BS ISO 26262-10:2018

BSI Standards Publication

Road vehicles — Functional safety

Part 10: Guidelines on ISO 26262

Documents
Document Sharing Hub

Full document details: BS ISO 26262-10:2018

National foreword

This British Standard is the UK implementation of ISO 26262-10:2018. It supersedes BS ISO 26262-10:2012, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AUE/32, Electrical and electronic components and general system aspects (Road vehicles).

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 89518 0

ICS 43.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 26262-10:2018

INTERNATIONAL STANDARD

ISO 26262-10

Second edition
2018-12

Road vehicles — Functional safety —

Part 10: Guidelines on ISO 26262

Véhicules routiers — Sécurité fonctionnelle —

Partie 10: Lignes directrices relatives à l'ISO 26262

Reference number
ISO 26262-10:2018(E)

Documents
Document Sharing Hub

© ISO 2018

Full document details: BS ISO 26262-10:2018

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 26262-10:2018

Contents

Page

Foreword ... **vi**

Introduction ... **viii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Key concepts of ISO 26262 ... **2**
4.1 Functional safety for automotive systems (relationship with IEC 61508[1]) ... 2
4.2 Item, system, element, component, hardware part and software unit ... 4
4.3 Relationship between faults, errors and failures ... 5
4.3.1 Progression of faults to errors to failures ... 5
4.4 FTTI and emergency operation tolerant time interval ... 6
4.4.1 Introduction ... 6
4.4.2 Timing model — Example control system ... 7

5 Selected topics regarding safety management ... **9**
5.1 Work product ... 9
5.2 Confirmation measures ... 9
5.2.1 General ... 9
5.2.2 Functional safety assessment ... 10
5.3 Understanding of safety cases ... 12
5.3.1 Interpretation of safety cases ... 12
5.3.2 Safety case development lifecycle ... 13

6 Concept phase and system development ... **13**
6.1 General ... 13
6.2 Example of hazard analysis and risk assessment ... 13
6.2.1 General ... 13
6.2.2 HARA example 1 ... 13
6.2.3 HARA example 2 ... 14
6.3 An observation regarding controllability classification ... 14
6.4 External measures ... 15
6.4.1 General ... 15
6.4.2 Example of vehicle dependent external measures 1 ... 15
6.4.3 Example of vehicle dependent external measures 2 ... 15
6.5 Example of combining safety goals ... 16
6.5.1 Introduction ... 16
6.5.2 General ... 16
6.5.3 Function definition ... 16
6.5.4 Safety goals applied to the same hazard in different situations ... 16

7 Safety process requirement structure — Flow and sequence of the safety requirements ... **17**

8 Concerning hardware development ... **19**
8.1 The classification of random hardware faults ... 19
8.1.1 General ... 19
8.1.2 Single-point fault ... 19
8.1.3 Residual fault ... 20
8.1.4 Detected dual-point fault ... 20
8.1.5 Perceived dual-point fault ... 20
8.1.6 Latent dual-point fault ... 21
8.1.7 Safe fault ... 21
8.1.8 Flow diagram for fault classification and fault class contribution calculation ... 21
8.1.9 How to consider the failure rate of multiple-point faults related to software-based safety mechanisms addressing random hardware failures ... 25
8.2 Example of residual failure rate and local single-point fault metric evaluation ... 25

© ISO 2018 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO 26262-10:2018

8.2.1 General 25
8.2.2 Technical safety requirement for sensor A_Master 25
8.2.3 Description of the safety mechanism 26
8.2.4 Evaluation of example 1 described in Figure 12 29
8.3 Further explanation concerning hardware 37
8.3.1 How to deal with microcontrollers in the context of an ISO 26262 series of standards application 37
8.3.2 Safety analysis methods 37
8.4 PMHF units — Average probability per hour 44

9 Safety Element out of Context 47
9.1 Safety Element out of Context development 47
9.2 Use cases 48
9.2.1 General 48
9.2.2 Development of a system as a Safety Element out of Context example 49
9.2.3 Development of a hardware component as a Safety Element out of Context example 51
9.2.4 Development of a software component as a Safety Element out of Context example 53

10 An example of proven in use argument 55
10.1 General 55
10.2 Item definition and definition of the proven in use candidate 56
10.3 Change analysis 56
10.4 Target values for proven in use 56

11 Concerning ASIL decomposition 57
11.1 Objective of ASIL decomposition 57
11.2 Description of ASIL decomposition 57
11.3 An example of ASIL decomposition 57
11.3.1 General 57
11.3.2 Item definition 57
11.3.3 Hazard analysis and risk assessment 58
11.3.4 Associated safety goal 58
11.3.5 System architectural design 58
11.3.6 Functional safety concept 59

12 Guidance for system development with safety-related availability requirements 60
12.1 Introduction 60
12.2 Notes on concept phase when specifying fault tolerance 61
12.2.1 General 61
12.2.2 Vehicle operating states in which the availability of a functionality is safety-related 61
12.2.3 Prevention of hazardous events after a fault 61
12.2.4 Operation after fault reaction 62
12.2.5 Fault tolerant item example 63
12.2.6 ASIL decomposition of fault tolerant items 68
12.3 Availability considerations during hardware design phase 69
12.3.1 Random hardware fault quantitative analysis 69
12.4 Software development phase 71
12.4.1 Software fault avoidance and tolerance 71
12.4.2 Software fault avoidance 71
12.4.3 Software fault tolerance 71

13 Remark on "Confidence in the use of software tools" 72

14 Guidance on safety-related special characteristics 73
14.1 General 73
14.2 Identification of safety-related special characteristics 74
14.3 Specification of the control measures of safety-related special characteristics 74
14.4 Monitoring of the safety-related special characteristics 75

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

Annex A (informative) **Fault tree construction and applications** **76**
Bibliography **79**

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

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; and

— general restructuring of all parts for improved clarity.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

NOTE The first edition of this document was published in 2012, therefore this document cancels and replaces ISO 26262-10:2012.

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.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

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;

— 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.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

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

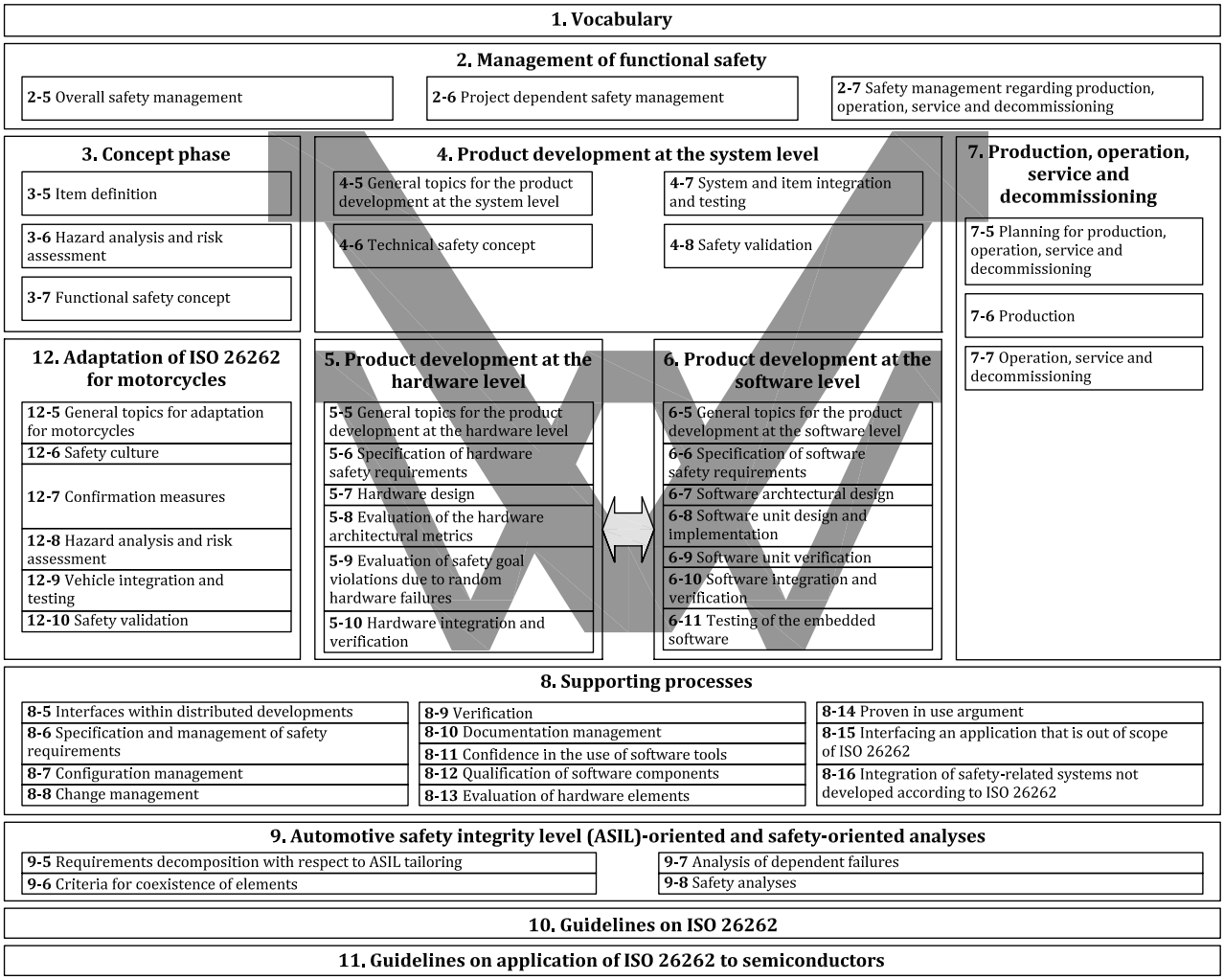


Figure 1 — Overview of the ISO 26262 series of standards

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

Documents
Document Sharing Hub

Road vehicles — Functional safety —

Part 10:
Guidelines on ISO 26262

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 provides an overview of the ISO 26262 series of standards, as well as giving additional explanations, and is intended to enhance the understanding of the other parts of the ISO 26262 series of standards. It has an informative character only and describes the general concepts of the ISO 26262 series of standards in order to facilitate comprehension. The explanation expands from general concepts to specific contents.

In the case of inconsistencies between this document and another part of the ISO 26262 series of standards, the requirements, recommendations and information specified in the other part of the ISO 26262 series of standards apply.

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 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

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 Key concepts of ISO 26262

4.1 Functional safety for automotive systems (relationship with IEC 61508[1])

IEC 61508, *Functional Safety of electrical/electronic/programmable electronic safety-related systems,* is designated by IEC as a generic standard and a basic safety publication. This means that industry sectors will base their own standards for functional safety on the requirements of IEC 61508.

In the automotive industry, there are a number of issues with applying IEC 61508 directly. Some of these issues and corresponding differences in the ISO 26262 series of standards are described below.

IEC 61508 is based upon the model of "equipment under control", for example an industrial plant that has an associated control system as follows:

a) A hazard analysis identifies the hazards associated with the equipment under control (including the equipment control system), to which risk reduction measures will be applied. This can be achieved through electrical/electronic/programmable electronic (E/E/PE) systems, or other technology safety-related systems (e.g. a safety valve), or external measures (e.g. a physical containment of the plant). The ISO 26262 series of standards contains a normative automotive scheme for hazard classification based on severity, probability of exposure and controllability.

b) Risk reduction allocated to E/E/PE systems is achieved through safety functions, which are designated as such. These safety functions are either part of a separate protection system, or can be incorporated into the plant control. It is not always possible to make this distinction in automotive systems. The safety of a vehicle depends on the behaviour of the control systems themselves.

The ISO 26262 series of standards uses the notion of safety goals and a safety concept as follows:

— a hazard analysis and risk assessment identifies hazards and hazardous events that need to be prevented, mitigated, or controlled;

— at least one safety goal is associated with each hazardous event that has been classified as ASIL A, B, C or D;

— an Automotive Safety Integrity Level (ASIL) is associated with each safety goal;

— the functional safety concept is a statement of the functionality to achieve the safety goal(s);

— the technical safety concept is a statement of how this functionality is implemented on the system level by hardware and software; and

— software safety requirements and hardware safety requirements state the specific safety requirements which will be implemented as part of the software and hardware design.

EXAMPLE The airbag system.

— One of the hazards is unintended deployment.

— An associated safety goal is that the airbag only deploys when a crash occurs that requires the deployment.

— The functional safety concept can specify a redundant function to detect whether the vehicle is in a collision.

© ISO 2018 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-10:2018

— The technical safety concept can specify the implementation of two independent accelerometers with different axial orientations and two independent firing circuits. The squib deploys if both are closed.

IEC 61508 is aimed at singular or low volume systems. The system is built and tested, then installed in the plant, and then safety validation is performed. For mass-market systems such as road vehicles, safety validation is performed before the release for volume (series) production. Therefore, the order of lifecycle activities in the ISO 26262 series of standards is different. Related to this, ISO 26262-7 addresses requirements for production. These are not covered in IEC 61508.

IEC 61508 does not address specific requirements for managing development across multiple organizations and supply chains. Because automotive systems are produced by vehicle manufacturers themselves, by one or more suppliers to the manufacturer or by collaboration between manufacturer and supplier(s), the ISO 26262 series of standards includes requirements to explicitly address this issue, including the Development Interface Agreement (DIA) (see ISO 26262-8:2018, Clause 5).

IEC 61508 does not contain normative requirements for hazard classification. The ISO 26262 series of standards contains an automotive scheme for hazard classification. This scheme recognises that a hazard in an automotive system does not necessarily lead to an accident. The outcome will depend on whether the persons at risk are actually exposed to the hazard in the situation in which it occurs; and whether the involved people are able to take steps to control the outcome of the hazard. An example of this concept, applied to a failure which affects the controllability of a moving vehicle, is given in Figure 2.

NOTE This concept is intended only to demonstrate that there is not necessarily a direct correlation between a failure occurring and the accident. It is not a representation of the hazard analysis and risk assessment process, although the parameters evaluated in this process are related to the probabilities of the state transitions shown in the figure.

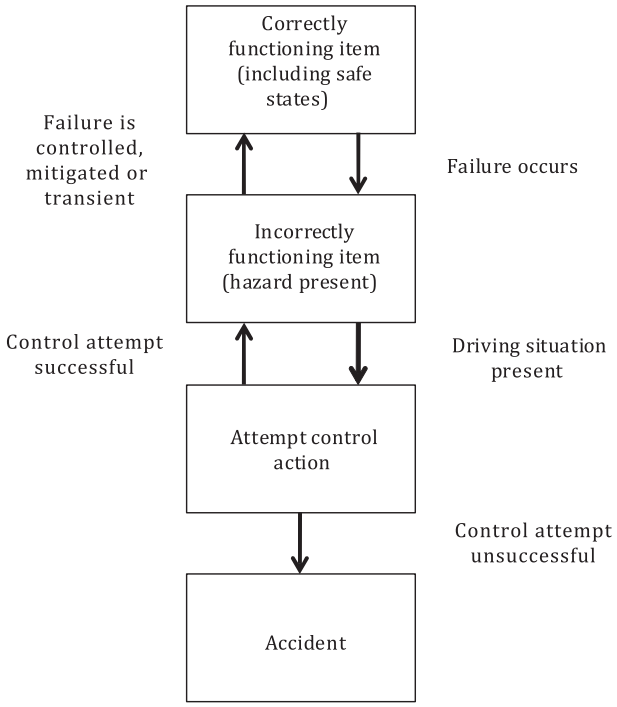


Figure 2 — State machine model of automotive risk

The requirements for hardware development (ISO 26262-5) and software development (ISO 26262-6) are adapted for the state-of-the-art in the automotive industry. For the methods listed in the ISO 26262 series of standards specific goals are provided. To achieve these goals, the provided methods can be applied or a rationale that alternative methods can also achieve the goal is provided.

Safety requirements in the ISO 26262 series of standards are assigned an ASIL (Automotive Safety Integrity Level) rather than a SIL (Safety Integrity Level). The main motivation for this [illegible]

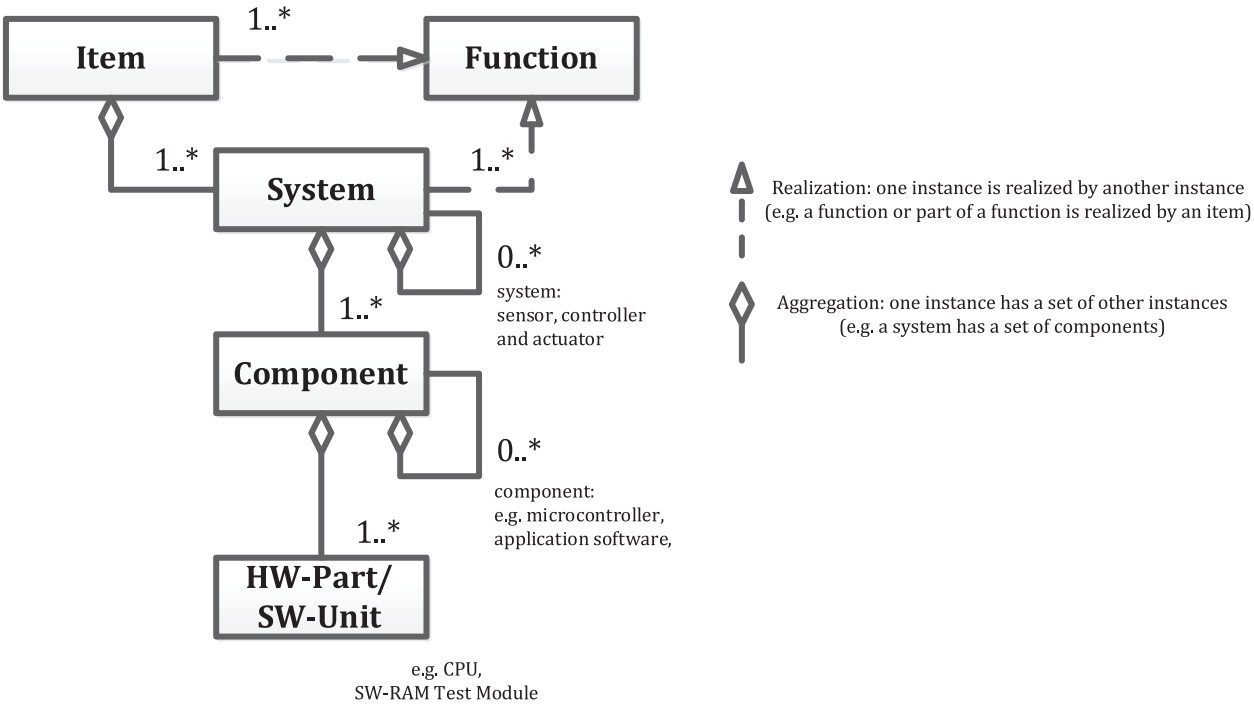
© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-10:2018

in IEC 61508 is stated in probabilistic terms (see IEC 61508-1:2010, Table 3). IEC 61508 acknowledges that qualitative judgement is often required in respect of systematic safety integrity while requiring quantitative techniques for hardware safety integrity. An ASIL in ISO 26262 is primarily concerned with requirements for achieving systematic safety in the system, hardware and software; however, there are probabilistic targets associated with compliance to the requirements of an ASIL with respect to random hardware failures.

4.2 Item, system, element, component, hardware part and software unit

The terms item, system, element, component, hardware part and software unit are defined in ISO 26262-1:2018. Figure 3 shows the relationship of item, system, component, hardware part and software unit. Figure 4 shows an example of item dissolution. A divisible element can be labelled as a system or a component. A divisible element that meets the criteria of a system can be labelled as a system. A component is a non-system level, logically and technically separable element. Often the term component is applied to an element that is only comprised of parts and units, but can also be applied to an element comprised of lower-level elements from a specific technology area e.g. electrical / electronic technology (see Figure 4). A hardware part can be further hierarchically composed of hardware subparts and hardware elementary subparts as applicable.



NOTE 1 Depending on the context, the term “element” can apply to the entities “system”, “component”, “hardware part” and “software unit” in this chart, according to ISO 26262-1:2018, 3.41.

NOTE 2 The system, as it is defined in ISO 26262-1:2018, 3.163, relates at least a sensor, a controller, and an actuator with one another. The related sensor or actuator can be included in the system, or can be external to the system.

NOTE 3 *means N are possible.

Figure 3 — Relationship of item, system, component, hardware part and software unit

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

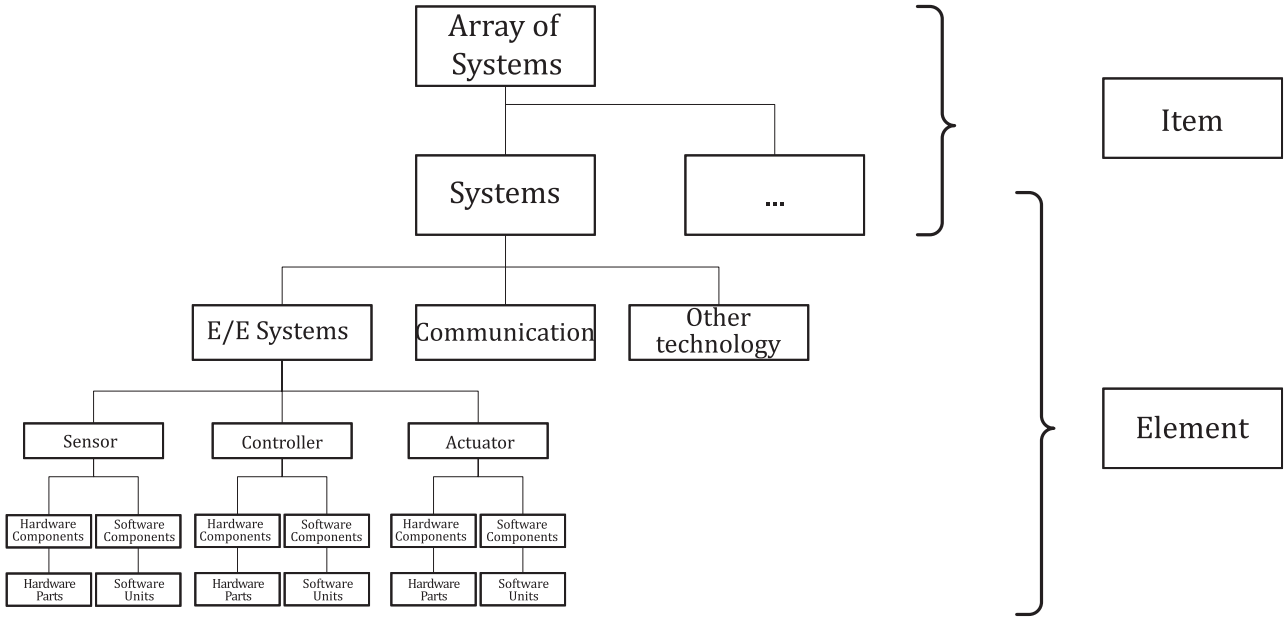


Figure 4 — Example item dissolution

4.3 Relationship between faults, errors and failures

4.3.1 Progression of faults to errors to failures

The terms fault, error and failure are defined in ISO 26262-1:2018. Figure 5 depicts the progression of faults to errors to failures from three different types of causes: systematic software issues, random hardware issues and systematic hardware issues. Systematic faults (see ISO 26262-1:2018, 3.165) are due to design or specification issues; software faults and a subset of hardware faults are systematic. At the component level, each different type of fault can lead to different failures. However, failures at the component level are faults at the item level. Note that in this example, at the vehicle level, faults from different causes can lead to the same failure. A subset of failures at the item level will be hazards (see ISO 26262-1:2018, 3.75) if additional environmental factors permit the failure to contribute to an accident scenario.

EXAMPLE If unexpected behaviour of the vehicle occurs while the vehicle is starting to cross an intersection, a crash can occur, e.g. the risk of the hazardous event “vehicle bucking when starting to cross intersection” is assessed for severity, exposure and controllability ("bucking" refers to making sudden jerky movements).

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

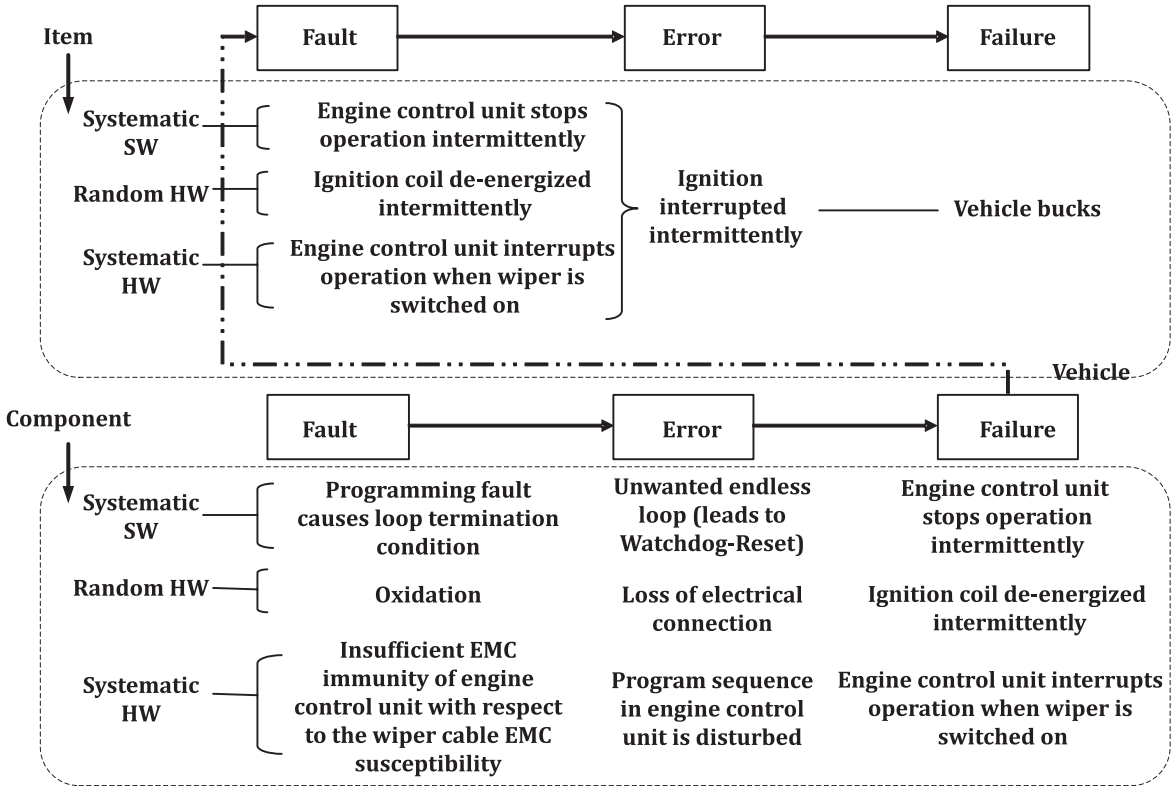


Figure 5 — Example of faults leading to failures

NOTE 1 Possible implemented error detection and control on component or item level is not depicted in Figure 5.

NOTE 2 The failure of the component is the fault on the item level (indicated by the dot dot dashed arrow).

4.4 FTTI and emergency operation tolerant time interval

4.4.1 Introduction

ISO 26262-3:2018, 6.4.4.3 states in the NOTE that the FTTI can be included as part of a safety goal. Furthermore, ISO 26262-4:2018, 6.4.2.2 specifies that the FTTI and emergency operation tolerance time interval are to be taken into account in the definition of fault handling time interval for each safety mechanism.

NOTE Fault handling time interval is a characteristic for a given safety mechanism. Fault tolerant time interval (FTTI) is a characteristic of an item.

As a part of the process of determining safety goals and functional safety requirements at concept phase, the FTTI is specified on vehicle level based on vehicle functionality. This time span can be taken into consideration during product development, leading to the determination of the maximum fault handling time interval (i.e. sum of the fault detection time interval and the fault reaction time interval as described in ISO 26262-1:2018, Figure 5) needed to avoid a hazardous event. FTTI is a necessary value in order to design the response time of a safety mechanism. Within the FTTI, the fault is controlled by a safety mechanism and the occurrence of a hazardous event can be prevented. This is achieved when the sum of the fault detection time interval and the fault reaction time interval is shorter than the FTTI.

An emergency operation (ISO 26262-4:2018, 6.4.2.2) is specified when a safe state cannot be reached within the FTTI. The emergency operation is an operating mode defined as part of the warning and degradation strategy. Emergency operation is initiated prior to the end of the FTTI and is maintained until the safe state is reached prior to the end of the emergency operation tolerance time interval. To

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

meet the safety goal, a safe state has to be reached before the end of the emergency operation tolerance time interval.

4.4.2 Timing model — Example control system

4.4.2.1 Control system description

This sub-clause applies the concepts of fault detection time interval (FDTI), fault tolerant time interval (FTTI), fault reaction time interval (FRTI), emergency operation tolerance time interval (EOTTI) and diagnostic test time interval (DTTI) to a valve control system example. The system consists of a valve, position sensor, controller and an electrical motor. The function of the system is to control the valve to a desired position using the electric motor.

A hazardous event resulting from an unintended flow can occur if the valve is opened a percentage more than intended. As a fault reaction, the motor is de-energized by a separate circuit in combination with a mechanical spring which pulls the valve to a default fixed opening position. This fixed opening position limits the flow resulting in a safe state for the item.

4.4.2.2 Application of timing model to example control system

The specific failure mode considered in this example is a motor fault which drives the valve to its maximum opening position. This condition can be the result of motor shorted to power or other motor control issues. Four scenarios are considered.

— Scenario 1: System without any safety mechanism preventing the violation of the safety goal.

  A short in the motor occurs resulting in the valve reaching its maximum position. Because no safety mechanism is in place a hazardous event can occur once the FTTI is exceeded.

— Scenario 2: System with implemented safety mechanism without emergency operation and a safe state is achieved within FTTI.

  A short in the motor occurs resulting in the valve reaching its maximum position. The implemented safety mechanism de-energizes the valve motor and the mechanical spring returns the valve to a low flow position within the FTTI, preventing a hazardous event. The safety mechanism (the spring) is designed to operate indefinitely and the safe state can be infinite.

— Scenario 3: System with implemented safety mechanism which prevents a hazardous event within the FTTI, but emergency operation is needed to transit to a safe state. The safe state is achieved within the emergency operation tolerance time interval by restricting the vehicle operating state.

  A short in the motor occurs resulting in the valve reaching its maximum position. The implemented safety mechanism de-energizes the valve motor and the mechanical spring returns the valve to a low flow position within the FTTI. The safety mechanism (the spring) is only designed to operate for a limited amount of time, the EOTTI. Prior to the expiration of the EOTTI, the vehicle operating state is restricted such that the flow from the valve cannot cause a hazardous event.

— Scenario 4: System with implemented safety mechanism which prevents a hazardous event is within the FTTI but emergency operation is needed to transit to a safe state. However, the transition time takes longer than the EOTTI. As a consequence, the cumulated risk becomes unacceptable, exceeding the target specified in the functional safety concept.

  A short in the motor occurs resulting in the valve reaching its maximum position. The implemented safety mechanism de-energizes the valve motor and the mechanical spring returns the valve to a low flow position within the FTTI. The safety mechanism (the spring) is only designed to operate for a limited amount of time, the EOTTI. In this scenario, the vehicle operation is not restricted and the item is in emergency operation longer than the expiration of the EOTTI, resulting in an unreasonable risk of safety goal violation.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

Figure 6 shows the timing model associated with the four scenarios. Figure 6 is based on ISO 26262-1:2018, Figure 4 and ISO 26262-1:2018, Figure 5.

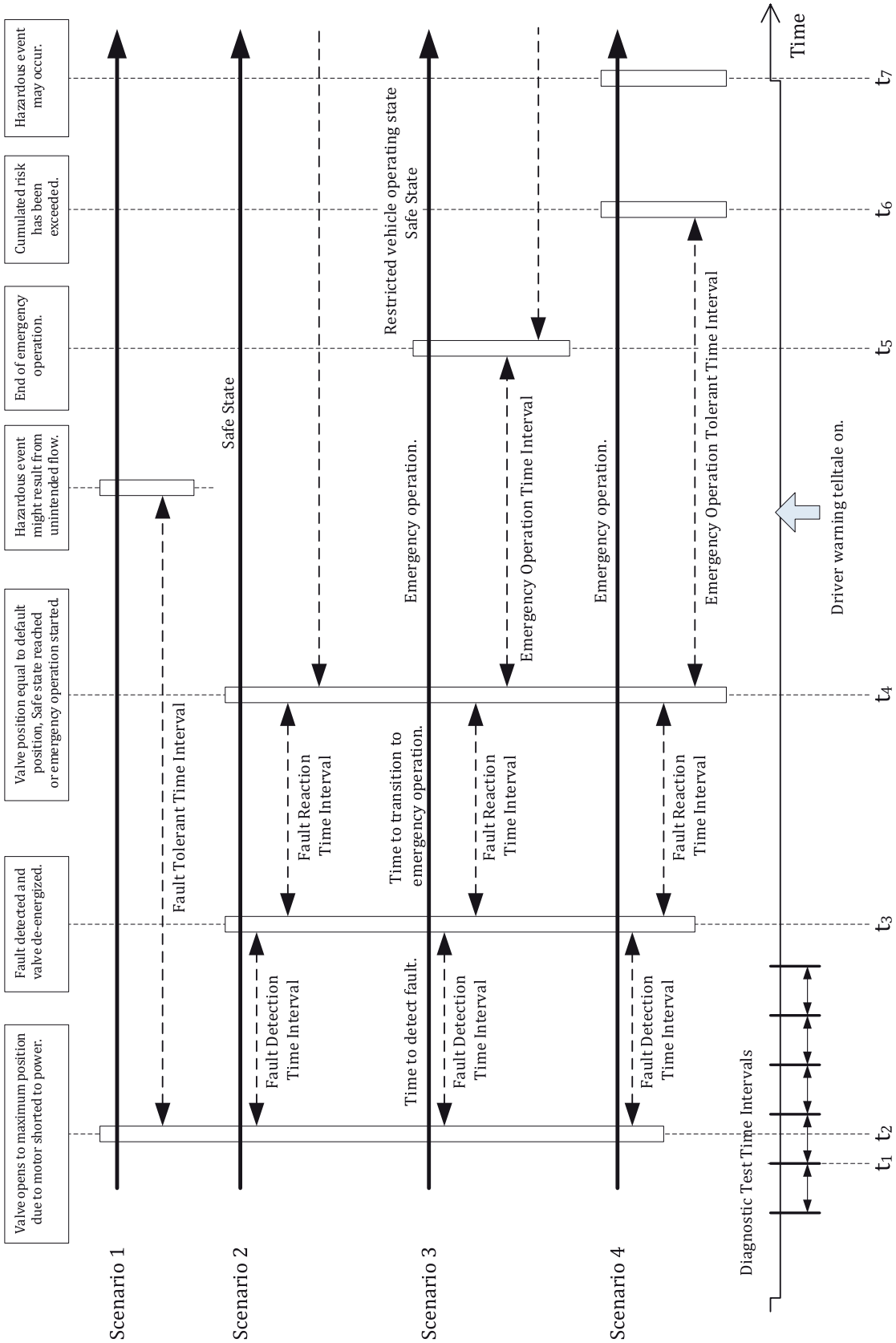


Figure 6 — Timing model example based on ISO 26262-1:2018, Figure 4

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

Figure 6 includes 7 time stamps described below:

t_1 Time of diagnostic test prior to occurrence of the fault.

t_2 Occurrence of fault, fault not detected.

t_3 Detection of fault (e.g. due to error counter reaching its threshold, see ISO 26262-1:2018, 3.55 FDTI EXAMPLE), start of fault reaction time interval.

t_4 Transition to safe state completed (scenario 2), start of emergency operation (scenarios 3 and 4).

t_5 End of emergency operation (scenario 3).

t_6 Time limit for emergency operation.

t_7 Occurrence of hazardous event.

4.4.2.3 Warning and degradation strategy

When the valve is in the default position, it can have an impact at the vehicle level. The functional safety concept may also include a requirement to warn the driver when in this state. This is part of the warning and degradation strategy and is indicated by the “Driver warning telltale on” arrow on Figure 6 which can occur within a specified time after t_3.

5 Selected topics regarding safety management

5.1 Work product

This sub-clause describes the term "work product".

A work product is the result of meeting the corresponding requirements of the ISO 26262 series of standards (see ISO 26262-1:2018, 3.185). Therefore, a work product can provide evidence of compliance with these safety requirements.

EXAMPLE A requirements specification is a work product that can be documented by means of a requirements database or a text file. An executable model is a work product that can be represented by modelling language files that can be executed (e.g. for simulation purposes by using a software tool).

The documentation of a work product (see ISO 26262-8:2018, Clause 10) serves as a record of the executed safety activities, safety requirements or of related information. Such documentation is not restricted to any form or medium.

EXAMPLE The documentation of a work product can be represented by electronic or paper files, by a single document or a set of documents. It can be combined with the documentation of other work products or with documentation not directly dedicated to functional safety.

To avoid the duplication of information, cross-references within or between documentation can be used.

5.2 Confirmation measures

5.2.1 General

In ISO 26262, specified work products are evaluated during subsequent activities, either as part of the confirmation measures or as part of the verification activities. This sub-clause describes the difference between verification and confirmation measures.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

The verification activities are the primary measures in ISO 26262 to provide evidence that a work product is suitable and complies with the corresponding requirements. The verification of work products can include:

— verification of the specification, or implementation, of derived safety requirements against the safety requirements at a higher level, regarding completeness and correctness; or

— the execution of test cases and the examination of test results to provide evidence of the fulfilment of specified safety requirements, by exercising the item or its element(s).

The verification activities are specified in ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6. Furthermore, generic requirements regarding the verification activities in the ISO 26262 series of standards are specified in ISO 26262-8:2018, Clause 9 and further details specific to the verification of safety requirements are specified in ISO 26262-8:2018, Clause 6.

Verification of work products can be performed by using techniques such as:

— reviews;

— simulation;

— analysis; or

— testing.

Confirmation measures are specified in ISO 26262-2:2018, 6.4.9 and are performed to evaluate the item's achievement of functional safety.

EXAMPLE If an ASIL decomposition is applied during the system architectural design phase:

— the verification of the resulting system architectural design is performed against the technical safety concept (see ISO 26262-4:2018, 6.4.9); and

— the confirmation of the correct application of the ASIL decomposition can be performed as part of a functional safety assessment, with regard to ISO 26262-9:2018, Clause 5, including the confirmation that a dependent failure analysis has been performed and justifies the claim of sufficient independence between the elements that implement the corresponding redundant safety requirements.

5.2.2 Functional safety assessment

If the highest ASIL of the item's safety goals is ASIL C or D, a functional safety assessment is performed to evaluate an item's achievement of functional safety. In ISO 26262-2, certain aspects of a functional safety assessment are described as well as further aspects of confirmation measures.

The scope of the functional safety assessment is defined in ISO 26262-2:2018, Clause 6.

In the case a functional safety assessment is performed, the results of the functional safety audit and of the confirmation reviews are an input for the functional safety assessment. The person responsible for the assessment can perform the assessment according to his/her discretion, including how to make use of the results of the functional safety audit and confirmation reviews.

EXAMPLE 1 If the results of the functional safety audit are satisfactory, the person responsible for the functional safety assessment can decide to rely on the results of the audit, without making a further judgement of the implementation of the processes required for functional safety.

EXAMPLE 2 Based on the confirmation review report of a particular work product, the person responsible for the assessment can decide to perform, or to request, a more in-depth review of certain aspects of that work product, or can check whether the confirmation review sufficiently considered the interplay between that work product and related work products.

NOTE 1 It is possible that the person responsible for the functional safety assessment performs a particular confirmation review i.e. a confirmation review is not necessarily performed by a person different from the person responsible for the assessment.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

A functional safety assessment can be repeated or updated.

EXAMPLE 3 A functional safety assessment update because of a change of the item, or element(s) of the item, that is identified by the change management as having an impact on the functional safety of the item (see ISO 26262-8:2018, Clause 8).

EXAMPLE 4 A functional safety re-assessment that is triggered by a functional safety assessment report that recommends a conditional acceptance or a rejection of the item's functional safety. In this case, the iteration includes a follow-up of the recommendations resulting from the previous functional safety assessment(s), including an evaluation of the performed corrective actions, if applicable.

If the highest ASIL of the item's safety goals is ASIL A or ASIL B, a functional safety assessment can be omitted or performed less rigorously. However, even if the functional safety assessment is not performed, other confirmation measures are still performed (see ISO 26262-2:2018, Table 1).

In the case of a distributed development, the scope of a functional safety assessment includes the work products generated, and the processes and safety measures implemented, by a vehicle manufacturer and the suppliers in the item's supply chain (see ISO 26262-2 and ISO 26262-8:2018, Clause 5).

The purpose of a functional safety assessment is to evaluate an item's achievement of functional safety, which is only possible at the item level. Therefore, a functional safety assessment of a supplier (that develops elements of the item) refers only to an assessment with a limited scope, which essentially serves as an input for the subsequent functional safety assessment activities (at the customer level). As the final customer in the item development, the vehicle manufacturer appoints person(s) to perform an overall functional safety assessment to judge an item's achievement of functional safety. This judgement includes providing a recommendation for acceptance, conditional acceptance, or rejection of the item's functional safety.

NOTE 2 For the case where a Tier 1 supplier is responsible for the item development including vehicle integration, this supplier takes over the aforementioned role of the vehicle manufacturer.

In a practical manner, a functional safety assessment in the case of a distributed development can thus be broken down into:

— functional safety assessments with a limited scope, concerning the suppliers in the supply chain. The applicable ASIL is the highest inherited ASIL (of the item's safety goals) across the elements, of the item, that are developed by the supplier (see also ISO 26262-8:2018, 5.4.5); and

— a final functional safety assessment that includes a judgement of the functional safety achieved by the integrated item e.g. performed by the vehicle manufacturer. The applicable ASIL is the highest ASIL of the safety requirements (see also ISO 26262-2).

EXAMPLE 5 A vehicle manufacturer develops an item with an ASIL D Safety Goal (SG1) and an ASIL B Safety Goal (SG2), and will perform a functional safety assessment regarding this item. It is possible that, for example, a Tier 2 or Tier 3 supplier only develops ASIL B elements of the item, i.e. only elements that inherit the ASIL of SG2 (however, refer to ISO 26262-9:2018, Clause 6, if criteria for coexistence of elements are applicable). There is a recommendation in ISO 26262-2:2018, Table 1 to perform a functional safety assessment with independence I0 regarding this element development.

The scope, procedure (e.g. work products to be made available by the supplier, work products to be reviewed by the customer) and execution of a functional safety assessment concerning the interface between a customer and a supplier are specified in the corresponding Development Interface Agreement (see ISO 26262-8:2018, Clause 5).

EXAMPLE 6 DIA between a vehicle manufacturer (customer) and a Tier 1 supplier. DIA between a Tier 1 supplier (customer) and a Tier 2 supplier.

A possible manner to perform a functional safety assessment in the case of a distributed development is that the vehicle manufacturer and the suppliers in the supply chain each address those aspects of the assessment activities for which the respective party is responsible for, as follows:

— a supplier reviews the safety measures implemented in the developed elements including their appropriateness and effectiveness to comply with the corresponding safety goals or safety

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-10:2018

requirements (provided by the customer or developed by the supplier), and evaluates its implemented processes and the applicable work products. A supplier also evaluates the potential impacts of the developed elements on the item's functional safety, e.g. identifies whether implemented safety measures can lead to new hazards; and

— the vehicle manufacturer evaluates the functional safety of the integrated item. A part of the evaluation can be based on the work products or information provided by one or more suppliers, including reports of the functional safety assessments.

NOTE 3 A customer can evaluate the safety measures implemented by a supplier and the work products made available by a supplier. A customer can also evaluate the processes implemented by a supplier at the supplier's premises (see ISO 26262-8:2018, 5.4.3.1)

5.3 Understanding of safety cases

5.3.1 Interpretation of safety cases

The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk when operated in an intended context.

The guidance given here focuses on the scope of ISO 26262.

There are three principal elements of a safety case, namely:

— the safety goals and related safety requirements (safety objectives of the item or element);

— the safety argument; and

— the ISO 26262 series of standards work products (i.e. the evidence).

The relationship between these three elements, in the context of the ISO 26262 series of standards, is depicted in Figure 7.

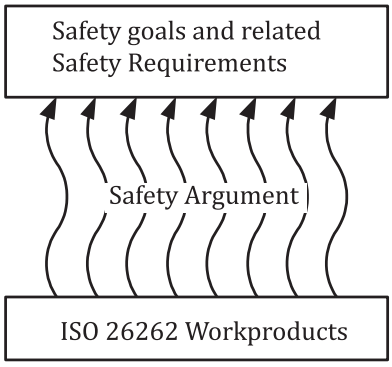


Figure 7 — Key elements of a safety case (see Reference [2])

The safety argument communicates the relationship between the evidence and the objectives. It is possible to present many pages of supporting evidence without clearly explaining how this evidence relates to the safety objectives. Both the argument and the evidence are crucial elements of the safety case. An argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without an argument is unexplained, resulting in a lack of clarity as to how the safety objectives have been satisfied. Safety cases are communicated through the development and presentation of safety case reports. The role of a safety case report is to summarise the safety argument and then reference the reports capturing the supporting safety evidence (e.g. test reports).

Safety arguments used to date in other industries have often been communicated in safety case reports through narrative text. Narrative text can describe how a safety objective has been interpreted, allocated and decomposed, ultimately leading to references to evidence that demonstrate fulfilment

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

of lower-level safety claims. Alternatively, or as a support, graphical argument notations (such as Claims–Argument–Evidence and the Goal Structuring Notation [2]) could be used to visually and explicitly represent the individual elements of a safety argument (requirements, claims, evidence and context) and the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument).

A safety argument that argues safety through direct appeal to features of the implemented item (e.g. the behaviour of a timing watchdog) is often termed a product argument. A safety argument that argues safety through appeal to features of the development and assessment process (e.g. the design notation adopted) is often termed a process argument.

Both types of argument can be used to achieve a sound argument for the safety of the item where a process argument can be seen as providing the confidence in the evidences used in the product argument.

5.3.2 Safety case development lifecycle

The development of a safety case can be treated as an incremental activity that is integrated with the rest of the development phases of the safety lifecycle.

NOTE The safety plan can include the planning for incremental steps and the preliminary versions of the safety case.

Such an approach allows intermediate versions of the safety case at given milestones of the product development. For example, a preliminary version of the safety case can be created after the verification of the technical safety requirements; an interim version of the safety case can be created after the verification of the system design; and the final version can be created just prior the final report of the functional safety assessment.

The safety case is subject to a confirmation review as given in ISO 26262-2:2018, 6.4.9.

If the item is modified, the impact on the safety case is evaluated and if necessary the safety case is updated considering the modifications.

6 Concept phase and system development

6.1 General

This clause provides an overview of the principles behind the hazard analysis and risk assessment using simplified examples to the concepts.

6.2 Example of hazard analysis and risk assessment

6.2.1 General

Consider the example of an item controlling an energy storage device embedded in the vehicle. For the purpose of this example, the stored energy is intended to be released only if the vehicle is running greater than or equal to 15 km/h. The release of the stored energy at less than 15 km/h can lead to the overheating and consequent explosion of the device.

6.2.2 HARA example 1

a) Hazard identification

The hazard, “unwanted release of energy of the device that can result in an explosion”, is identified.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

b) Hazardous event

The driving situation in which the identified hazard can lead to a hazardous event is considered as driving less than 15 km/h. If an unwanted release of energy due to a failure in the item occurs during this driving condition, the energy storage device could explode, causing severe harm to the occupants of the vehicle.

c) Classification of the identified hazardous event

The explosion leads to life-threatening injuries for the passengers of the vehicle, with survival uncertain: the severity could be estimated as S3.

The vehicle is travelling at a speed of less than 15 km/h. Based on traffic statistic for the target market of the vehicle, this condition occurs between 1 % and 10 % of the driving time: the exposure of this situation could be estimated as E3.

The ability of the driver or the passengers of the vehicles to control the item failure and the explosion of the device is considered as implausible: this controllability could be estimated as C3 (difficult to control or uncontrollable).

The application of ISO 26262-3:2018, Table 4: ASIL determination leads to an ASIL C.

6.2.3 HARA example 2

This clause considers the case where the impact of unwanted release of energy is inherently restricted by design improvement. This would result in an evaluation of the HARA as follows:

a) Hazard identification

As a hazard, “unwanted release of energy of the device that can result in an explosion”, is identified.

b) Hazardous event

For all driving situations an unwanted release of energy does not lead to a hazardous event. Therefore, the item failure cannot result in harm.

c) Classification of the identified hazardous event

Since the item failure does not lead to harm, the severity is classified as S0 and controllability does not need to be determined. Therefore, a safety goal does not need to be defined.

6.3 An observation regarding controllability classification

As explained in ISO 26262-3:2018, Clause 6, the controllability represents an estimation of the probability that the driver or other traffic participant is able to avoid the specific harm.

In the simplest case, only one outcome is considered for a given hazardous event and the controllability represents an estimation of the probability that this outcome is avoided. However, there can be other cases. For example, a severe outcome (e.g. severity class S2) can be possible but relatively easy to avoid (e.g. controllability C1) while a less severe outcome (e.g. S1) is more difficult to avoid (e.g. C3). Assuming that the exposure class is E4, the following set of values can be the result, which illustrates that it is not necessarily the highest severity that leads to the highest ASIL:

— E4, S2, C1 → ASIL A; and

— E4, S1, C3 → ASIL B.

In this example, ASIL B is an appropriate classification of the hazardous event.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

6.4 External measures

6.4.1 General

An external measure is a measure separate and distinct from the item that reduces or mitigates the risks resulting from a failure of the item.

NOTE 1 External measures can be considered in the HARA, if they are independent with regards to the function to be implemented by the item.

NOTE 2 External measures as a technical assumption to reduce an ASIL are validated according to ISO 26262-3:2018, 6.4.4.4.

6.4.2 Example of vehicle dependent external measures 1

Vehicle A is equipped with a manually operated transmission gear box which can be left in any gear, including neutral, upon key off. Vehicle B is equipped with an automatic gear box which, at key off, maintains one gear engaged and a normally closed clutch. Both vehicles have an additional item, Electrical Parking Brake (EPB).

A scenario is analysed for both vehicles which includes:

— The vehicle is parked (key off, driver not present);

— Vehicle is kerbside on an incline, located in a populated urban area; and

— A failure involving a sudden release of EPB occurs.

In this scenario, Vehicle A, when unintentionally left in neutral at key off, will potentially roll away if left unattended. This can result in an assessed controllability rating of C3, a severity rating of S2 or higher depending on the presence of nearby vulnerable persons, and an exposure ranking greater than E0. Depending on the exposure rating assigned, the ratings proposed result in an assigned ASIL between ASIL A and ASIL C or QM.

Vehicle B however always engages a gear, so it does not move. Thus there is no resulting hazard. The vehicle-dependent external measures included in this design contribute to the elimination of risk for this scenario, but only if the automatic gear box and the EPB can be shown to be sufficiently independent.

6.4.3 Example of vehicle dependent external measures 2

Vehicle A is equipped with dynamic stability control in addition to a stop-start feature. Vehicle B is only equipped with the stop-start feature.

A scenario is analysed for both vehicles which includes:

— The vehicle is being driven at medium-high speed (50 km/h < v < 90 km/h);

— The road surface is paved and dry, and in a suburban area;

— The vehicle is approaching a medium curvature bend in the road;

— The vehicle speed and road curvature contribute to a medium-high lateral acceleration; and

— A failure in the stop-start feature triggering an undesired engine shutdown results in a sudden loss of traction power during the scenario.

As a result of the sudden loss of traction power, a yaw moment is induced on the vehicle, requiring the driver to adjust steering input to re-establish the control of the vehicle. Performing this manoeuvre in Vehicle B can be shown to have a lower controllability, which can contribute to high risk. The risk classification will be dependent on the exposure rating assigned. By contrast, the dynamic stability control feature in Vehicle A limits the effects of the lateral instability. As a result, the controllability rating will be better for Vehicle A. Therefore, the vehicle-dependent external measures provided by the

© ISO 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018

dynamic stability control contribute to the reduction of risk for this scenario. However, this is the case only if it can be shown that the failure in the start-stop function being considered cannot propagate to the dynamic stability control function.

NOTE An in-depth analysis of the hazard used in the example can be found in Reference [6].

6.5 Example of combining safety goals

6.5.1 Introduction

Safety goals are top-level safety requirements for the item. They lead to the functional safety requirements needed to avoid an unreasonable risk for a hazardous event. They are determined in the concept phase in accordance with ISO 26262-3:2018, 6.4.4. When safety goals are similar or refer to the same hazard in different situations, they can be combined into a single safety goal with the highest ASIL of the original safety goals. This can simplify the further development, as fewer safety goals will be managed, while still covering all the identified hazards.

6.5.2 General

In the following example, the item, the safety goals and the ASIL classifications shown are only intended to illustrate the safety goal combination process. This example does not reflect the application of the ISO 26262 series of standards on a similar real-life project. In particular, it is not complete in terms of failure modes identification, situation analysis and the assessment of vehicle level effects.

For simplicity, the example is limited to the composition of two safety goals, but the same approach can be extended to a higher number of initial safety goals.

6.5.3 Function definition

Consider a vehicle equipped with an Electrical Parking Brake (EPB) system. The EPB system, when activated by a specific driver’s request, applies brake torque to the vehicle's rear wheels to prevent unintended vehicle movement while parked (parking function).

6.5.4 Safety goals applied to the same hazard in different situations

6.5.4.1 Hazard analysis and risk assessment

To simplify the example, consider just the following failure mode of the parking function:

— unintended parking brake activation.

NOTE In this context, the term “unintended activation” refers to function actuation without the driver’s request.

This failure mode can lead to different vehicle effects depending on the specific situation present when the fault occurs, as shown in Table 1.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-10:2018