INTERNATIONAL STANDARD

ISO 26262-7

First edition
2011-11-15

Road vehicles — Functional safety —

Part 7: Production and operation

Véhicules routiers — Sécurité fonctionnelle —

Partie 7: Production et utilisation

Reference number
ISO 26262-7:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 26262-7 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 26262 consists of the following parts, under the general title *Road vehicles — Functional safety*:

— *Part 1: Vocabulary*

— *Part 2: Management of functional safety*

— *Part 3: Concept phase*

— *Part 4: Product development at the system level*

— *Part 5: Product development at the hardware level*

— *Part 6: Product development at the software level*

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

— *Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

— *Part 10: Guideline on ISO 26262*

Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector 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 of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system 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. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

a) provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;

b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASIL)];

c) uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;

d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e) provides requirements for relations with suppliers.

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 by the management processes.

Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

Figure 1 shows the overall structure of this edition of ISO 26262. ISO 26262 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 between ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

— 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 Clause 6 of ISO 26262-2.

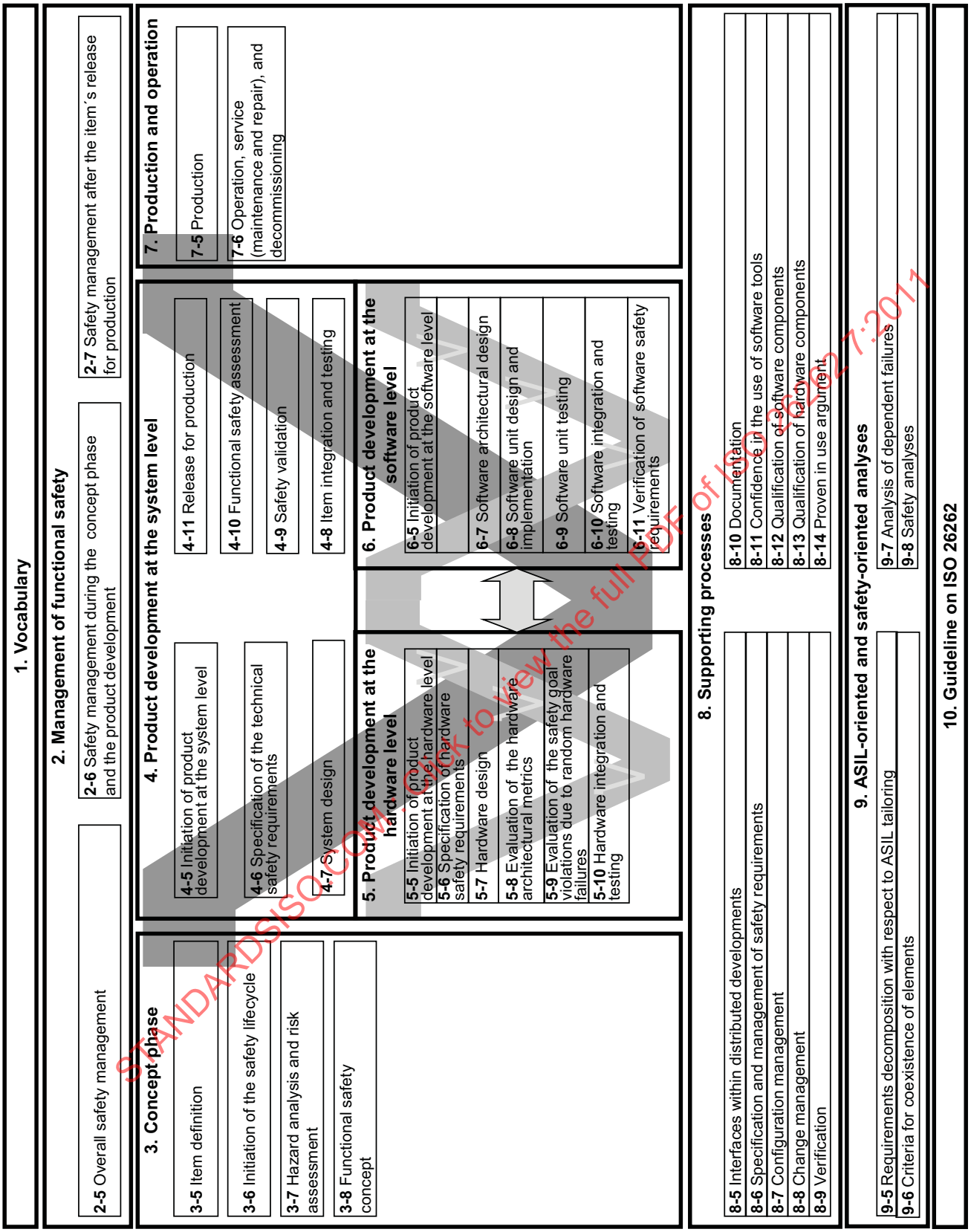

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 7:
Production and operation

1 Scope

ISO 26262 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 passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related 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 E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

This part of ISO 26262 specifies the requirements for production, operation, service and decommissioning.

2 Normative references

The following referenced documents are indispensable for the application 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 26262-1:2011, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-2:2011, *Road vehicles — Functional safety — Part 2: Management of functional safety*

ISO 26262-3:2011, *Road vehicles — Functional safety — Part 3: Concept phase*

ISO 26262-4:2011, *Road vehicles — Functional safety — Part 4: Product development at the system level*

ISO 26262-5:2011, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:2011, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-8:2011, *Road vehicles — Functional safety — Part 8: Supporting processes*

ISO 26262-9:2011, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1:2011 apply.

4 Requirements for compliance

4.1 General requirements

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

a) tailoring of the safety activities in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply, or

b) a rationale is available that the non-compliance is acceptable and the rationale has been assessed in accordance with ISO 26262-2.

Information marked as a “NOTE” or “EXAMPLE” 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 ISO 26262 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.

4.2 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 methods shall be applied as recommended in accordance with the ASIL. If methods other than those listed are to be applied, a rationale shall be given that these fulfil the corresponding requirement.

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 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;

— "o" indicates that the method has no recommendation for or against its usage for the identified ASIL.

4.3 ASIL-dependent requirements and recommendations

The requirements or recommendations of each subclause shall be complied with 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 26262-9:2011, Clause 5, the ASIL resulting from the decomposition shall be complied with.

If an ASIL is given in parentheses in ISO 26262, the corresponding subclause 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.

5 Production

5.1 Objectives

The first objective of this clause is to develop and maintain a production process for safety-related elements or items that are intended to be installed in road vehicles.

The second objective is to achieve functional safety during the production process by the relevant manufacturer or the person or organisation responsible for the process (vehicle manufacturer, supplier, sub-supplier, etc.).

5.2 General

The compliance with safety-related special characteristics of items or elements during their production, determined during the development phases, is necessary to achieve functional safety. Examples of such safety-related special characteristics are specific process parameters (e.g. temperature range or fastening torque), material characteristics, production tolerance, or configuration.

This phase defines requirements ensuring that functional safety is achieved during the production process by including these safety-related special characteristics in production planning and control.

The requirements and recommendations of this clause apply to the production and installation in the vehicle of items, systems or elements

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 26262-4:2011, 7.5.4, and ISO 26262-5:2011, 7.5.4;

— specification of dedicated measures for hardware in accordance with ISO 26262-5:2011, 9.5.2; and

— release for production report in accordance with ISO 26262-4:2011, 11.5.1.

5.3.2 Further supporting information

The following information can be considered:

— production plan (from external source); and

— production control plan (from external source).

5.4 Requirements and recommendations

5.4.1 Production planning

5.4.1.1 The production process shall be planned by evaluating the item and by considering the following:

a) the requirements for production;

EXAMPLE Assembly instructions (e.g. the calibration and setup of a sensor); safety-related special characteristics (e.g. the tolerance for the selection of elements).

b) the conditions for storage, transport and handling of hardware elements;

EXAMPLE Allowed storage time for the element.

c) the approved configurations defined in the release for production documentation;

d) the lessons learned on the capability from previously released production plans;

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

f) the competences of the personnel.

5.4.1.2 The production plan shall describe the production steps, sequence and methods required to achieve the functional safety of the item, system or element. It shall include:

a) the production process flow and instructions;

b) the production tools and means;

c) the implementation of the traceability measures; and

EXAMPLE Labelling for the element.

d) if applicable, the implementation of dedicated measures applying to hardware parts and specified during hardware development in accordance with ISO 26262-5:2011, 9.4.2.4.

NOTE The production process also includes processes or operations required to rework the item.

5.4.1.3 A procedure shall be defined to ensure that the correct embedded software and the associated calibration data are loaded into the ECUs as part of the production process.

EXAMPLE 1 The use of a checksum, so that the checksum of the loaded executable and configuration data is compared to the correct checksum for this particular model and 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 When developing the production control plan, the controls' description and criteria for the item, system or element as well as the safety-related special characteristics shall be considered.

5.4.1.5 The sequence and methods of the control steps shall be described in the production control plan, together with the necessary test equipment, tools and test criteria.

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

5.4.1.7 The system, hardware or software development level safety requirements on the producibility of the item, system or element arising during production planning shall be specified and directed to the persons responsible for the development (see ISO 26262-4, ISO 26262-5 and ISO 26262-6).

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 If changes to the item, system or element are required during the production process, the change management process described in ISO 26262-8:2011, Clause 8, shall be complied with.

5.4.2 Pre-production series production

5.4.2.1 The pre-production process and its control measures should correspond to the target production process.

NOTE Pre-production series are items, systems or elements, produced before release for production.

5.4.2.2 Differences between pre-production process and target production process shall be analysed in order to identify which part of the production process can be assessed at the pre-production stage and for which part of the target production process an assessment will be required.

NOTE If the pre-production process equals the target production process, the result of assessments (e.g. proof of capability of the production process) can be used when performing the functional safety assessment in accordance with ISO 26262-2:2011, 6.4.9.4.

EXAMPLE Deviations can concern the production rate, the sequence and methods of the production or control steps, as well as necessary means of production, test equipment, and tools.

5.4.3 Production

5.4.3.1 The production process and its control measures shall be implemented and maintained as planned.

NOTE The appropriate training of the personnel involved in production is part of this implementation.

5.4.3.2 Process failures occurring during production (including deviation of safety-related special characteristics from their authorised range) and their potential effects on functional safety shall be analysed, the appropriate measures shall be taken and their ability to maintain functional safety shall be verified.

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

5.4.3.3 The capability of the following shall be assessed and maintained with regard to functional safety:

a) production process;

b) means of production; and

c) tools and test equipment.

NOTE 1 The capability of the process can be proven by periodic process audits or by periodic qualification measures for each person performing the process steps.

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

5.4.3.4 The test equipment shall be subject to control of monitoring and measuring devices.

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

NOTE 1 In the case of manual controls, the identification of the controlled object and control results are sufficient.

NOTE 2 The identification of the controlled object can be a vehicle identification number or a production number for a vehicle-level control measure or a part number or a serial number for a controlled component.

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.

5.4.3.6 Only approved configurations shall be produced, as defined in the release for production documentation, unless a deviation from the release for production documentation is authorized by the responsible person(s). The release for production documentation may be updated later in accordance with this authorized deviation.

5.4.3.7 Changes to the production process initiated during the production phase shall comply with Clause 5.

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, 5.4.1.6 and 5.4.3.2.

5.5.2 **Safety-related content of the production control plan** including the test plan, resulting from requirements 5.4.1.4, 5.4.1.5, 5.4.3.4, and 5.4.3.6.

5.5.3 **Control measures report** resulting from requirement 5.4.3.5.

5.5.4 If applicable, **specification of requirements on the producibility at system, hardware or software development level** resulting from requirement 5.4.1.7.

NOTE This specification can be appended to the relevant documentation of the corresponding phases.

5.5.5 **Assessment report for capability of the production process**, resulting from requirement 5.4.2.2 and 5.4.3.3.

6 Operation, service (maintenance and repair), and decommissioning

6.1 Objectives

The objective of this clause is to specify the customer information, maintenance and repair instructions, as well as disassembly instructions regarding the item, system or element, in order to maintain the functional safety over the lifecycle of the vehicle.

6.2 General

This clause provides requirements for developing repair instructions and user information, including the user manual and the planning, execution and monitoring of the maintenance work, taking into account the safety-related special characteristics of the item.

During decommissioning, the phases “before disassembling”, “disassembling” and “after disassembling” can be distinguished. This clause addresses only those activities “before disassembling”.

6.3 Input to this clause

6.3.1 Prerequisites

The following information shall be available:

— requirements specification for production, operation, service and decommissioning in accordance with ISO 26262-5:2011, 7.5.4;

— release for production report in accordance with ISO 26262-4:2011, 11.5.1; and

— warning and degradation concept, included in the functional safety concept in accordance with ISO 26262-3:2011, 8.5.1.

6.3.2 Further supporting information

The following information can be considered:

— maintenance plan (from external source).

6.4 Requirements and recommendations

6.4.1 Planning of operation, service (maintenance and repair), and decommissioning

6.4.1.1 The operation, repair and maintenance processes shall be planned by evaluating the item and by considering the following:

a) the requirements for maintenance and repair;

b) the requirements for the information that shall be made available to the user to ensure the safe operation of the vehicle;

c) the warning and degradation concept;

d) the measures for field data collection and analysis;

e) the conditions for storage, transport and handling of the hardware elements;

EXAMPLE Allowed storage time for the element.

f) the approved configurations defined in the release for production documentation; and

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

g) the competence of the personnel involved.

6.4.1.2 The maintenance plan shall describe the sequence and methods of the maintenance steps or activities, the maintenance intervals, and the necessary means of maintenance and tools.

6.4.1.3 The maintenance plan and repair instructions shall describe the following:

a) the work steps, procedures, diagnostic routines and methods;

b) the maintenance tools and means;

EXAMPLE Programming, sensor calibration/setup 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 item, systems or elements configurations, including the traceability measures;

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

EXAMPLE Labelling for the element is a way of ensuring traceability.

e) the allowed deactivation of the item, systems or elements and necessary changes in the vehicle;

f) the driver information for the allowed deactivations and changes; and

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

g) the provision of replacement parts.

6.4.1.4 User information, including the user's manual, shall provide relevant usage instructions and warnings concerning the proper usage of the item, as well as the following information if applicable:

a) a description of the relevant functions, (i.e. the intended usage, 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 concept;

c) a description of the maintenance activities expected from the customer in the case of a failure indicated by the warning and degradation concept;

d) the warnings regarding known hazards resulting from interactions with third party products; and

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

e) the warnings regarding safety-related innovative functions of the item that could lead to driver's misunderstanding or misuse.

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

6.4.1.5 The decommissioning instructions shall describe the activities and measures to be applied before disassembly, and required to prevent the violation of a safety goal during disassembling, handling or decommissioning of the vehicle, 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.

6.4.1.6 System, hardware or software level safety requirements arising during the planning of operation, service (maintenance and repair), and decommissioning, shall be specified and directed to the persons responsible for the development (see ISO 26262-4, ISO 26262-5 and ISO 26262-6).