# IEC 62508

Edition 1.0 2010-06

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Guidance on human aspects of dependability

## Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement

## About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

## About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00



## A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

## A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

# IEC 62508

Edition 1.0 2010-06

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Guidance on human aspects of dependability

## Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement



INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX **XA**

ICS 03.120.01

ISBN 978-2-88912-023-9

CONTENTS

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.**

# 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.

# 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 [1]

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.

---

[1] 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] [2]

**3.1.7**
**human error**
discrepancy between the human action taken or omitted, and the action intended[3]

**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.

---

2 To be published.

3 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]

NOTE 1 In the context of dependability, a system will have:

– a defined purpose expressed in terms of intended functions;
– stated conditions of operation/use; and
– defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1:2003, definition 3.6]

NOTE 3 For some systems, such as information technology products, data is an important part of the system elements.

NOTE 4 Humans can form part of a system.

**3.1.18**
**violation**
deliberate but not necessarily reprehensible deviation from practices deemed necessary

### 3.2 Abbreviations

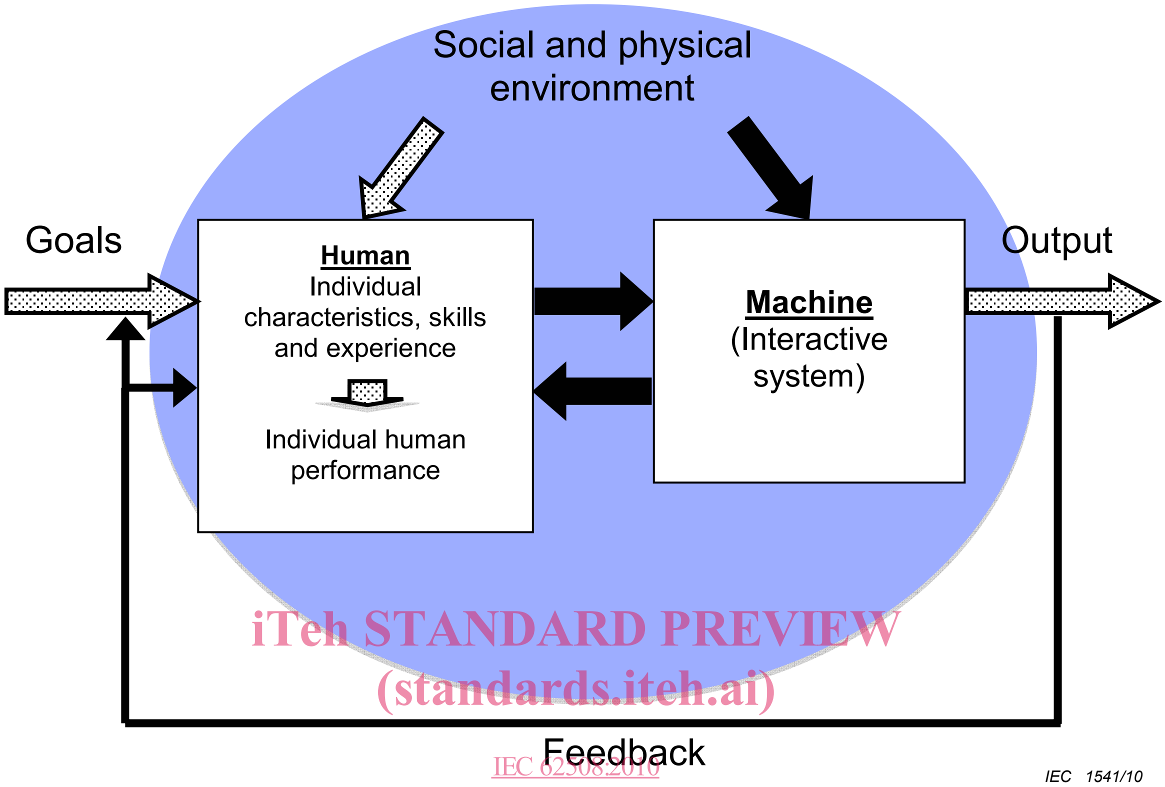
| | |
|---|---|
| ASEP | Accident Sequence Evaluation Program |
| ATHEANA | A Technique for Human Error ANAlysis |
| CAD | Computer Aided Design |
| CAHR | Connectionism Assessment of Human Reliability |
| CARA | Controller Action Reliability Assessment |
| COTS | Commercial Off The Shelf |
| CPC | Common Performance Condition |
| CREAM | Cognitive Reliability and Error Analysis Method |
| EFC | Error Forcing Context |
| ESAT | ExpertenSystem zur Aufgaben-Taxonomie (expert system for task taxonomy) |
| FMEA | Failure Modes and Effects Analysis |
| FMECA | Failure Modes Effects and Criticality Analysis |
| HCD | Human-Centred Design |
| HCR | Human Cognitive Reliability |
| HEART | Human Error Assessment and Reduction Technique |
| HEP | Human Error Probability |
| HF | Human Factors |
| HRA | Human Reliability Analysis |
| HR | Human Resources |
| HS | Human System |
| HSI | Human System Interaction |
| ILS | Integrated Logistics Support |
| MERMOS | Méthode d'Evaluation de la Réalisation des Missions Opérateur pour la Sûreté (method for the evaluation of the relisation of an operator's mission regarding safety) |
| ORE | Operator Reliability Experiments |
| PSF | Performance Shaping Factor |
| RR | Reliability Rating |
| SHERPA | Systematic Human Error Reduction and Prediction Approach |
| SLI | Success Likelihood Index |
| SLIM | Success Likelihood Index Methodology |
| SPAR-H | Standardized Plant Analysis Risk |
| THERP | Technique for Human Error Rate |
| UI | User Interface |



## 4 Human aspects

### 4.1 Overview

Human actions can have a strong influence on the dependability of the whole system and the quality of the output. Therefore important benefits accrue from consideration of human aspects, among which are preventing failures, improving system performance, ensuring safety, increasing reliability and enhancing cost effectiveness. A system that requires human interaction involves human(s), machine(s) and the social and physical environment in which they operate. The dependability of the system and the efficiency and effectiveness with which the goals of the system are achieved depend on each component of the system individually and the interactions between them (Figure 1).




IEC 1541/10



**Figure 1 – Components of the system and their interactions**

The grey arrows represent the performance shaping factors (PSFs) (described in 4.4).

The components shown in Figure 1 are as follows.

- Goals: what the work system has to achieve (4.2.2).
- Human: person who performs the task (4.2.3).
- Machine: interactive system designed to support achievement of the work system goals (4.2.4).
- Environment: social and physical factors that can influence the human(s) and machine (4.2.5).
- Output: that which should be achieved with the required level of effectiveness and efficiency (4.2.6).
- Feedback: feedback coming from the machine (4.2.7).

## 4.2 Components of the system and their interactions

### 4.2.1 Introductory remark

This subclause describes each component of Figure 1.

### 4.2.2 Goals

The objective of the work system is to achieve goals with a desired effectiveness and efficiency.

### 4.2.3 Humans

The role of humans in the system is to perform a task or interact with a machine in order to achieve a defined goal. The human operator can either have a monitoring role (such as in a process control or road traffic control room), or an active role (for example when resolving a road traffic incident).

Human influence can both be negative (e.g. human errors and violations) or positive (e.g. preventing system breakdowns or system problems). Humans can influence the system through action or inaction. Even in an automated system a human is part of the system, through design, maintenance and monitoring functions.

A range of people (shown in Table 1) may be involved in the different phases in the life cycle of a system each influences the dependability of the system through their actions and decisions.

**Table 1 – People who influence dependability**

| Job function | Examples of influence |
|---|---|
| Project manager | Awareness of dependability needs in system concepts |
| Designer | • Takes account of human factors in normal use and reasonably foreseeable misuse<br>• Designs for recognition and recovery from fault conditions including where there are multiple failure modes |
| Operational procedure writer | Establishes procedures that minimize human failures |
| Operational manager and supervisor | • Ensures appropriate working conditions resources, communication, feedback and training<br>• Motivates operators<br>• Ensures compliance with procedures |
| Operator | Observes and reports consequences of human error |
| Trainer | Highlights error-prone situations in training |
| Maintenance personnel | Understand, interpret and ensure compliance with procedures |



Human performance including strengths and limitations and the potential for humans to improve or degrade system operation should be taken into account when considering total system dependability. Although this appears to be additional work with financial implications, the cost of failure, if total system dependability is not considered, could be significant. The possible adverse consequences of human failures (including mistakes, slips, lapses, violations or malicious human actions) are particularly important when the human is part of a complex system with safety, security or mission critical applications. Human error can also have severe consequences in business and e-commerce environments.

For details of human characteristics, see 4.3.

### 4.2.4 Machine (interactive system)

The machine is designed to achieve functional and performance objectives within the environments in which it is to function.

During operation the machine receives input from the human through its controls and will provide output that progresses the system's task. The output will often be displayed to provide feedback to the human on the operation of the machine.

For the system as a whole to work effectively the interface and interaction between the machine and the people who work with it at all stages of the life cycle from design to disposal needs to take account of the human aspects. These include the fundamental human characteristics together with specific skills and experience, and the tasks that are to be performed. In particular, the interaction between the human operator and the machine (i.e. tasks, displays and controls) should be designed to be easy for the operator to use and to ensure acceptable levels of mental comfort.

#### 4.2.5 Social and physical environment

##### 4.2.5.1 Social environment

Organizational structure, work flows and the resulting social factors influence the human and system performance and need to be designed to support efficient and reliable human performance. An organizational structure is characterized by the transfer of tasks (delegation), decision competence, information, communication and decision paths as well as the number of hierarchy levels. The work process is characterized for example by the work flow method, the shift system, the work time and the work planning and execution.

Other features like leadership behaviour, participation, safety culture and climate can also influence human motivation and behaviour when using a system.



##### 4.2.5.2 Physical environment

Physical environmental factors that affect people, and hence system reliability, include light, noise, mechanical vibrations, climate, dirt, humidity, air pressure, toxic gas and radiation. Environmental factors can directly influence the capabilities of human beings (e.g. noise, toxic gas, etc.), or they can influence interactions between people and machines (e.g. mechanical vibration) or they can influence the machine itself (e.g. side winds when driving a car). However, apart from their negative effects, they can also provide a feedback function that enhances the ability of the human to interact effectively with the machine (e.g. the engine noise/vibration when driving a car).



Some factors of the physical environment can require people to use protective equipment (e.g. breathing apparatus). Some individual human limitations can require the use of assistive technologies (e.g. reading spectacles or specialized input devices). These technologies can have an effect on their ability and will need to be taken into account in design.

#### 4.2.6 Output

The task goals should be achieved with the required level of effectiveness and efficiency.

#### 4.2.7 Feedback from the machine to the person

Appropriate feedback from the machine is an important characteristic of dependable design. Feedback concerning input occurs from the machine to the person through sonic, visual and tactile signals. Feedback concerning the output of the system as a whole provides information on the achievement of the goals.

Feedback is important for a number of reasons. It allows a person to correct undesired behaviour of the machine or the system as a whole in order to improve performance or to correct undesired actions. In addition, lack of appropriate feedback can produce errors, e.g. when a computer is slow to provide visual feedback in response to the delete button, the operator will often repeat the action. Feedback can also contribute to performing a task more accurately, e.g. feedback from the car brake pedal helps the driver brake smoothly. Feedback