BS EN 62508:2010

Guidance on human aspects of dependability

Documents
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN 62508:2010. It is identical to IEC 62508:2010.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology.

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.

© BSI 2010

ISBN 978 0 580 61716 4

ICS 03.120.01

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 30 November 2010.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS 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

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 62508:2010 E

Documents
Document Sharing Hub

Full document details: BS EN 62508:2010

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).

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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.

Documents
Document Sharing Hub
Full document details: BS 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.

Publication	Year	Title	EN/HD	Year
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	-

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

CONTENTS

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

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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

Documents
Document Sharing Hub
Full document details: BS 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.

Documents
Document Sharing Hub
Full document details: BS 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 [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.

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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.

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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]

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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

AVA Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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).

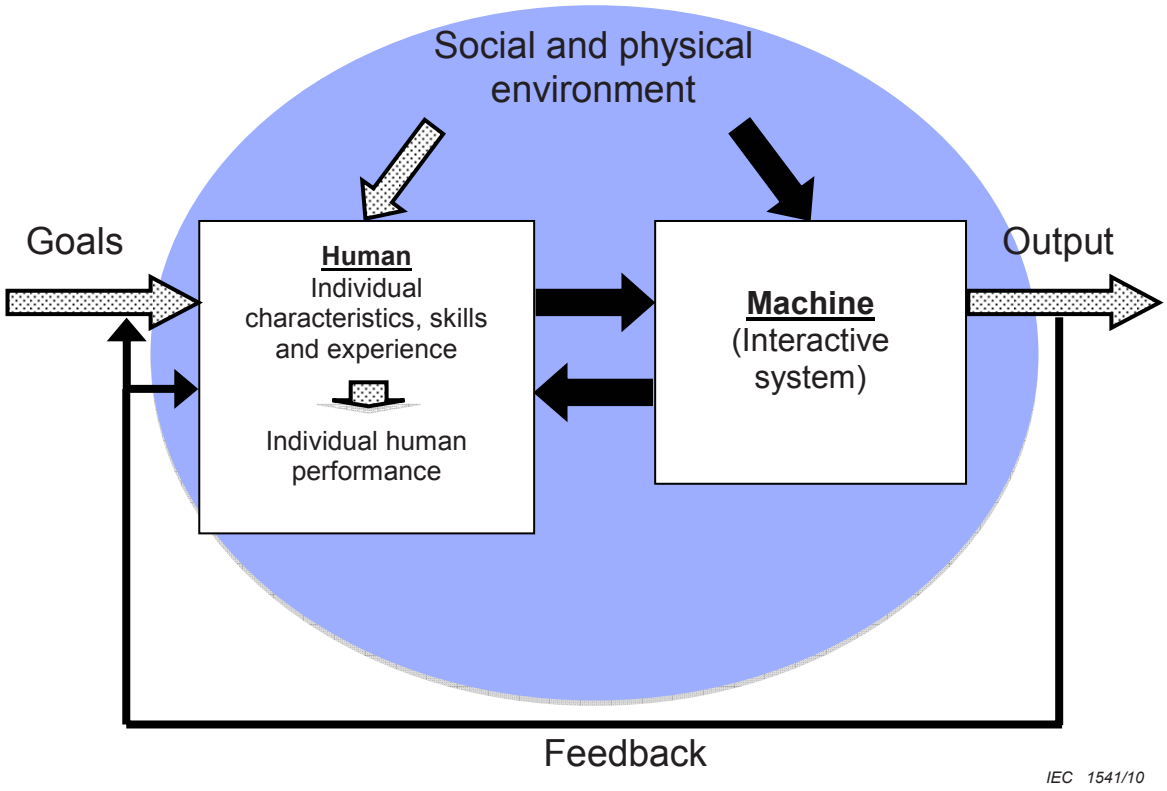

Figure 1 – Components of the system and their interactions

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.

AVA Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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 • 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 • Motivates operators • 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.

Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

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

AVA Documents
Document Sharing Hub
Full document details: BS EN 62508:2010

from the machine and the system also help provide situational awareness. In some circumstances, feedback can result in a change to the goals.

4.3 Human characteristics

4.3.1 Introductory remark

Human beings have a set of physical, cognitive and psychological characteristics that vary from person to person (4.5.2). These characteristics provide fundamental limitations to the human capabilities that need to be taken into account in systems design. Appropriate training and experience will enable people to work more effectively, but only within their limitations.

Human reliability and performance will be influenced by the design of the machine and by the physical and social environment (4.5.1). To ensure a working situation with high dependability, the system should be designed so that the stress on the human being due to the work task, work environment and technical design remains within acceptable limits.

4.3.2 Human limitations

The design should take account of human limitations.

a) Physical limitations

- Anthropometric and biomechanical constraints.
- Sensory constraints (e.g. the range of signals that can be perceived and differentiated).

b) Cognitive limitations

- The time needed between perception of a signal and an action in response. This can range from a few hundred milliseconds for skill-based actions where response is quasi automatic (and is not reasoned), to several seconds or minutes where reasoning and analysis is necessary.
- Limitations of short-term memory. Only 5 to 7 items of information can be held in short-term memory. For larger amounts of information, mental models or patterns are constructed.
- Limitations on the amount of information that can be processed at one time (working memory).
- The inability to focus effectively on more than one task at a time or process information in parallel.
- Potential for loss of situational awareness resulting in actions based on incorrect perception of reality.

c) Psychological limitations

- Performance degradation due to physical and mental fatigue or boredom.
- Tendency for decisions and actions to be based on emotional rather than reasoned responses particularly under situations of stress.

Since these characteristics of humans cannot be designed out of the system, the division of tasks between people and the rest of a system and the design of technical systems and interfaces have to be taken into account. The relative strengths of humans and machines should be considered (4.4.3).

4.3.3 Comparison of humans and machines

The allocation of activities and operational steps between human beings and machines should take into account the relative strengths of humans and machines.

AVA Documents
Document Sharing Hub

Full document details: BS EN 62508:2010