



DPC: 24 / 30455481 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 22 January 2024

Origin: International

Latest date for receipt of comments: 13 March 2024

Project No. 2022/00890

Responsible committee: DS/1 Dependability

Interested committees:

Title: BS EN IEC 62508 Guidance on human aspects of dependability

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 13 March 2024**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **April McMullen (BSI)**

Direct tel:

E-mail: april.mcmullen@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 62508 ED2	
DATE OF CIRCULATION: 2024-01-19	CLOSING DATE FOR VOTING: 2024-04-12
SUPERSEDES DOCUMENTS: 56/1955/CD, 56/1991B/CC	

IEC TC 56 : DEPENDABILITY	
SECRETARIAT: United Kingdom	SECRETARY: Ms Stephanie Lavy
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING Attention IEC-CENELEC parallel voting The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Guidance on human aspects of dependability

PROPOSED STABILITY DATE: 2025

NOTE FROM TC/SC OFFICERS:

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms and definitions and abbreviations	8
3.1 Terms and definitions	8
3.2 Abbreviated terms	11
4 Dependability elements of a socio-technical system	11
4.1 Overview	11
4.2 Task element	13
4.3 Human element.....	13
4.3.1 Role of Humans in a System	13
4.3.2 Dependability characteristics of humans	14
4.4 Machine element.....	15
4.5 Organization and team elements	15
4.5.1 Overview	15
4.5.2 Teamwork/operational environment	15
4.5.3 Organizational environment and structure.....	16
4.5.4 Physical environment.....	16
4.5.5 Cultural environment.....	16
4.6 Feedback within the socio-technical system.....	16
5 Human factors influence on dependability	17
5.1 Overview	17
5.2 Influence of the human element on dependability	18
5.2.1 Overview	18
5.2.2 Human strengths and limitations in an operational environment.....	18
5.2.3 Performance shaping factors (human factors)	19
5.2.4 External human factors	20
5.2.5 Internal human factors	20
5.2.6 Information Processing.....	20
5.3 Influence of the machine element on dependability	21
5.4 Influence of the task element on dependability.....	21
5.4.1 General	21
5.4.2 Allocation of tasks to humans vs. machines to optimize dependability	21
6 Human dependability program: Identifying the steps to improve human dependability.....	22
6.1 Introduction.....	22
6.2 Analysing dependability failures to define countermeasures	22
6.2.1 Overview	22
6.2.2 Human failures.....	22
6.2.3 Machine failures.....	24
6.2.4 Human- System interaction failures	24
6.3 Analysis of dependability data	24
6.4 Improving human dependability	25
6.4.1 Minimizing risk due to human-related failures	25

48	6.4.2	Human decision-making	25
49	6.5	Improving machine dependability through a human factors approach.....	26
50	6.6	Improving socio-technical system dependability	26
51	7	Human dependability at each life-cycle stage	27
52	7.1	Overview of human dependability aspects of life cycle stages	27
53	7.2	Concept/Definition stage	27
54	7.2.1	Concept stage.....	27
55	7.2.2	Human-centred design planning	28
56	7.2.3	System requirements	28
57	7.2.4	Human-centred design requirements	28
58	7.3	Design and development stage.....	29
59	7.3.2	Human-centred design guidelines.....	29
60	7.3.3	Human-centred design activities.....	30
61	7.3.5	Human dependability analysis in design and development	31
62	7.4	Realization/implementation stage	32
63	7.5	Operations and maintenance stage.....	32
64	7.6	Enhancement stage.....	33
65	7.7	Retirement/decommissioning stage	33
66	Annex A (informative)	Examples of Human Reliability Analysis (HRA) methods	34
67	Annex B (informative)	Summary of human-oriented design activities and their impact	
68		on system dependability	39
69	B.1	Overview	39
70	B.2	Automation	39
71	B.3	Design for maintainability	39
72	B.4	Human-machine interface.....	40
73	B.5	Incorporation of displays, controls, and alarm functions.....	40
74	B.6	Incorporation of input devices.....	41
75	B.7	Environment.....	41
76	B.8	Safety	41
77	B.9	Security	41
78	Annex C (informative)	Best practices for human-centred design.....	42
79	Bibliography		47
80			
81	Figure 1 – Components and interaction of a socio-technical system		12
82	Figure 2 – Performance shaping factors (PSFs) that can influence human dependability		20
83	Figure 3 – Model of typical human information processing		21
84	Figure 4 – Hierarchy of human failures		23
85	Figure 5 – System life cycle		27
86	Figure 6 – Human-centred design activities		31
87			
88	Table 1 – People who influence dependability		14
89	Table A.1 – HRA methods and their application		34
90	Table B.1 – Automation.....		39
91	Table B.2 – Design for maintainability		39
92	Table B.3 – Human-machine interface.....		40
93	Table B.4 –Incorporation of displays, controls, and alarm functions.....		40
94	Table B.5 – Incorporation of input devices		41

95	Table B.6 – Environment.....	41
96	Table B.7 – Safety	41
97	Table B.8 – Security	41
98	Table C.1 – Examples of methods and techniques that contribute to best practices	42
99		
100		
101		

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.

IEC 62508 has been prepared by subcommittee 21: Aspects of Human Dependability, of IEC technical committee 56: Dependability. It is an International Standard.

This 2nd edition cancels and replaces the 1st edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) The emphasis on user-centred design in the previous edition was reduced in favour of a greater emphasis on human dependability in an existing operational environment.
- b) The emphasis on human error and error-rate determination methods was reduced in favour of a greater emphasis on means of providing organizational support for the workforce in their execution of required tasks.
- c) Where appropriate, discussions of human factors in an operational environment were aligned with current theory, terminology and practice.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
56/XX/FDIS	56/XX/RVD

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

The language used for the development of this International Standard is English. This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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

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

INTRODUCTION

This International Standard is intended as a basic guide for managers, engineers and other professionals. It concerns good practice for improving dependability of humans in an operational environment, as well as optimising the interactions between humans and equipment, software, and organizational systems. Modern workplaces often involve the integration of humans with complex technologies and production systems. This document is intended to assist management to:

- understand the basis for human dependability, including designing equipment and systems to minimise human error, rather than over-reliance on the workforce to act correctly,
- assess the risks related to human performance in an operational environment, and
- implement changes in an operational environment in order to improve the effectiveness of personnel in relation to the technology and systems with which they interact.

One objective in implementing the guidelines in the document is to optimise the interactions between humans and equipment, software, facilities and organizational systems. A second objective is to reduce the potential for failures to occur that might adversely affect production, equipment maintenance, safety or the well-being of the workforce. Towards this end, guidance on applicable methods and metrics are included for assessing the risks associated with human dependability.

This standard is not intended as a handbook or theoretical guide to the fields of human factors or human/systems interactions. These are available elsewhere, and some useful texts are listed in the bibliography. Rather, it is intended as a tool for managers and engineers who are tasked with designing, assessing or controlling the human and technical elements of their area of responsibility.

Rather than being a review of human ‘undependability’, the aim is to describe the elements of operational systems that positively contribute to human performance. This guide provides an awareness of the relative importance of these elements to dependability, and the tools for assessing how well they are functioning in the organization, and how they might be enhanced.

In accordance with other dependability standards (cf. IEC 60300-1), the term ‘human reliability’ will refer to quantitative measures of human performance. The term ‘human dependability’ will be applied more broadly to the ability of humans to conduct a task or job as-required and when-required, with an outcome that satisfies agreed stakeholder expectations. The concepts of ‘maintainability’ and ‘supportability’ will still apply, but in the broader context of the organizational factors required for maintaining and supporting human performance.

Although knowledge of the field of human factors in the workplace and principles of human-centred design would be useful, this standard will help managers, engineers and other professionals to identify the areas of their responsibility that most need improvement in terms of human dependability, and to put in place interventions designed to optimise human performance.

This standard primarily addresses complex technical systems, but some parts are also applicable to manufacturing of mass-produced industrial and consumer products. Principles for the design of the human-machine interface (usability) are described, and further information can be found in technical literature and in relevant product standards.

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

1 Scope

This standard provides guidance on current knowledge and practice concerning dependability in an operational environment, in terms of the humans, teams and organizations involved in conducting the work. It is part of a suite of IEC standards that are intended to address the dependability of both the technical and human elements of equipment and organizations.

The document describes the human elements of a typical operational system, and the importance of those elements to overall dependability. It also describes the means of assessing how well these elements are functioning, and general concepts on how the reliability of humans might be improved. These elements typically include the individual workers, the groups or teams into which they are organised, the interfaces between humans and technical systems, and the overall organization.

The following guidance is applicable to any industry that depends on human-systems interactions involving the technology, software, or systems of work required to support the production and safety objectives of an organization. This standard primarily addresses complex technical systems, but some parts are also applicable to the manufacturing of industrial and consumer products. Principles for design of the human-machine interface (usability) are described, and further information can be found in the technical literature and in relevant product standards. Although this document does not specifically cover worker health or safety, the application of this standard can raise related issues, particularly in process safety, which is closely associated with system reliability.

2 Normative references

There are no normative references in this document.

3 Terms and definitions and abbreviations

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

For the purposes of this document, the terms and definitions given in IEC 60050-192 and the following apply.

3.1 Terms and definitions

3.1.1

dependability

ability to perform as and when required

Note 1 to entry: A dependable item or service is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder expectations.

Note 2 to entry: In most cases, the term dependability is used as an umbrella term to express its core attributes of reliability, maintainability, and supportability and the attribute of availability derived therefrom. In some cases, attributes such as resilience, recoverability, durability, integrity, safety, security, trustworthiness are also included in or overlap with dependability.

Note 3 to entry: In order to express the ability to perform, requirements in terms of functions to be performed, when the performance is to be achieved, and the life profile conditions are specified by the customers/ users/ stakeholders.

Note 4 to entry: The attributes of dependability can be expressed qualitatively or quantitatively.

Note 5 to entry: It is also a common practice to use the term dependability in the context of a subject of study or discipline.

[SOURCE: IEC 60050-192:2015, 192-01-22, modified – an item has been deleted, the notes have been deleted, and new notes to entry have been added]

3.1.2**ergonomics**

human factors

HF

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

[SOURCE: ISO6385:2016, 2.3]

3.1.3**human error resistance**

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

3.1.4**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

3.1.5**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 to entry: 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 to entry: 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 to entry: 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.

[SOURCE: ISO 9241-210:2019, 3.7, modified - Note 2 to entry added, and Notes 1 and 3 to entry renumbered]

3.1.6**human error**

discrepancy between the human action taken or omitted, and that intended or required

[SOURCE: IEC 60050-192:2015, 192-03-14, modified – Example omitted]

3.1.7**human error probability**

probability that an operator will fail in an assigned task

Note 1 to entry: 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.

Note 2 to entry: 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.

3.1.8**human failure**

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

Note to entry: 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.

3.1.9**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

3.1.10

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

3.1.11

human reliability analysis

human reliability assessment

systematic process to evaluate human reliability

Note to entry: Evaluation methods can be qualitative alone or can be expanded to provide quantitative results.

3.1.12

machine

non-human component of a system that assists humans to achieve the organization's output.

Note to entry: Machine includes hardware and software used to perform physical, computational, decisional & creative tasks.

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 task, workplace or organizational environment that influence the outcome of human activities

3.1.15

requirement

statement which translates or expresses a need and its associated constraints and conditions

Note 1 to entry: Requirements exist at different levels in the system structure.

Note 2 to entry: A requirement is an expression of one or more particular needs in a very specific, precise and unambiguous manner.

Note 3 to entry: A requirement always relates to a system, software or service, or other item of interest.

Note 4 to entry: A requirement is a statement where evidence or assurance of compliance can be provided.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19, modified – Note 4 to entry added]

3.1.16

situational awareness

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

3.1.17

socio-technical system

set of interrelated or interacting technical, human and organizational elements which produce an output generally based on inputs and tasks.

EXAMPLE A system producing IT, a factory production line, an office processing paperwork or a mine extracting minerals.

NOTE 1 to entry: 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 to entry: The structure of a system may be hierarchical.

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

3.1.18**task**

defined activity that is assigned to a person or machine in order to achieve a specific goal

Note 1 to entry: These activities can be physical, perceptual and/or cognitive.

Note 2 to entry: While goals are independent of the means used to achieve them, tasks describe particular means of achieving goals.

3.1.19**violation**

deliberate, but not necessarily malicious, deviation from practices deemed necessary

3.1.20**workplace**

permanent, temporary, physical, or virtual location where tasks are accomplished.

EXAMPLE a component of a socio-technical system.

3.2 Abbreviated terms

ASEP	Accident Sequence Evaluation Program
ATHEA	A Technique for Human Error Analysis
CAD	Computer Aided Design
CAHR	Connectionism Assessment of Human Reliability
CARA	Controller Action Reliability Assessment
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
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HF	Human Factors
HRA	Human Reliability Analysis
HR	Human Resources
IT	Information Technology
MERMOS	Méthode d'Evaluation de la Réalisation des Missions Opérateur pour la Sécurité (Method for evaluating the accomplishment of an operator's safety tasks)
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-Human Reliability Analysis
THERP	Technique for Human Error Rate Prediction

4 Dependability elements of a socio-technical system**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, promoting safe systems of work, increasing reliability and enhancing cost effectiveness. A system that requires human interaction involves human(s), machine(s) and the organizational and physical environment in which they operate. The dependability of the system and the efficiency and effectiveness with which the output or tasks of the system are achieved depend on each component of the system individually and the interactions between them (Figure 1).

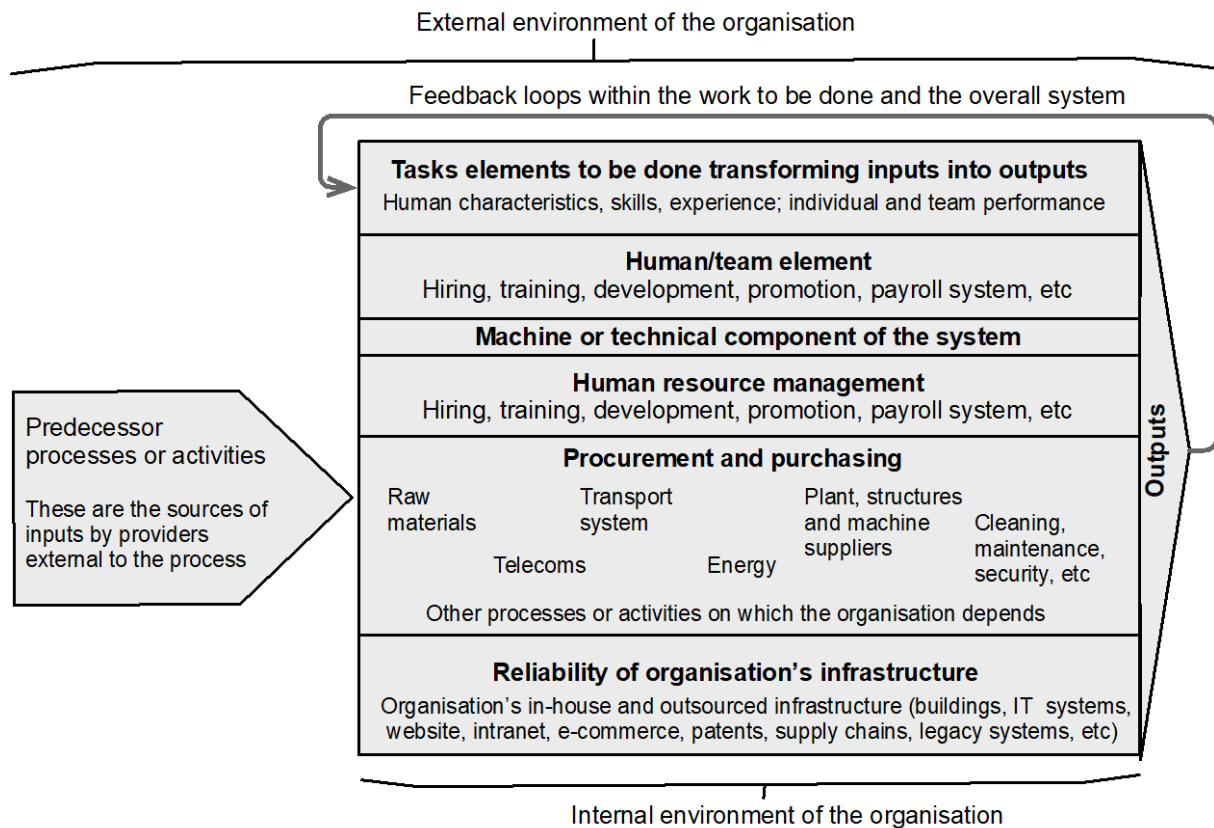


Figure 1 – Components and interaction of a socio-technical system

The elements shown in Figure 1 are as follows.

- Task element: what the work system is expected to achieve (4.2).
- Human/team element: person or people who performs the task (4.3).
- Machine: technical component of the system designed to support achievement of the work system tasks by interacting with the human element. (4.4).
- Team and organizational element: structure of the social and organizational operating environment, and systems for organising the human element (4.5).
- Physical and cultural environment: factors in the operational environment that can influence the humans and organization (4.5.3).
- Output: that which the system achieves with the required level of effectiveness, efficiency and satisfaction.
- Feedback: information exchanged between elements of the system to indicate successful or unsuccessful achievement of the output (4.6).
- In addition, all the elements of the system are influenced by performance shaping factors (PSFs) (5.2.2).

Dependability is usually characterized in terms of reliability, maintainability, supportability, and availability. In some cases, attributes such as resilience, recoverability, durability, and integrity, are also included in dependability. Dependability is critical at all life-cycle stages. Dependability also affects other attributes such as safety and environmental protection, where the inability to perform a required function could result in safety-related or environmentally damaging consequences. Dependability should therefore be actively managed throughout the system life-cycle. Section 7 describes the details of human dependability at each life-cycle stage.

NOTE The dependability objective could be different from the safety objective at each life-cycle stage because dependability is defined as "ability to perform as and when required" and safety is "freedom from unacceptable risk". Although this document does not directly refer to safety nor environmental issues, much of the guidance in this document could also be applied to them.

4.2 Task element

Achieving the goals of a work system can require the satisfactory completion of many tasks. The objective of the work system is to complete these tasks with a desired effectiveness and output quality, within an efficient timeframe, in accordance with defined processes and procedures (including a safe system of work).

Tasks within an operational environment vary depending on the work system. Tasks can be value-adding or non-value adding; both can affect dependability. Examples of different types of tasks include:

- design of the system (not covered by this standard);
- construction tasks e.g. assembling, connecting, testing and commissioning;
- operational tasks e.g. sampling, monitoring, changing configurations, adjustment of parameters, removing impediments;
- maintenance tasks e.g. inspection, fault-finding, cleaning, repair/replacement, calibration, lubrication, up-dating;
- travelling and movement within the system;
- transferring information e.g. communication, reporting, handovers and briefings;
- supervision e.g. planning, issuing directions to personnel, monitoring and correcting;
- training, instruction and assessment e.g. determining skills required, determining skills level, assigning to appropriate training courses and materials.

The allocation of tasks between humans and technology (such as machines and software) should be based on performance criteria, such as performance demands (e.g. work constraints, speed of response, frequency of action, need for judgement and decision-making) and relative capabilities of humans vs. technology (see 5.4.2 for allocation of tasks to humans vs. machines). The dependability of human tasks can be affected by factors such as difficulty or complexity, and how routine or unusual the task is, as well as support factors, such as the clarity of procedures, resources and time available, and the quality of planning and training.

Design of tasks and jobs within an operational environment should manage the risks associated with that work, pre-empt potential work-arounds, and minimise the potential for excessively high or low workload (either physical or cognitive workload).

Tasks can be described by objectives, resource allocation, and operational procedures. To improve understanding, a complex task is usually decomposed into sub-tasks in hierarchical or chronological order. Each task can have its objectives described by a list of key performance indicators that need to be maximized or minimized while managing other task requirements and constraints.

Resource allocation describes the natural, machine, and human resources needed to execute the task. Operating procedures include standard operating procedures that describe how to complete the task in normal operating conditions, as well as emergency operating procedures that describe how to recover from incidents and accidents, or minimize further damage and risk.

4.3 Human element

4.3.1 Role of Humans in a System

The role of humans in the system is to perform a task or interact with technology or other humans in order to produce a defined product or achieve a defined outcome. The human operator can either have an active role (for example when maintaining or operating a piece of equipment) or a monitoring role (such as in process control and air traffic control, or supervising the workforce).

Human influences on dependability can either be positive (e.g. changing operating parameters or resolving system faults to prevent system breakdowns), or negative (e.g. poor decision-making or not adhering to procedures). Humans can influence the function of a system through action or inaction. Even in an automated system, a human is part of the system, through design, installation, maintenance and monitoring functions.

A range of people (shown in Table 1) can 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, based on their knowledge and availability of information.

Table 1 – People who influence dependability

Job /Function/ Position	Examples of influence
Organizational management	Coordinating dependability requirements in system operations, including schedules, labour and financial resources, and information flow. Providing an environment that allows people to work dependably and effectively.
Designer Usability Engineer User Experience Designer	Takes account of human factors in normal use or operation, and reasonably foreseeable maintenance requirements. Designs for recognition and recovery from fault conditions, including instances of multiple contributors to failure (e.g. both machine and human causes). Responsible for improving the usability and user experience of a product or service
Operational manager and supervisors Maintenance manager and supervisors	Responsible for appropriate working conditions, training, support resources, systemic improvements, communication between stakeholders, and feedback to workers. Motivates operators and maintainers to achieve best outcomes. Confirms that procedures are up-to-date and are complied with. Ensures faults (localised and systemic) detected by personnel are corrected in a timely, cost-effective and systematic manner.
Operator Users	Fault-finding through regular use of an item or system. Observes and adjusts system function, and reports or corrects consequences of system faults.
Maintainer	Prevents and corrects equipment faults. Understands and complies with maintenance procedures. Reports contributors to lack of dependability in technology, procedures and operational tasks. Conducts regular testing and tests after repairs
Trainer	Improves knowledge and awareness, and avoids error-prone situations through training
Reliability/Process Safety Engineer	Analyses contributors to specific and systemic defects and identifies actions to improve dependability.
Inspectors	Investigates system function, and reports or analyses system faults. Verifies that safety barriers are still active.

Both technology and human performance, including their strengths and limitations, and the potential for humans to improve or degrade system operation, should be taken into account when considering total system dependability. The possible adverse costs and consequences of human failures, including mistakes, slips, lapses, or procedure violations (see 6.2.2) could be significant, if total system dependability is not considered. These should be considered where the human is part of a complex system in which failures have health, safety, environmental, security or mission-critical consequences.

4.3.2 Dependability characteristics of humans

Humans require physical and psychological capabilities and resources to perform tasks capably. Appropriate motivation, such as the perception that the task is useful, is also needed to expend these resources in an accurate and timely manner for successful task performance. Physical capabilities are used to receive input from hardware interfaces and to effect psychomotor functions, including interactions with interfaces. Psychological capability enables information processing of data received via sensory and perceptual input from both machine and software interfaces, as well as cognitive processing of information received in the form of raw data.