



# SLOVENSKI STANDARD SIST EN 62508:2010

01-december-2010

---

## Napotki o človeških vidikih zagotovitljivosti (IEC 62508:2010)

Guidance on human aspects of dependability (IEC 62508:2010)

Leitlinien zu den menschlichen Aspekten der Zuverlässigkeit (IEC 62508:2010)

Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement (CEI 62508:2010)

**(standards.iteh.ai)**

**Ta slovenski standard je istoveten z: EN 62508:2010**

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

### **ICS:**

03.120.01      Kakovost na splošno      Quality in general

**SIST EN 62508:2010**

**en**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN 62508:2010

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN 62508**

October 2010

ICS 03.120.01

English version

**Guidance on human aspects of dependability**  
(IEC 62508:2010)

Lignes directrices relatives aux facteurs  
humains dans la sûreté de fonctionnement  
(CEI 62508:2010)

Leitlinien zu den menschlichen Aspekten  
der Zuverlässigkeit  
(IEC 62508:2010)

This European Standard was approved by CENELEC on 2010-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

**CENELEC**

European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

**Management Centre: Avenue Marnix 17, B - 1000 Brussels**

## Foreword

The text of document 56/1365/FDIS, future edition 1 of IEC 62508, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62508 on 2010-10-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-07-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-10-01

Annex ZA has been added by CENELEC.

---

## Endorsement notice

The text of the International Standard IEC 62508:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60812:2006	NOTE Harmonized as EN 60812:2006 (not modified).
ISO 6385:2004	NOTE Harmonized as EN ISO 6385:2004 (not modified).
ISO 9000:2005	NOTE Harmonized as EN ISO 9000:2005 (not modified).
ISO 9241-1:1997	NOTE Harmonized as EN ISO 9241-1:1997 (not modified).
ISO 9241-2:1992	NOTE Harmonized as EN ISO 9241-2:1993 (not modified).
ISO 9241-3:1992	NOTE Harmonized as EN 29241-3:1993 (not modified).
ISO 9241-4:1998	NOTE Harmonized as EN ISO 9241-4:1998 (not modified).
ISO 9241-5:1998	NOTE Harmonized as EN ISO 9241-5:1999 (not modified).
ISO 9241-6:1999	NOTE Harmonized as EN ISO 9241-6:1999 (not modified).
ISO 9241-7:1998	NOTE Harmonized as EN ISO 9241-7:1998 (not modified).
ISO 9241-8:1997	NOTE Harmonized as EN ISO 9241-8:1997 (not modified).
ISO 9241-9:2000	NOTE Harmonized as EN ISO 9241-9:2000 (not modified).
ISO 9241-11:1998	NOTE Harmonized as EN ISO 9241-11:1998 (not modified).
ISO 9241-12:1998	NOTE Harmonized as EN ISO 9241-12:1998 (not modified).
ISO 9241-13:1998	NOTE Harmonized as EN ISO 9241-13:1998 (not modified).
ISO 9241-15:1997	NOTE Harmonized as EN ISO 9241-15:1997 (not modified).
ISO 9241-16:1999	NOTE Harmonized as EN ISO 9241-16:1999 (not modified).
ISO 9241-17:1998	NOTE Harmonized as EN ISO 9241-17:1998 (not modified).

ISO 9241-20:2008	NOTE	Harmonized as EN ISO 9241-20:2009 (not modified).
ISO 9241-110:2006	NOTE	Harmonized as EN ISO 9241-110:2006 (not modified).
ISO 9241-151:2008	NOTE	Harmonized as EN ISO 9241-151:2008 (not modified).
ISO 9241-171:2008	NOTE	Harmonized as EN ISO 9241-171:2008 (not modified).
ISO 9241-210:2010	NOTE	Harmonized as EN ISO 9241-210:2010 (not modified).
ISO 9241-300:2008	NOTE	Harmonized as EN ISO 9241-300:2008 (not modified).
ISO 9241-302:2008	NOTE	Harmonized as EN ISO 9241-302:2008 (not modified).
ISO 9241-303:2008	NOTE	Harmonized as EN ISO 9241-303:2008 (not modified).
ISO 9241-304:2008	NOTE	Harmonized as EN ISO 9241-304:2008 (not modified).
ISO 9241-305:2008	NOTE	Harmonized as EN ISO 9241-305:2008 (not modified).
ISO 9241-306:2008	NOTE	Harmonized as EN ISO 9241-306:2008 (not modified).
ISO 9241-307:2008	NOTE	Harmonized as EN ISO 9241-307:2008 (not modified).
ISO 9241-400:2007	NOTE	Harmonized as EN ISO 9241-400:2007 (not modified).
ISO 9241-410:2008	NOTE	Harmonized as EN ISO 9241-410:2008 (not modified).
ISO 11064-1	NOTE	Harmonized as EN ISO 11064-1.
ISO 11064-2	NOTE	Harmonized as EN ISO 11064-2.
ISO 11064-3	NOTE	Harmonized as EN ISO 11064-3.
ISO 11064-4	NOTE	Harmonized as EN ISO 11064-4.
ISO 11064-5	NOTE	Harmonized as EN ISO 11064-5.
ISO 11064-6	NOTE	Harmonized as EN ISO 11064-6.
ISO 11064-7	NOTE	Harmonized as EN ISO 11064-7.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

---

## Annex ZA (normative)

### Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60300-1	2003	Dependability management - Part 1: Dependability management systems	EN 60300-1	2003
IEC 60300-2	-	Dependability management - Part 2: Guidelines for dependability management	EN 60300-2	-
IEC 60300-3-15	-	Dependability management - Part 3-15: Application guide - Engineering of system dependability	EN 60300-3-15	-

ITeT STANDARD PREVIEW  
(standards.iteh.ai)

SIST EN 62508:2010

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>



IEC 62508

Edition 1.0 2010-06

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



Guidance on human aspects of dependability

Lignes directrices relatives aux facteurs humains dans la sûreté de  
fonctionnement

[SIST EN 62508:2010](https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010)

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX

**XA**

ICS 03.120.01

ISBN 978-2-88912-023-9

## CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references.....	7
3 Terms, definitions and abbreviations.....	7
3.1 Terms and definitions.....	7
3.2 Abbreviations.....	10
4 Human aspects.....	10
4.1 Overview.....	10
4.2 Components of the system and their interactions.....	11
4.2.1 Introductory remark.....	11
4.2.2 Goals.....	11
4.2.3 Humans.....	12
4.2.4 Machine (interactive system).....	12
4.2.5 Social and physical environment.....	13
4.2.6 Output.....	13
4.2.7 Feedback from the machine to the person.....	13
4.3 Human characteristics.....	14
4.3.1 Introductory remark.....	14
4.3.2 Human limitations.....	14
4.3.3 Comparison of humans and machines.....	14
4.4 Human performance shaping factors.....	15
4.4.1 External performance shaping factors.....	16
4.4.2 Internal performance shaping factors.....	16
4.5 Human reliability analysis (HRA).....	16
4.5.1 Overview.....	16
4.5.2 Identifying the potential for human error.....	17
4.5.3 Analysing human failures to define countermeasures.....	17
4.5.4 Quantification of human reliability.....	18
4.6 Critical systems.....	18
4.7 Human-centred design guidelines.....	19
4.8 Human-centred design process.....	20
4.8.1 Human-centred design principles within the design process.....	20
4.8.2 Human-centred design activities.....	21
5 Human-oriented design in the system lifecycle.....	21
5.1 Overview.....	21
5.2 The system life cycle.....	22
5.3 Integrating human-oriented design in systems engineering.....	23
6 Human-oriented design at each life cycle stage.....	24
6.1 Overview.....	24
6.2 Concept/definition stage.....	24
6.2.1 Concept.....	24
6.2.2 Human-centred design planning.....	24
6.2.3 Understanding needs.....	25
6.2.4 System requirements.....	25
6.2.5 Human-centred design requirements.....	25



6.3	Design/development.....	26
6.4	Realization/implementation.....	26
6.5	Operation/maintenance .....	27
6.6	Enhancement .....	27
6.7	Retirement/decommission .....	28
6.8	Outsourcing projects and related human-centred design issues.....	28
7	Human-centred design methods .....	29
7.1	Classification of human-centred design activities.....	29
7.2	Applications of human-centred design methods.....	30
	Annex A (informative) Examples of HRA methods.....	31
	Annex B (informative) Summary of human-oriented design activities and their impact on system dependability .....	37
	Annex C (informative) Best practices for human-centred design.....	41
	Bibliography.....	47
	Figure 1 – Components of the system and their interactions .....	11
	Figure 2 – Human performance shaping factors .....	16
	Figure 3 – Simple model of human information processing.....	17
	Figure 4 – Human-centred design activities .....	21
	Figure 5 – Human aspects of the system life cycle.....	23
	Table 1 – People who influence dependability.....	12
	Table A.1 – HRA methods and their application.....	31
	Table B.1 – Automation .....	37
	Table B.2 – Design for maintainability.....	37
	Table B.3 – Computer-human interface.....	38
	Table B.4 – Incorporation of displays, controls and alarm functions .....	39
	Table B.5 – Incorporation of input devices .....	39
	Table B.6 – Environment.....	40
	Table B.7 – Safety .....	40
	Table B.8 – Security .....	40
	Table C.1 – Examples of methods and techniques that contribute to best practices .....	41

iTeH STANDARD PREVIEW  
(standards.iteh.ai)

SIST EN 62508:2010  
<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

## GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62508 has been prepared by IEC technical committee 56: Dependability.

This first edition cancels and replaces IEC/PAS 62508 published in 2007.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1365/FDIS	56/1373/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

## **iTeh STANDARD PREVIEW (standards.iteh.ai)**

[SIST EN 62508:2010](#)

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

## INTRODUCTION

This International Standard provides guidelines on human aspects of dependability of systems. It fills the need for a standard to address the dependability of human/machine systems.

It gives guidance on how the human aspects of dependability can be considered at all the system life cycle stages, including ergonomic principles during design and human reliability understanding for system applications.

This standard provides an overview of the principles with some examples of the types of methods that can be used.

It is intended that a supporting standard, which describes more detailed methods that include quantification of human reliability will follow the issue of this standard in due course.

This standard contains recommendations, and does not include any requirements. Attention is drawn to the possibility of the existence of regulatory requirements for systems covered by the scope of this standard.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN 62508:2010](#)

<https://standards.iteh.ai/catalog/standards/sist/9369a490-8ebb-4241-8ce6-4672539c059b/sist-en-62508-2010>

## GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

### 1 Scope

This International Standard provides guidance on the human aspects of dependability, and the human-centred design methods and practices that can be used throughout the whole system life cycle to improve dependability performance. This standard describes qualitative approaches. Examples of quantitative methods are given in Annex A.

This International Standard is applicable to any area of industry where human/machine relationships exist, and is intended for use by technical personnel and their managers.

This International standard is not intended to be used for certification, regulatory or contractual use.

### 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.

IEC 60300-1:2003, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

IEC 60300-3-15, *Dependability management – Part 3-15: Application guide – Engineering of system dependability*

### 3 Terms, definitions and abbreviations

For the purposes of this document, the following terms, definitions and abbreviations apply.

NOTE Certain terms have been taken from the draft text of the second edition of IEC 60050-191, *International Electrotechnical Vocabulary – Part 191: Dependability*, currently under consideration.

#### 3.1 Terms and definitions

##### 3.1.1

##### **dependability**

ability to perform as and when required <sup>1</sup>

NOTE 1 Dependability characteristics include availability and its inherent or external influencing factors, such as reliability, fault tolerance, recoverability, integrity, security, maintainability, durability and maintenance support.

NOTE 2 Dependability is also used descriptively as an umbrella term for time-related quality characteristics of a product or service, and it can also be expressed as a grade, degree, confidence or probability of fulfilling a defined set of characteristics.

NOTE 3 Specifications for dependability characteristics typically include: the function the product is to perform; the time for which that performance is to be sustained; and the conditions of storage, use and maintenance. Requirements for safety, efficiency and economy throughout the life cycle can also be included.

<sup>1</sup> Future IEC 60050-191, definition 191-41-26, second edition, under consideration.

### 3.1.2 ergonomics human factors HF

scientific discipline concerned with the understanding of interactions among human and other elements of a system that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance

[ISO 6385:2004, definition 2.3, modified]

### 3.1.3 error resistance

ability of a system to minimize the probability of human error occurring

### 3.1.4 error tolerance

ability of a system or component to continue normal operation despite the presence of erroneous inputs

[ISO/IEC 24765:2009, definition 3.1034]

### 3.1.5 human aspects

abilities, limitations, and other human characteristics that are relevant to the design, operation and maintenance of systems and/or their components affecting overall system performance

### 3.1.6 human-centred design

approach to system design and development that aims to make interactive systems more usable by focussing on the use of the system, applying human factors, ergonomics and usability knowledge and techniques

NOTE 1 Usable systems provide a number of benefits including improved productivity, enhanced user well-being, avoidance of stress, increased accessibility, and reduced risk of harm.

NOTE 2 This standard uses the term "human-oriented design" to refer to the need to take account of humans in system design, but retains the term "human-centred design" used in ISO standards to refer to the specific principles and activities.

NOTE 3 The term "human-centred design" is used rather than "user-centred design" in order to emphasize that this standard addresses a number of stakeholders, not just those typically considered as users. However, in practice, these terms are often used synonymously.

[ISO 9241-210:–, definition 2.7, modified] <sup>2</sup>

### 3.1.7 human error

discrepancy between the human action taken or omitted, and the action intended<sup>3</sup>

### 3.1.8 human error probability

HEP  
probability that an operator will fail in an assigned task

NOTE 1 This can be based on the ratio of the average number of errors within a certain task in relation to the overall number of error possibilities for this type of task.

<sup>2</sup> To be published.

<sup>3</sup> Future IEC 60050-191, definition 191-43-13, second edition, under consideration.

NOTE 2 Human error probability is expressed in a distribution where the distribution needs to be determined in accordance with the human variations and situational variations under which the task needs to be conducted.

### 3.1.9

#### **human failure**

deviation from the human action required to achieve the objective, regardless of the cause of that deviation

NOTE For any particular system or situation the range of human failures is the combination of human errors and violations that lead to system failures and/or hazardous outcomes.

### 3.1.10

#### **human-oriented design**

takes a user-centric approach to design by adapting technologies to meet human performance requirements, account for human limitations, achieve mental comfort and enhance overall system performance

### 3.1.11

#### **human reliability**

capability of human beings to complete a task under a given condition within a defined period of time and within the acceptance limits

### 3.1.12

#### **human reliability analysis**

HRA

systematic process to evaluate human reliability

NOTE Evaluation methods can be just qualitative but can be expanded to provide quantitative results.

### 3.1.13

#### **mistake**

deficiency or failure in the judgemental or inferential process involved in selection of an objective or in specification of the means to achieve it irrespective of whether or not the actions run according to plan

### 3.1.14

#### **performance shaping factors**

characteristics of the external environment, of the task and of humans that shape individual performance

### 3.1.15

#### **requirement**

need or expectation that is stated, generally implied or obligatory

[ISO 9000:2005, definition 3.1.2]

NOTE In the context of this standard, this is a need or expectation which should be met or possessed by a system, system component, product, or service.

### 3.1.16

#### **situational awareness**

human perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future

### 3.1.17

#### **system**

set of interrelated or interacting elements

[ISO 9000:2005, definition 3.2.1]