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)

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

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.

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.

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.

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

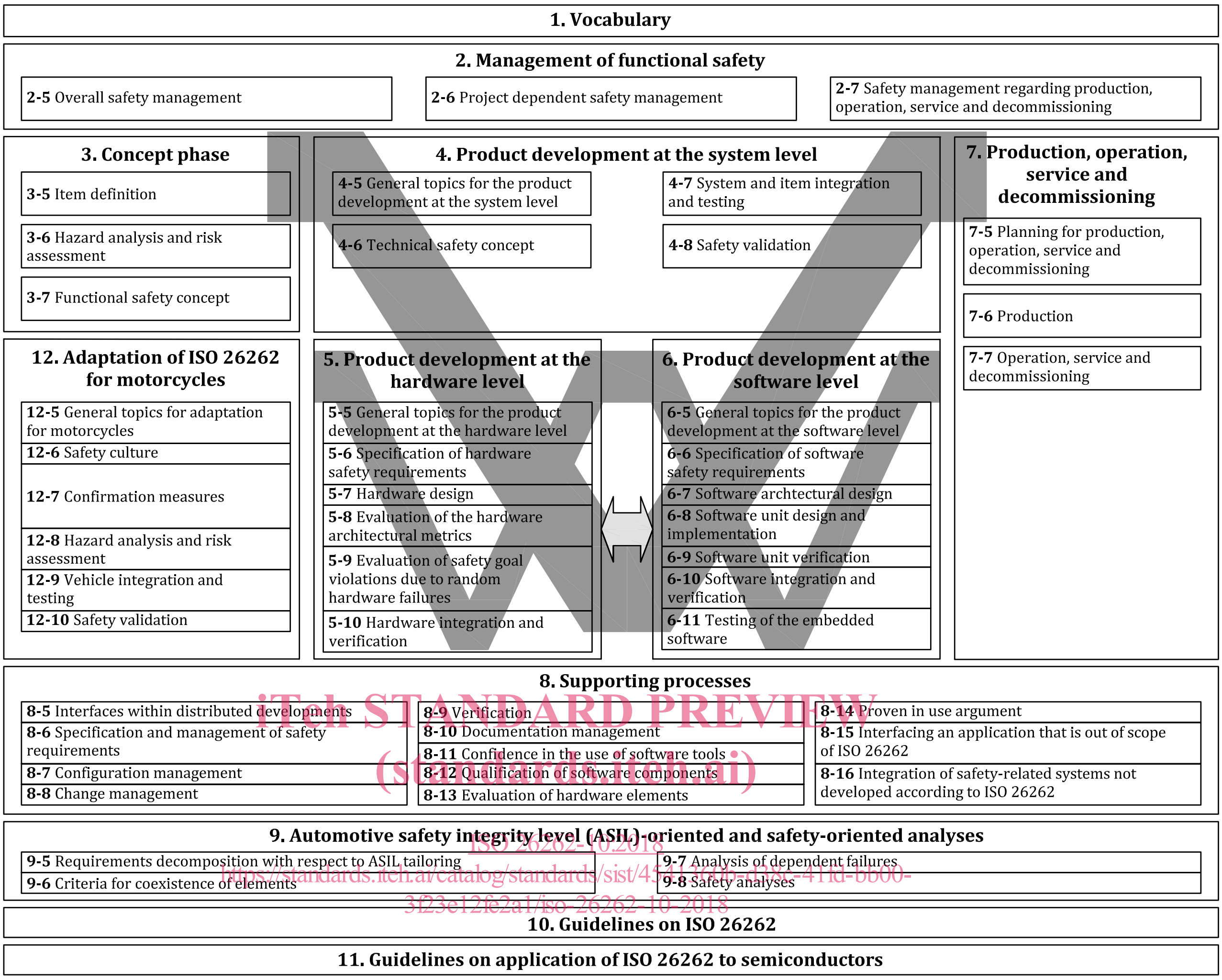


Figure 1 — Overview of the ISO 26262 series of standards

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*

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.

— 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.

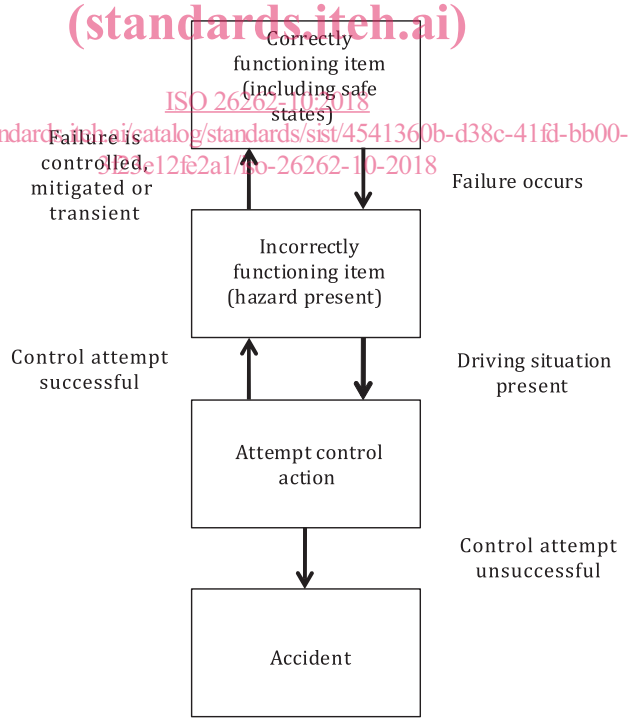


Figure 2 — State machine model of automotive risk

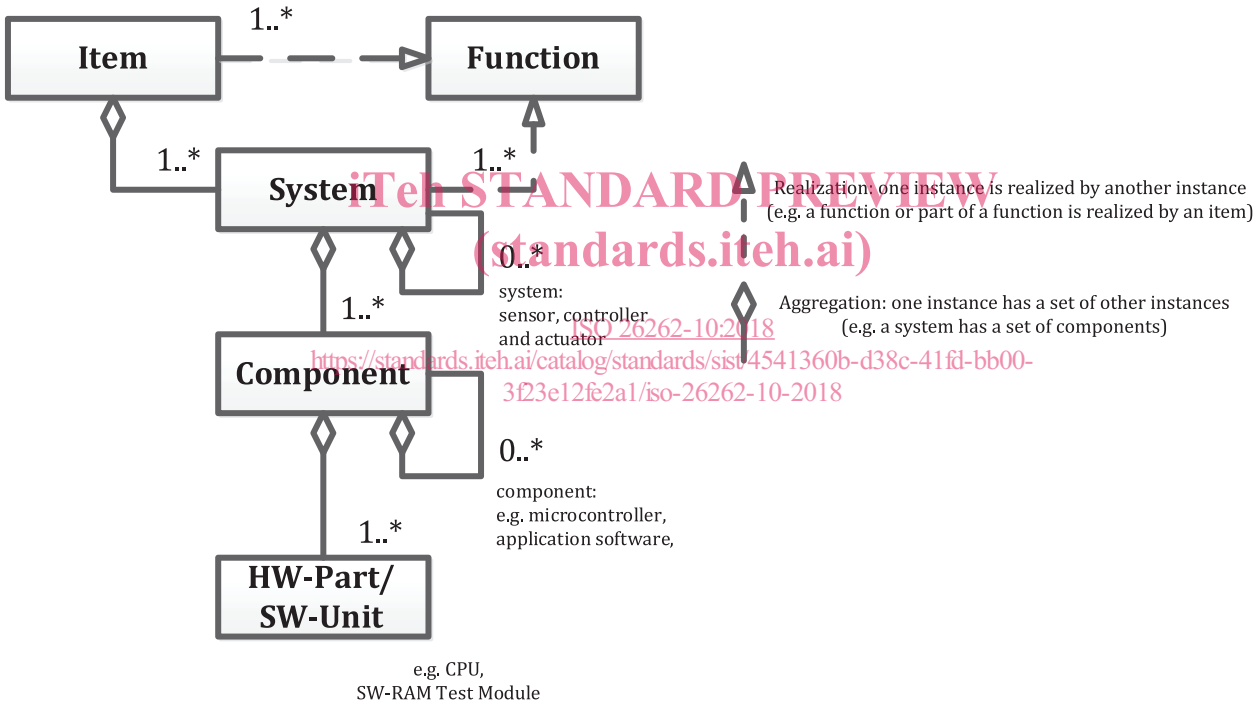
The requirements for hardware development (ISO 26262-5) and software development (ISO 26262-6) are adapted for the state-of-the-art in the automotive industry. For the methods listed in the ISO 26262 series of standards specific goals are provided. To achieve these goals, the provided methods can be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

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

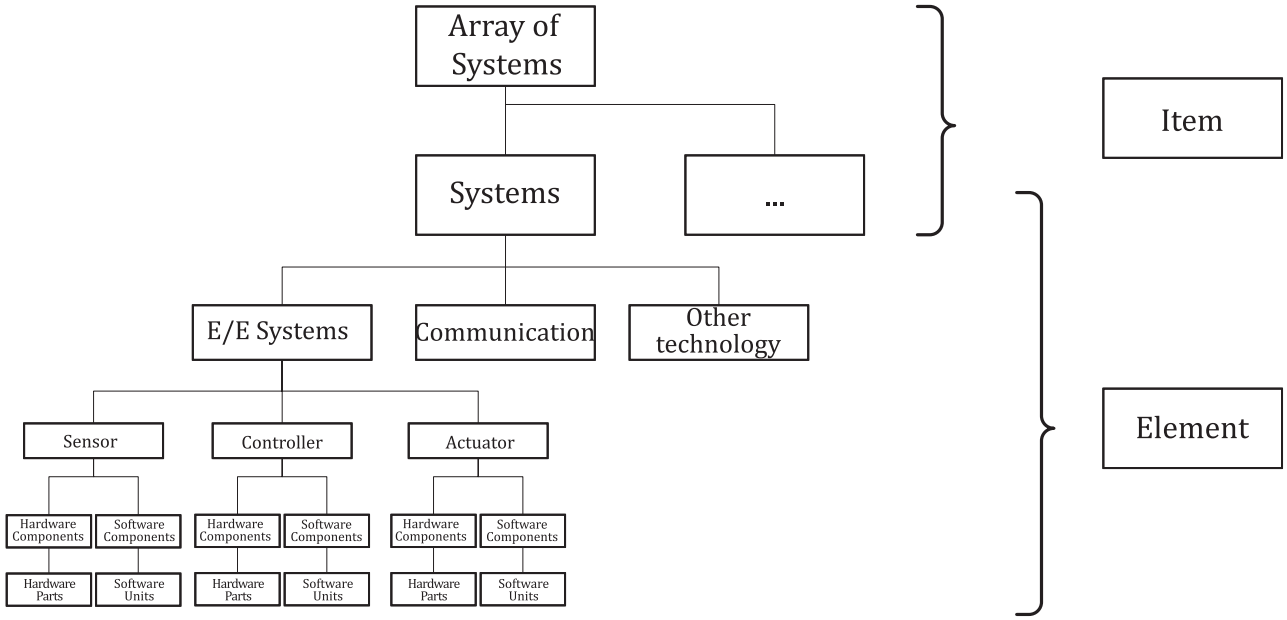


Figure 4 — Example item dissolution

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).