning of operation, service and decommissioning

5.4.3.1 The operation, service and decommissioning processes shall be planned for the item by considering the following:

- a) the requirements for maintenance and repair;
- b) the requirements for the information necessary to ensure the safe operation of the vehicle, which shall be made available to the user (see [5.4.3.4](#));
- c) the requirements for decommissioning;
- d) the requirements for emergency rescue services;
- e) the warning and degradation strategy;
- f) the field monitoring process (see [7.4.1.1](#));
- g) the conditions for handling of elements;

EXAMPLE 1 Allowed storage time for a hardware element.

EXAMPLE 2 Correct flashing of software onto an ECU.

- h) the configurations defined in the release for production documentation; and

EXAMPLE 3 Allowed configurations of hardware, software and software calibration data during repair.

- j) the competence of the personnel involved.

5.4.3.2 The service plan shall describe the sequence and methods of the maintenance activities performed on an item or element including maintenance intervals and required tools.

5.4.3.3 The instructions for service shall describe the following:

- a) the procedures, methods, work steps and diagnostic routines;
- b) tools and equipment;

EXAMPLE 1 Programming, sensor calibration and diagnostic equipment.

- c) the sequence and methods of the control steps and control criteria used to verify the safety-related special characteristics;
- d) the relevant configurations of the item or elements including the traceability measures;

NOTE This includes service tool features used to ensure that the correct version of software is loaded into the vehicle, if such an operation is performed during service.

EXAMPLE 2 Labelling of an element ensuring traceability.

- e) the allowed deactivation of the item or elements and any consequential changes to the vehicle;
- f) the driver information necessary when deactivations and changes are made; and

EXAMPLE 3 Notifying the driver that an assistance function has been deactivated.

- g) the supply of replacement parts.

5.4.3.4 User information, including the user manual, shall provide relevant instructions and warnings concerning the proper use of the item or element, as well as the following information if applicable:

- a) a description of the relevant functions (i.e. the intended use, the status information or user interaction) and their operating modes;
- b) a description of the customer actions required to ensure controllability in the case of a failure indicated by the warning and degradation strategy;
- c) a description of the service activities expected from the customer in the case of a failure indicated by the warning and degradation strategy;
- d) the warnings regarding known hazards resulting from interactions with third party products; and

EXAMPLE 1 The user needs to be made aware that the parking assist can no longer scan behind the vehicle when using an additional third party tow hitch with a trailer.

- e) the warnings regarding the proper use of safety-related novel vehicle functions to prevent misunderstanding or misuse by drivers.

EXAMPLE 2 A misuse of an automatic parking brake when compared to a manual parking brake can lead to a driver leaving the vehicle without engaging the parking brake.

5.4.3.5 The decommissioning instructions shall describe the activities and measures to be applied during disassembly to ensure a safe decommissioning of the item or its elements.

EXAMPLE Instructions for the deactivation of airbags before the disassembly of the vehicle to avoid harm to the decommissioning personnel.

5.4.3.6 Safety requirements identified during the planning for operation, service and decommissioning shall be directed to the persons responsible for the system, hardware or software development as appropriate in accordance with ISO 26262-2:2018, Clause 6.

EXAMPLE Software specification of an error logging function in the ECU to ease diagnosis during service.

5.4.3.7 Information for rescue services, including rescue instruction sheet or emergency rescue guide, shall provide relevant instructions and warnings to avoid hazards during rescue operations, if applicable.

EXAMPLE Information to prevent unexpected airbag deployment or electrical injuries.

5.5 Work products

5.5.1 Safety-related content of the production plan resulting from requirements [5.4.1.1](#), [5.4.1.2](#), [5.4.1.3](#) and [5.4.1.4](#).

5.5.2 Safety-related content of the production control plan, including the test plan, resulting from requirements [5.4.1.5](#) and [5.4.1.6](#).

5.5.3 Producibility requirements specification resulting from requirement [5.4.1.7](#).

NOTE This specification can be included in the relevant documentation of the corresponding phases.

5.5.4 Production process capability report resulting from requirement [5.4.2.2](#).

5.5.5 Safety-related content of the service plan resulting from requirements of [5.4.3.1](#) to [5.4.3.3](#).

5.5.6 Safety-related content of the service instructions resulting from requirement [5.4.3.3](#).

5.5.7 Safety-related content of the information made available to the user resulting from requirement [5.4.3.4](#).

5.5.8 Safety-related content of the decommissioning instructions resulting from requirement [5.4.3.5](#).

5.5.9 Operation, service and decommissioning requirements specification, resulting from requirement [5.4.3.6](#).

NOTE This specification can be included in the relevant documentation of the corresponding phases.

5.5.10 Safety-related content of the rescue services instructions resulting from requirement [5.4.3.7](#).

6 Production

6.1 Objectives

The objective of this clause is to ensure that functional safety is achieved during the production phase (after release for production) by the relevant manufacturer or the person or organization responsible for the production process of items and elements (vehicle manufacturer, supplier, sub-supplier, etc.).

6.2 General

The requirements and recommendations of this clause apply to the production of items and elements including their installation in the vehicle.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

- release for production report in accordance with ISO 26262-2:2018, 6.5.6;
- safety-related content of the production plan in accordance with [5.5.1](#);
- safety-related content of the production control plan, including the test plan, in accordance with [5.5.2](#);
- producibility requirements specification in accordance with [5.5.3](#), if applicable; and
- production process capability report in accordance with [5.5.4](#), if applicable.

6.4 Requirements and recommendations

6.4.1 Production

6.4.1.1 The production process and its control measures shall be implemented and maintained as planned in accordance with [5.4.1](#).

NOTE This includes the appropriate training of the personnel involved in production.

6.4.1.2 The production process, including deviation of safety-related special characteristics, shall be analysed in order to:

- a) identify process failures;
- b) identify potential effects on functional safety resulting from the identified process failures;
- c) implement appropriate measures to ensure that the identified effects are avoided or mitigated; and

NOTE Such measures can include performing further control measures, sorting, processing, and exchange of elements.

- d) verify the effectiveness of the implemented measures.

6.4.1.3 The capability of the following shall be evaluated and maintained with regard to functional safety:

- a) production process;
- b) equipment and tools; and
- c) test equipment.

NOTE 1 Evidence regarding the capability of the production process can be obtained by periodic process audits or by periodic qualification measures for each person performing the process steps in conjunction with the quality management system.

NOTE 2 The capability of the process covers the ability to maintain the safety-related special characteristics.

6.4.1.4 The test equipment shall be controlled in accordance with the applied quality management system.

EXAMPLE The control of monitoring and measuring equipment requirements in IATF 16949.

6.4.1.5 The controls shall be performed in accordance with the production control plan. The related control report shall include the control date, the identification of controlled object, and the control results.

NOTE 1 The identification of the controlled object for a vehicle-level control measure can be a vehicle identification number or a production number.

NOTE 2 The identification of the controlled object for a controlled component can be a part number or a serial number.

NOTE 3 The control results can consist of either a single status, e.g. pass or fail, or the evaluation of a collection of data against boundary limits.

6.4.1.6 Only approved configurations shall be produced, as defined in the release for production report, unless a deviation is authorized by the responsible persons.

6.4.1.7 Changes to the production process initiated during the production phase shall be managed in accordance with the requirements in ISO 26262-8:2018, Clause 8.

6.5 Work products

6.5.1 Control measures report resulting from requirement [6.4.1.1](#), [6.4.1.2](#), [6.4.1.5](#) and [6.4.1.6](#).

6.5.2 Production process capability report resulting from requirement [6.4.1.3](#) and [6.4.1.4](#).

NOTE The capability of the production process can be included in the Production Part Approval Process (PPAP) documentation.

7 Operation, service and decommissioning

7.1 Objectives

The objective of this clause is to ensure that functional safety is achieved during the operation, service (maintenance and repair) and decommissioning sub-phases of the vehicle lifecycle.

7.2 General

This clause provides requirements for the execution and monitoring of operation, service and decommissioning, taking into account the safety-related special characteristics of the item.

Decommissioning includes the sub-phases “before disassembling”, “disassembling” and “after disassembling”. This clause addresses the activities during the sub-phase “before disassembling”, including the instructions for the activities and measures during the sub-phase “disassembling”.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

- release for production report in accordance with ISO 26262-2:2018, 6.5.6;
- safety-related content of the service plan in accordance with [5.5.5](#);
- safety-related content of the service instructions in accordance with [5.5.6](#);
- safety-related content of the information made available to the user in accordance with [5.5.7](#);

- safety-related content of the decommissioning instructions in accordance with [5.5.8](#);
- operation, service and decommissioning requirements specification in accordance with [5.5.9](#), if applicable; and
- safety-related content of the rescue services instructions in accordance with [5.5.10](#), if applicable.

7.3.2 Further supporting information

The following information can be considered:

- maintenance plan (from an external source).

7.4 Requirements and recommendations

7.4.1 Operation, service and decommissioning

7.4.1.1 The field monitoring process for potential safety-related incidents related to the item or its elements shall be implemented in order to:

- a) provide field data that can be analysed to detect the presence of functional safety issues;
- b) analyse this field data to detect the presence of functional safety issues; and
- c) trigger actions to address identified functional safety issues.

NOTE 1 Field monitoring data can provide the evidence required by the proven in use argument in accordance with ISO 26262-8:2018, Clause 14 for subsequent deployment of the item or element in another context.

NOTE 2 The field monitoring process for safety-related incidents includes decision making processes, defining the measures for containment and correction, e.g. a recall, as well as the reporting of incidents to the stakeholders. The stakeholders can be within the organization and, in the case of a distributed development, external to the organization.

7.4.1.2 The operation, service and decommissioning of the item or its elements shall be conducted and documented in accordance with the service plan, instructions for service and instructions for decommissioning.

NOTE 1 This includes the application of repair and maintenance procedures and the provision of either paper or electronic documentation of this application.

NOTE 2 This includes remanufacturing of elements for T&B vehicles.

NOTE 3 The supply, storage and transport of parts is implemented in accordance with [5.4.3.1](#).

7.4.1.3 Changes to the item or its elements, and changes to the processes for operation (including field monitoring), service or decommissioning, shall be managed in accordance with the requirements in ISO 26262-8:2018, Clause 8.

NOTE This includes rebuilding of a T&B vehicle.

7.5 Work products

7.5.1 Field observation instructions resulting from requirement [7.4.1.1](#).