

Australian Standard[®]

Guidance on human aspects of dependability



This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 19 October 2011. This Standard was published on 14 November 2011.

The following are represented on Committee QR-005:

- Asset Management Council
 - Australian Industry Group
 - Australian Organisation for Quality
 - CSIRO Information and Communication Technologies Centre
 - Department of Defence (Australia)
 - Energy Networks Association
 - Engineers Australia
 - Independent Transport Safety & Reliability Regulator
 - Risk Management Association of Australia
 - Risk Management Institution of Australasia
 - The University of New South Wales
 - University of Wollongong
-

This Standard was issued in draft form for comment as DR AS IEC 62508.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

Guidance on human aspects of dependability

First published as AS IEC 62508—2011.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9959 4

PREFACE

This Standard was prepared by the Standards Australia Committee QR-005, Dependability.

The objective of this Standard is to provide guidance on human aspects of dependability and the application of human centred design methods throughout the system lifecycle to improve dependability performance. The standard applies to any industry where human machines relationships exist and is intended for technical personnel and their managers.

This Standard is identical with, and has been reproduced from IEC 62508, Ed.1.0 (2010), *Guidance on human aspects of dependability*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number appears on the cover and title page while the International Standard number appears only on the cover.
- (b) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
IEC		AS IEC	
60300	Dependability management	60300	Dependability management
60300-1	Part 1: Dependability management systems	60300.1	Part 1: Dependability management systems
60300-2	Part 2: Guidance for dependability programme management	60300.2	Part 2: Guidance for dependability programme management
60300-3-15	Part 3-15: Application guide—Engineering of system dependability	60300.3.15	Part 3.15: Application guide—Engineering of system dependability

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

CONTENTS

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

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.

AUSTRALIAN 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 intended³

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

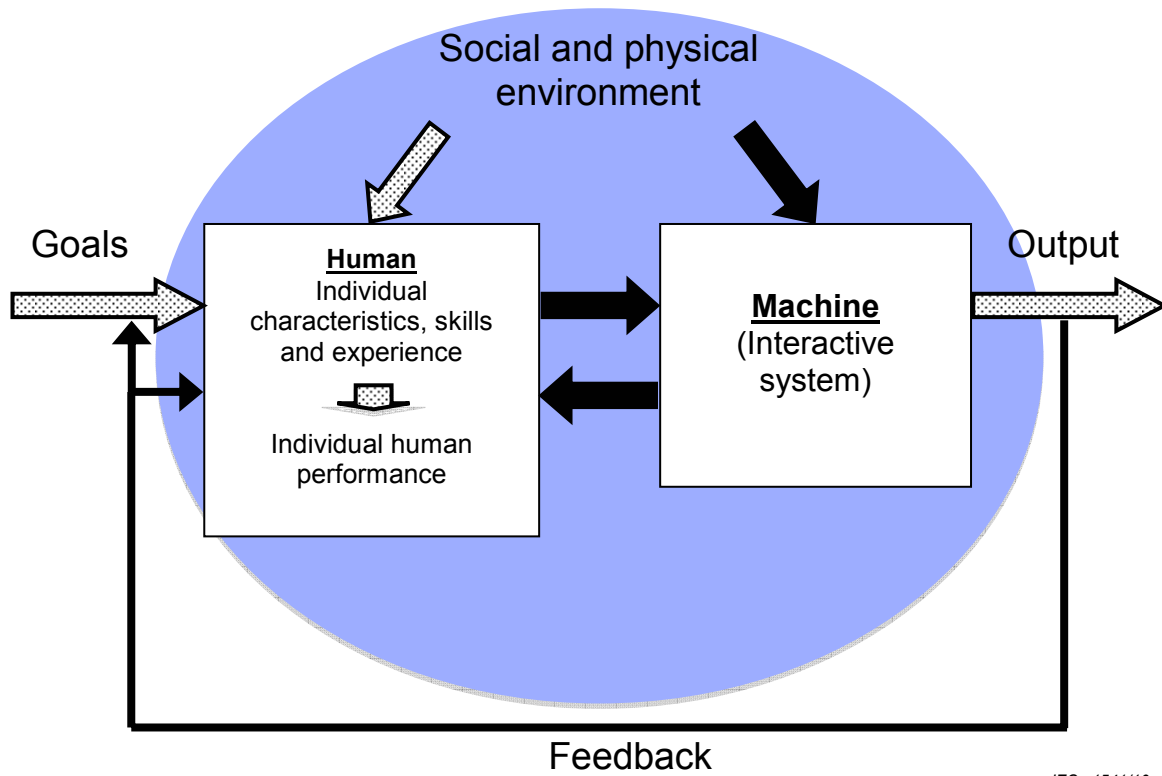
ASEP	Accident Sequence Evaluation Program
ATHEANA	A Technique for Human Error ANALysis
CAD	Computer Aided Design
CAHR	Connectionism Assessment of Human Reliability
CARA	Controller Action Reliability Assessment
COTS	Commercial Off The Shelf
CPC	Common Performance Condition
CREAM	Cognitive Reliability 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 Sécurité (method for the evaluation of the realisation 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 • 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.

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

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.

a) Human strengths

- Ability to perceive patterns of light or sound.
- Ability to improvise and use flexible procedures.
- Ability to store very large amounts of information for long periods and to recall relevant facts at the appropriate time.
- Ability to reason inductively.
- Ability to exercise judgement.

b) Machine strengths

- Ability to detect small amounts and a wider range of visual and acoustic signals.
- Ability to respond quickly to control signals, and to apply great force smoothly and precisely.
- Ability to perform repetitive and routine tasks consistently and accurately.
- Ability to store information briefly and then to erase it completely.
- Ability to reason deductively, including computational ability.
- Ability to handle highly complex operations and to do many different things at once.

There are major differences between humans and machines.

- Machines can be modified, redesigned, and retrofitted whereas humans cannot. Humans are born with innate, genetically determined differences that are shaped by the environment. Innate aptitudes or abilities are developed through education and training.
- Machines can be manufactured to provide exact output and duplicate precise operation. Humans are not identical and vary across all sensory, cognitive, physical and performance characteristics. Specific aspects of human performance can be made more equal through selection and training.

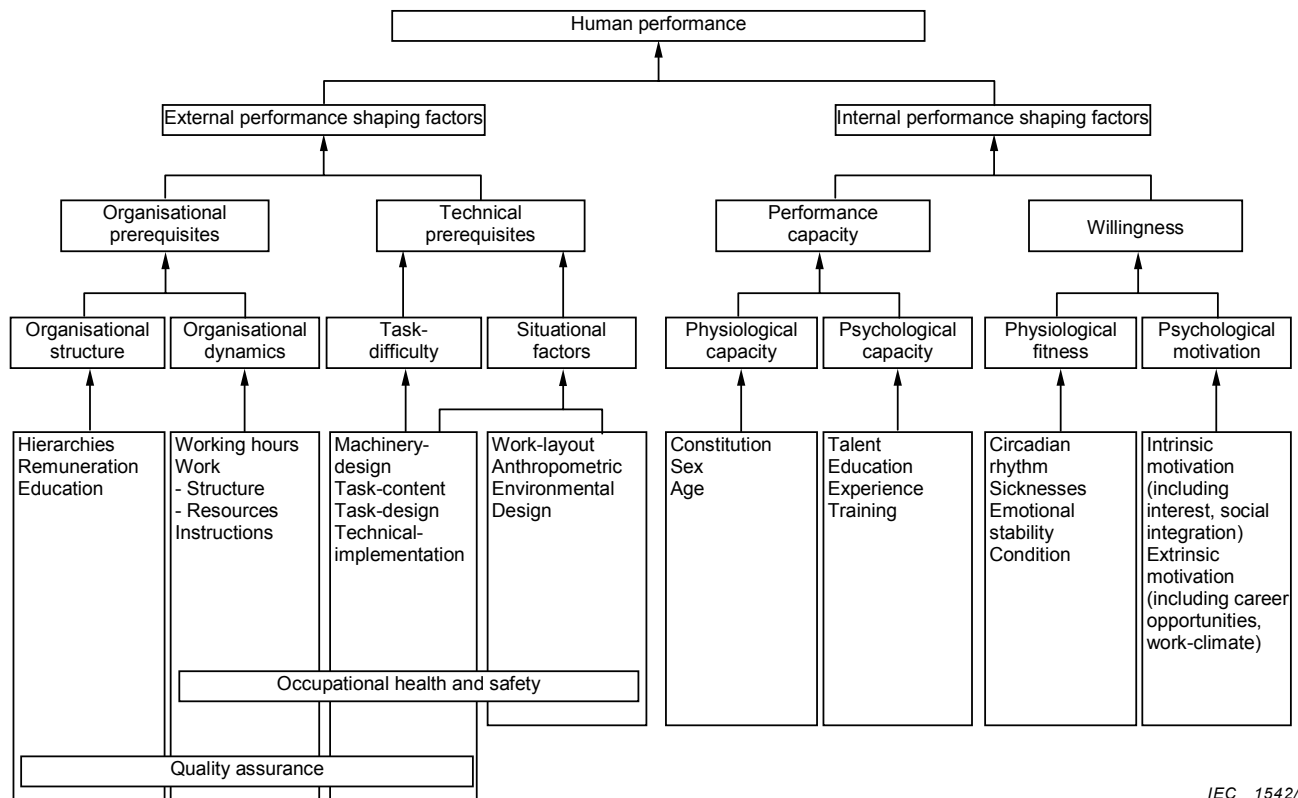
4.4 Human performance shaping factors

4.4.1 General

The performance and reliability of people within a system will vary depending on a range of internal and external conditions that differ from person to person and from one instant to another. The factors that influence the capability of human beings to reliably accomplish a task are called performance shaping factors (also known as the context of use).

Figure 1 indicates the types of performance shaping factors with grey arrows.

Figure 2 provides examples distinguishing between external and internal performance shaping factors.



IEC 1542/10

Figure 2 – Human performance shaping factors

4.4.2 External performance shaping factors

External performance shaping factors are the result of organizational and technical prerequisites. Organizational prerequisites (4.2.5.1) can often only be described qualitatively. Technical prerequisites including machine design (4.2.4) and environmental factors (4.2.5.2), on the other hand, can most often be described quantitatively.

Taking account of the external performance shaping factors in design will have a positive impact on the performance.

4.4.3 Internal performance shaping factors

Internal performance shaping factors can be separated into performance capacity and willingness. They represent factors caused by physiological and psychological variations in people and are shown as “individual characteristics, skills and experience” in Figure 1.

These include human limitations (4.3.2), and differences in size and strength, differences in talent, skill, experience and knowledge, psychological variations and motivational factors.

4.5 Human reliability analysis (HRA)

4.5.1 Overview

The analysis of human reliability is part of the overall analysis of the reliability of a technical system. Human reliability analysis involves the following activities.

- Identification of potential for human failure.
- Analysis of sources of error and causes of violations so as to be able to define appropriate counter-measures.