IEC 62508

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Guidance on human aspects of dependability

Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62508

Edition 1.0 2010-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Guidance on human aspects of dependability

Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 03.120.01

ISBN 978-2-88912-023-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

FOREWORD

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

1 Scope

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

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

3 Terms, definitions and abbreviations

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

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

3.1 Terms and definitions

3.1.1
dependability
ability to perform as and when required [1]

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

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

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

---

[1] Future IEC 60050-191, definition 191-41-26, second edition, under consideration.

3.1.2
ergonomics
human factors
HF
scientific discipline concerned with the understanding of interactions among human and other elements of a system that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance

[ISO 6385:2004, definition 2.3, modified]

3.1.3
error resistance
ability of a system to minimize the probability of human error occurring

3.1.4
error tolerance
ability of a system or component to continue normal operation despite the presence of erroneous inputs

[ISO/IEC 24765:2009, definition 3.1034]

3.1.5
human aspects
abilities, limitations, and other human characteristics that are relevant to the design, operation and maintenance of systems and/or their components affecting overall system performance

3.1.6
human-centred design
approach to system design and development that aims to make interactive systems more usable by focussing on the use of the system, applying human factors, ergonomics and usability knowledge and techniques

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

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

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

[ISO 9241-210:–, definition 2.7, modified] [2]

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

3.1.8
human error probability
HEP
probability that an operator will fail in an assigned task

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

---

2 To be published.

3 Future IEC 60050-191, definition 191-43-13, second edition, under consideration.

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

3.1.9
human failure
deviation from the human action required to achieve the objective, regardless of the cause of that deviation

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

3.1.10
human-oriented design
takes a user-centric approach to design by adapting technologies to meet human performance requirements, account for human limitations, achieve mental comfort and enhance overall system performance

3.1.11
human reliability
capability of human beings to complete a task under a given condition within a defined period of time and within the acceptance limits

3.1.12
human reliability analysis
HRA
systematic process to evaluate human reliability

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

3.1.13
mistake
deficiency or failure in the judgemental or inferential process involved in selection of an objective or in specification of the means to achieve it irrespective of whether or not the actions run according to plan

3.1.14
performance shaping factors
characteristics of the external environment, of the task and of humans that shape individual performance

3.1.15
requirement
need or expectation that is stated, generally implied or obligatory

[ISO 9000:2005, definition 3.1.2]

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

3.1.16
situational awareness
human perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future

3.1.17
system
set of interrelated or interacting elements

[ISO 9000:2005, definition 3.2.1]

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

– a defined purpose expressed in terms of intended functions;

– stated conditions of operation/use; and

– defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1:2003, definition 3.6]

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

NOTE 4 Humans can form part of a system.

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

3.2 Abbreviations

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

4 Human aspects

4.1 Overview

Human actions can have a strong influence on the dependability of the whole system and the quality of the output. Therefore important benefits accrue from consideration of human aspects, among which are preventing failures, improving system performance, ensuring safety, increasing reliability and enhancing cost effectiveness. A system that requires human

interaction involves human(s), machine(s) and the social and physical environment in which they operate. The dependability of the system and the efficiency and effectiveness with which the goals of the system are achieved depend on each component of the system individually and the interactions between them (Figure 1).

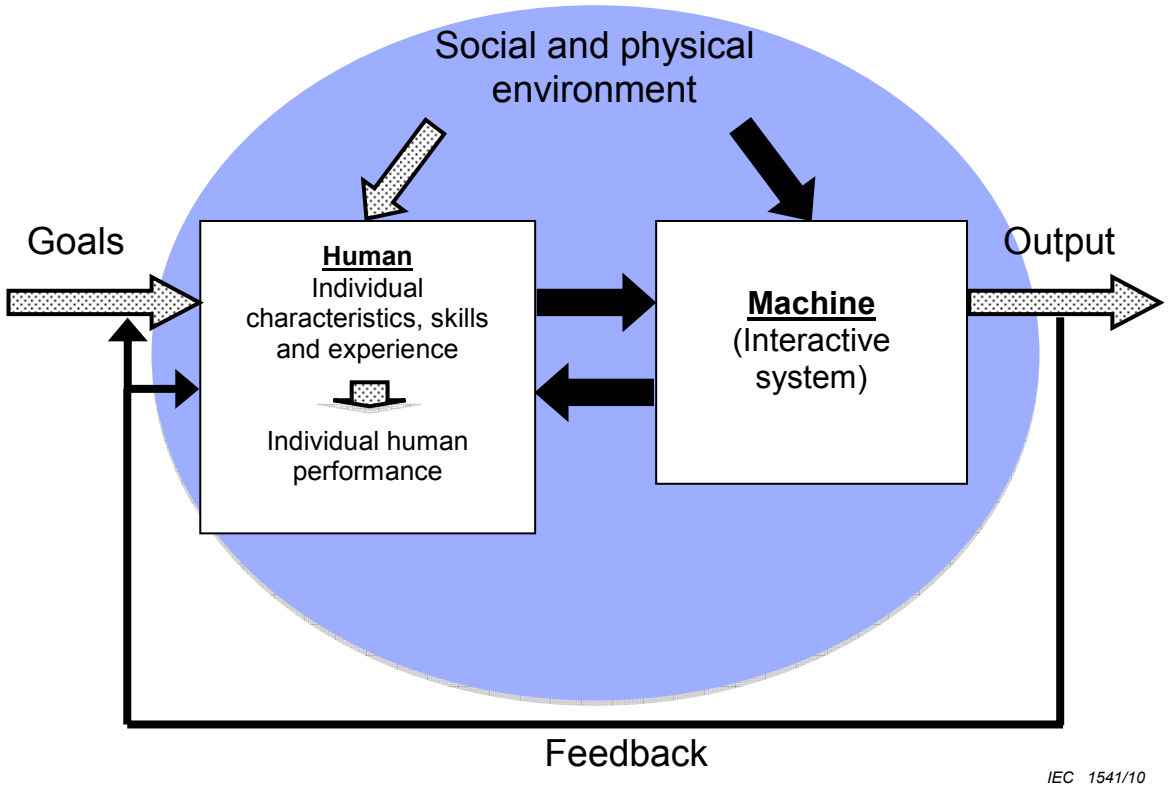

Figure 1 – Components of the system and their interactions

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.

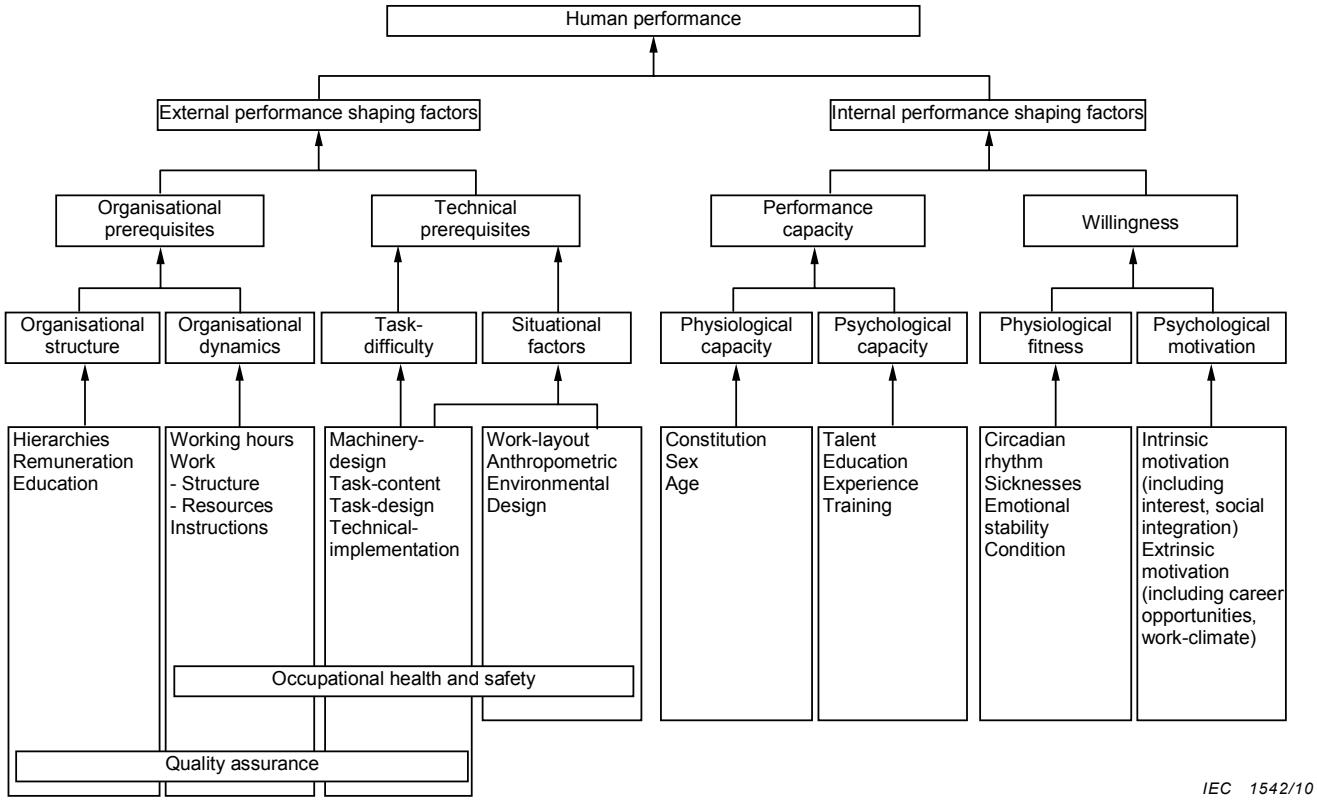

Figure 2 – Human performance shaping factors

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.

- Where appropriate, quantification of human reliability so as to be able to quantify the reliability of the system as a whole.
- Decision as to whether improvements are necessary.

4.5.2 Identifying the potential for human error

In general the role of humans in the system is to receive an input such as instructions or information via a sensory process. This input is then subjected to a cognitive process involving knowledge, memory or training to make a decision on how to respond. The resulting decision is implemented by a motor process of action involving the use of appropriate muscles. Often the action generates feedback that provides additional inputs which either confirms the correctness of the action or indicates a problem that needs correcting (Figure 3). This applies whether the task involves operating a machine, following procedures, designing equipment or procedures or undertaking a management or supervisory task.

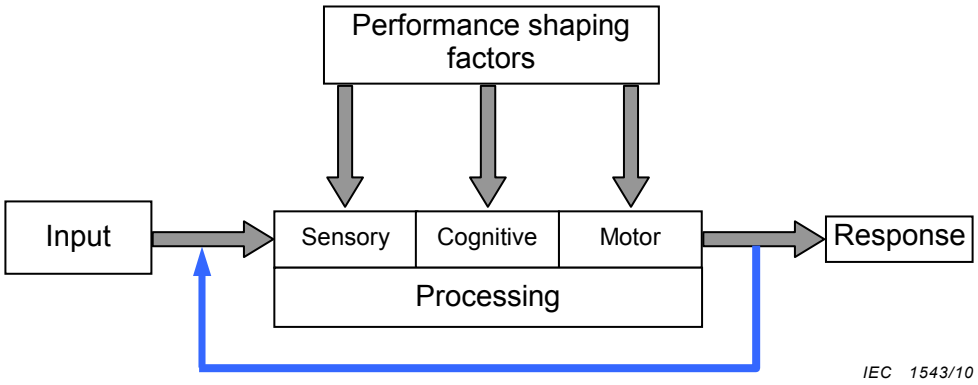

Figure 3 – Simple model of human information processing

The input in Figure 3 includes task goals, environment and feedback.

Information processing and decision making often requires use of memory and can require further external information. Errors can occur at any of the steps of this cognitive process, and the potential for error can be identified by considering each cognitive step, in turn, in order to look for where problems might occur. The potential for human error can also be identified using Failure Mode and Effect Analysis (FMEA) which starts with a task analysis and identifies likely errors at each step of the tasks and how these errors might occur (see Annex A).

4.5.3 Analysing human failures to define countermeasures

An understanding of how and why humans fail helps to define appropriate counter-measures and improve system dependability.

Human failures can be separated into violations and errors. Violations are deviations from a known correct path. They typically occur because there are unintended rewards for incorrect behaviour (for example saving time and effort or peer approval). Rules might be violated because it is perceived that there is a better way to achieve the end, to cover up mistakes or to assist colleagues. Violations may occur maliciously but this is rare.

Errors are when a planned sequence of mental or physical activities fail to achieve their intended outcome. This may be because the plan was inadequate or because the activities did not go as planned. This distinction leads to a classification of errors into mistakes, slips and lapses.

Another type of error is where the action an individual intends to carry out is correct but the performance of the action is incorrect. These errors can also be divided into two groups.

- Slips, which are failures in execution, often when performing well known and routine tasks automatically with little mental processing, for example typing or driving.
- Lapses are failures of memory or cognition (such as losing ones place in a list) or accidentally following a well known procedure instead of a required new one.

The classification is a useful starting point for analysing causes of human failure. The following approaches may be taken in design when problems are found or suspected.

To minimize violations, reasons why people might act incorrectly need to be considered and "rewards" attached to correct rather than incorrect behaviour. For example violations are less likely where the easy way of doing something is the correct way.

Mistakes are minimized by taking into account the inherent human limitations in design, then by ensuring that people have the correct knowledge and skill for the task and sufficient time to reason correctly. Clear instructions, intuitive displays and controls and aids to memory help minimize mistakes.

Slips and lapses are more difficult to minimize since the person's intention is correct and the errors often arise when performing automatic activities where the individual is not in conscious control. Designs that maintain and check situational awareness, match unconscious mental expectations and provide early feedback that an error has occurred can help ensure that slips and lapses are corrected before overall dependability is compromised.

Clause A.1 lists a number of HRA methods which include techniques for analysing mechanisms and causes of human failures which are then reviewed to define counter-measures. Human failures of all types can also be reduced by considering performance shaping factors in the design of the system and its components and designing to enhance human performance.

4.5.4 Quantification of human reliability

When the reliability of a system is to be quantified it may be appropriate to also put a value on the probability of human error. There are a number of different methods that can be applied to do this. These are listed with brief descriptions in Annex A. Usually, probabilities are applied to slips, lapses and mistakes, taking into account the performance shaping factors. Normally malicious violations are excluded from the analysis (i.e. it is assumed that people are well intentioned but can still make slips, lapses and mistakes).

4.6 Critical systems

A critical system is a computer, electronic, mechanical or electromechanical system whose failure to operate as required can have a significant impact, such as injury or human deaths, major equipment damage or large financial loss. In the design of critical systems, it is particularly important that consideration is given both to normal operation and operation under possible fault conditions where the operator may be making decisions under stress. It is important to envisage how the operator would respond to the widest possible range of abnormal situations, and to design the interface to minimize the possibility of misinterpretation.

Critical systems are normally designed to limit or exclude human intervention. However, when human intervention is needed, the human action is usually required to be correct, swift and decisive to stop or prevent further progress of adverse conditions.

There are broadly three abnormal situations where human input is critical. These situations are not exclusive and some cases may evolve from one situation to another:

a) in an emergency situation, when human decision capability is often degraded, and information can be misinterpreted;

b) in normal or abnormal situations where the operator does not realise the impact of his/her actions. In this case the operator is not stressed, in fact they may not be paying adequate attention and thus contribute to harm in some way;

c) where the operator cannot know outcomes and needs support in making and following-through decisions (maybe over very extended periods of time).

Appropriate human decisions in these situations can be achieved by the following measures:

- identify the increased potential for and consequence of single person error in highly automated systems;
- simulating emergency situations with prototype interfaces to assess human understanding, and using the feedback obtained to improve the interfaces;
- where there is any remaining potential confusion, training the operators in how to respond to the situation;
- selecting staff who are able to perform effectively in stressful multi-tasking environments;
- training the operators in regular intervals to being able to handle the system under possible fault conditions by hand;
- put in place means to address complacency/lack of awareness, such as staff selection, checking procedures, behavioural safety system, etc.;
- where it is not possible to know the risks in advance, and operators have to act with high uncertainty (e.g. finance, defence, exploration, waste disposal, etc) include procedures and tools for modelling and decision making.

4.7 Human-centred design guidelines

The following human-centred design guidelines will contribute to improved human reliability and system dependability, when applied appropriately.

a) Fitness for use

- Make the design durable, reliable and applicable for its intended use.
- Allocate functions between people and technology appropriately.
- Accommodate physical, cognitive and psychological characteristics of the users.
- Test with users.

b) Simplicity

- Design to be as simple as possible.
- Minimize the need for training.
- Make functions obvious.

c) Error tolerant and resistant

- Make the system error tolerant.
- Design such that it is not possible to make a mistake.
- Design to be fail-safe.

d) Consistency

- Make design consistent with user experience, with real life objects and with similar systems.

e) Standardization

- Use standardized hardware and software where practicable.

- Maintain identical interfaces for identical functions.
- Make controls, displays, markings, coding, labelling, and arrangement uniform.
- Make appearance distinctive.
- Standardize terminology, look, and feel.
- Make equipment with similar functionality interchangeable.

f) User-centred perspective

- Understand user roles, responsibilities, decisions and goals.
- Provide timely and informative feedback.
- Use familiar terms and images.
- Design within user abilities.
- Maximize human performance and satisfaction.
- Minimize training requirements.
- Facilitate transfer of skills.
- Accommodate physical diversity.

g) Maintainability and maintenance support

- Design for ease of disassembly and reassembly.
- Provide for specialized tools if necessary.
- Provide logistic support where needed.
- Design for common tools.
- Make design easy to maintain.

Annex B summarizes the human factors design influence and impact on system dependability in specific situations.

4.8 Human-centred design process

4.8.1 Human-centred design principles within the design process

Human-oriented design involves the process of engineering the total system design to meet the needs of the human operator and other stakeholders. The aim is to maximize the overall system capabilities and performance in operation.

Whatever the design process and allocation of responsibilities and roles adopted, the incorporation of a human-oriented approach to design should follow the human-centred design principles listed below (and described more fully in ISO 9241-210).

a) The design is based on an explicit understanding of users, tasks and environments.

b) Users are involved throughout design and development.

c) The design is driven and refined by user-centred evaluation.

d) The process is iterative.

e) The design addresses the entire user experience (including how the user will respond to the task, working environment, support, training and long-term use).

f) The design team includes multi-disciplinary skills and perspectives.

4.8.2 Human-centred design activities

Five linked human-centred design activities shall take place during a system development project (described in ISO 9241-210). They take place throughout the project and vary in detail and degree, depending on the project stage.

a) Plan the human-oriented design activities.

b) Analyse, understand and specify the context of use.

c) Analyse user needs and specify user requirements.

d) Use current human factors knowledge to design solutions to meet these requirements.

e) Evaluate the design solutions against requirements and user feedback, and modify the design and/or requirements accordingly.

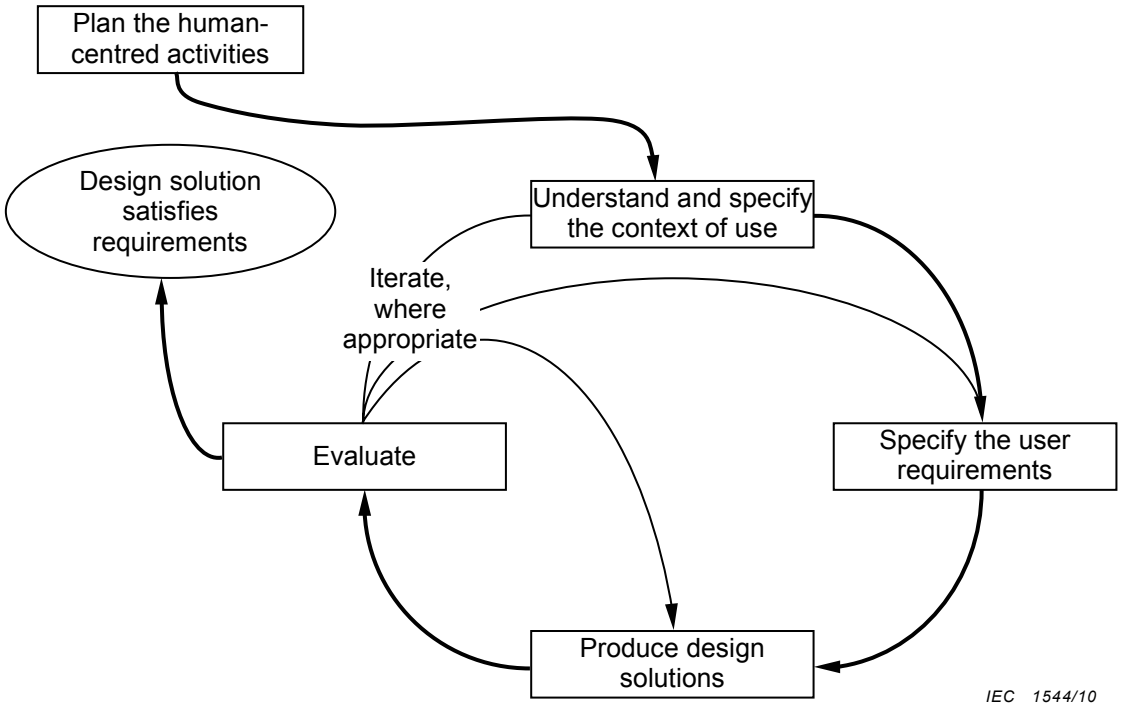

Figure 4 – Human-centred design activities

In practice, these activities can overlap or can represent distinct stages. Later activities can also modify the assumptions made in the earlier stages. Figure 4 (taken from ISO 9241-210) illustrates their interdependence.

5 Human-oriented design in the system lifecycle

5.1 Overview

The purpose of considering human aspects in systems engineering is to incorporate the interests and needs of the individuals and/or groups that will work with the system. This has the following benefits.

- Projects anticipate and address the issues and risks arising from human-system interaction.
- The system has a life cycle phase planning and resourcing designed to combat human factors risks in a cost-effective manner.

- The needs of the stakeholders in the system are communicated to the development organization.
- Overall system dependability is improved.

The human-oriented approach to design involves the application of human-centred design methods in the system lifecycle whilst being cognizant of the variability of performance and reliability of humans..

Systems should be designed to minimize the potential for human error and to reduce the impact of errors should they occur. To achieve acceptable human reliability, the design process needs to take account of all relevant human issues, such as the following.

- Eliciting and defining the full range of users, maintainer and other stakeholder requirements.
- Defining the contexts in which the system will be used and maintained, including the characteristics of the users, the tasks and the working environments.
- Defining the human performance and mental comfort requirements necessary to achieve system objectives during all phases of the life cycle.
- Identifying potential for human error by operators, maintainers and others who form part of the system during different life cycle phases.

Human-oriented design utilizes the human factor knowledge base for application in user-centric, error-resistant and error-tolerant designs by adapting appropriate technologies to mitigate challenges in meeting human performance requirements and to enhance human-system interaction.

Taking a human-oriented approach to design not only improves human reliability but also has other important benefits, such as listed below.

- Increased productivity, improved performance and greater user satisfaction.
- Reduced errors in design and operation.
- Simplified system operation and maintenance procedures.
- Reduced time in user support.
- Reduced need for special skills training.
- Reduced risks of serious accidents.
- Cost avoidance and reduce life cycle costs.

5.2 System life cycle

Human aspects should be integrated with systems engineering and the system life cycle process. The system life cycle concept adapted from IEC 60300-3-15 is shown in Figure 5 to identify the key human-oriented design influence in the system life cycle. The system life cycle stages are briefly described as follows.

– The *Concept/Definition* stage is to identify the market needs, define/identify the operational use environment/timeline, define preliminary system requirements and confirm feasible design solutions by producing technical specifications for the system design. The process activities involve the definition and analysis of requirements, architectural design, and functional design/evaluation to provide high-level system specifications. The human aspects to be considered at this stage are the variability of performance and reliability of persons who will be operating the system. HCD activities should commence with a plan which includes all the requirements.

– The *Design/Development* stage is to plan and execute selected engineering design solutions for the realization of system functions. This is transcribed into an appropriate system development effort, including engineering modelling, prototype construction, risk assessment, and interface identification of system and subsystem elements. Continued

attention to the variability of operators is necessary at this stage. Maintenance needs should also be identified at this stage in order to ensure the appropriate access is catered for in the initial design. The variability of performance and reliability of those humans who will carry out the maintenance should be considered.

– The *Realization/Implementation* stage is to execute make-buy decisions for acquisition and deployment of subsystem elements. The realization efforts deal with activities such as technology applications, manufacturing, packaging and supplies sourcing to ensure the complete transformation from system design to the specified product or subsystem elements. The realized products or elements can comprise a combination of hardware and software functions. Implementation includes such activities as integration of system functions, verification of subsystems and installation of the system. Training of operators and those who will maintain the system should be conducted at this stage.

– The *Operation/Maintenance* stage is used to deploy the system for delivery of service and to support system operational capability by means of maintenance. The process activities include operating and maintaining the system for service in accordance with system performance requirements, operators and maintainers training to maintain skills competency, customer interface to establish service relationship, and record keeping on system performance status and reporting failure incidents to initiate timely corrective and preventive actions.

– The *Enhancement* stage is to improve the system performance with added features to meet growing user demands on the system. The process activities include software upgrade, hardware addition, repair and overhaul, skills training, simplifying procedures to improve operational efficiency, obsolescence management, organizational restructuring to increase expediency and customer value. All the human aspects considered in previous phases should be revisited to realise any improvements that may be achieved out of the knowledge of operating the system.

– The *Retirement/Decommissioning* stage is to end the existence of the system entity. Upon termination of system service to the customer, the system might be disassembled, redeployed for other use, or disposed of where possible without affecting the environments. The physical and mental characteristics of those who will be operating the disposal and recycling process should be considered.

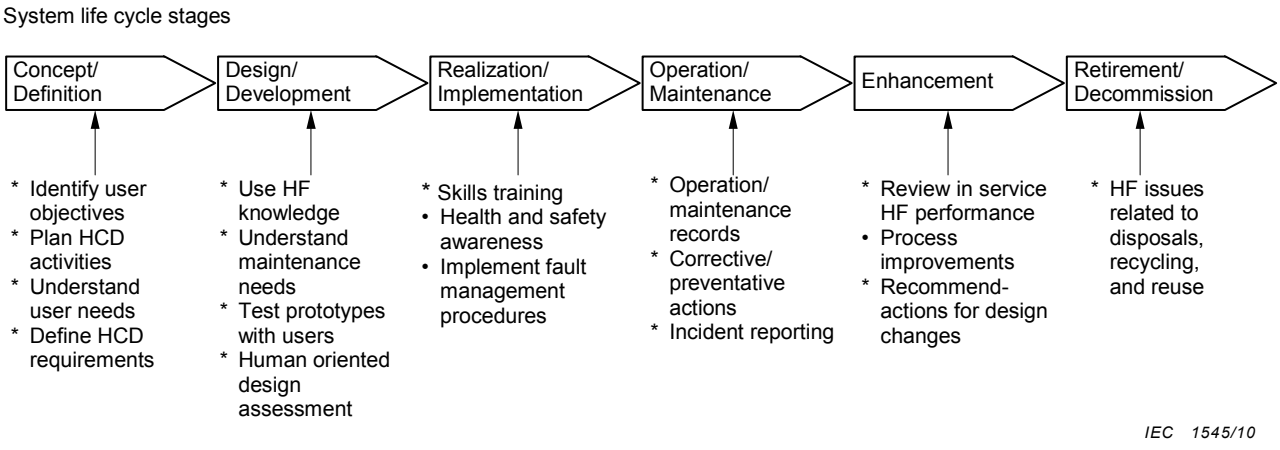

Figure 5 – Human aspects of the system life cycle

5.3 Integrating human-oriented design in systems engineering

Integrating human-oriented design in systems engineering is done throughout the system life cycle, especially during the design/development, realization/implementation and operation/ maintenance stages. It is during these stages that human-oriented design has the most influence on systems engineering tasks related to design enhancements, safety features, automation impacts, human-system performance trade-offs, ease of use and workload.

The key activities are listed below:

a) Obtain a complete and in depth understanding of the needs of the users and user organizations.

b) Identify risks to dependability arising from human involvement in the system (related to both unintended errors and potential malicious human behaviour).

c) Identify factors that will shape human performance (see 4.5).

d) Apply human factors knowledge to the design in order to achieve optimum human performance and minimize risks.

e) Iterate proposed design solutions and incorporating feedback from users into the design.

These activities are described in more detail in the following clauses. The resources allocated to the use of human-centred design activities should depend on the projected benefits of carrying out the activities at particular lifecycle stages and the associated risks if they are not carried out. Risks to be considered should include the possibility of not achieving requirements for reliability, dependability or other stakeholder needs, the operational or business implications and the associated costs of any necessary rework. The best practices are described below and listed in Annex C.

6 Human-oriented design at each life cycle stage

6.1 Overview

Annex C provides a list of the activities that are necessary to implement human-oriented design at each system life cycle stage. These are summarized in this clause.

6.2 Concept/definition stage

6.2.1 Concept

At the concept stage, it is important to obtain a clear understanding of the objectives which the user or user organization wants to achieve through use of the system, to assess the viability of these objectives and to identify any risks that might need to be incorporated into specifications and considered during design. Dependability requirements for the system should be specified, as this can affect human roles within the system.

6.2.2 Human-centred design planning

A human-centred design plan is essential to establish a strategy for managing the human-centred design effort to support system development and operation. The objective is to address human-centred design issues to improve total system performance and reduce developmental and life cycle costs. This is achieved by optimizing human performance when the system is operated and maintained in the application environment. The planning approach should include the following activities.

- Derive the goals for the human-centred activities from the overall organizational goals for the system.
- Determine the resources devoted to use of human-centred design methods. This should depend on the level of risk that would be incurred by the project at each stage if human-centred methods were not used.
- Specify how and when human-centred activities integrate into the overall system life cycle and how input from the activities is used in the system life cycle.
- Decide which methods will be included, and how they will link together in the life cycle.
- Make allowance for iteration where necessary.
- Identify the need for and cost of user involvement.
- Define outputs and criteria for success for each activity.

- Identify the necessary specialist skills and plan how to provide them.

A human-centred design plan should be developed in the early concept/definition stage of the system life cycle to maximize its effectiveness to influence system definition and framework development. The human-centred design plan should be part of the system overall plan.

6.2.3 Understanding the needs

The roles of each group of stakeholders likely to be affected by the system (including user groups and maintainers) should be identified, and the tasks that they are to perform should be analysed. The extent to which ease of use and error-free human performance are important should be established. The overall context of use in which the system is expected to be used should be identified, including the environmental factors (see 4.2.5.2) and the organizational structures, tasks and work flows (see 4.2.5.1). Field visits might be necessary to obtain this type of information.

6.2.4 System requirements

The purpose of incorporating human issues in system requirements includes the following:

- provide human-centred design inputs to develop system specifications;
- include human-centred design requirements in the quality assurance process;
- include human-centred design requirements for outsourcing and subcontracting;
- establish human-oriented procedures for system operation and maintenance.

The objective is to achieve a human-centred, error resistant and tolerant system framework that is suitable and usable for effective system operation.

- User requirements should be established in conjunction with potential users.
- The intended behaviour and performance of the system with respect to the users should be established.

6.2.5 Human-centred design requirements

The human-centred requirements analysis provides the necessary information and relevant data for the following activities:

- determination of human-centred design issues in system application and operating scenario;
- integration of human-centred design principles into the system context;
- tailoring the human-centred design project to meet system requirements.

Human-centred design requirements should include the following:

- operator and maintainer roles and responsibilities;
- human-system interfaces influencing user performance efficiency and effectiveness;
- specification of the context in which the system will be used, including the environmental factors (see 4.2.5.2) and the organisational structures, tasks and work flows (see 4.2.5.1);
- system performance metrics including operator/maintainer performance;
- mental comfort and user satisfaction requirements;
- system architecture design affecting human-system interactions;
- system application environment impacting human resources and requirements.

The human-centred design requirements should be presented to relevant stakeholders to obtain feedback. Scenarios of use can be used to present the requirements. They have the

benefits of being relatively easy to test and being easy for other project stakeholders to understand.

The human-centred design requirements analysis should be conducted in conjunction with the human-centred design plan during concept/definition stage of the system life cycle. This facilitates the tailoring process working to meet specific project needs in the system definition. The project tailoring process is described in IEC 60300-2.

6.3 Design/development

Human-centred design analysis in system design is conducted during the design/development stage of the system life cycle. The objective is to ensure that

- human-system capabilities and limitations are properly reflected in the system requirements,
- human-system performance characteristics provide relevant information to identify design options and alternatives,
- human reliability and other human related system dependability risks are identified, assessed and appropriately addressed in design.

System specifications and the operation and maintenance procedures should take into account of the following elements:

- human performance such as human capabilities and limitations (see 4.3.3), workload, function allocation, hardware and software design, decision aids, environmental constraints, and team versus individual performance;
- training needs such as duration of training, training effectiveness, skills retraining, training devices and facilities, and embedded training;
- staffing requirements such as staffing levels, team composition, and organizational structure;
- personnel selection such as minimum skill levels, special skills, competency and experience;
- health and safety risks that can arise at all subsequent stages of the life cycle. Issues include hazardous materials and conditions, system and equipment design for safe operation, biomedical influences, protective equipment, and warning and alarm requirements.

The design of the system should take into account that humans need to detect, diagnose and correct faults during operation including complexities where there may be multiple failures.

The system should be reviewed in accordance with applicable knowledge of human sciences, style guides, standards, guidelines, regulations and legislation, and prototypes should be evaluated by users to refine the usability of the developing system. The system should be tested as part of verification and validation to ensure that it meets the requirements of the users, the tasks and the environment, as defined in its specification. This can be achieved using a prototype in a simulated working environment to test how humans interact with the proposed design. For more complex systems and/or components, where human interactions are particularly important, the system should be tested during initial operations.

6.4 Realization/implementation

In this stage the product is manufactured, the system components are assembled, and the product is put in place for application and operation.

The human-centred design includes the following activities.

- Review of human-machine interactions in the light of experience.

- More detailed assessment of risks including human reliability risks of operation and maintenance stage.
- Training in the skills needed to use the system.
- Creation of health and safety awareness.
- Implementation of fault management procedures.
- Review of regulatory compliance.
- Testing of the final system to ensure that it meets human-oriented requirements.

6.5 Operation/maintenance

Errors during operation and maintenance are reduced by good design but not eliminated. It is important that errors are reported so they can be reviewed and improvements made. This requires a culture where error is able to be reported freely without fear of punishment, and understanding of underlying causes of error and the conditions which tend to provoke error.
Regular simulation and/or training should be provided in responding to emergency situations and the lessons learnt should be used to enhance the system performance and the human awareness and skills.

Human-centred design assessment in the operation/maintenance stage is intended to check that human-centred design considerations have been adequately integrated into the system for effective performance operation. The assessment is achieved by system testing and performance verification with the aim of producing evidence of conformance to human-centred design requirements in an application environment. The human-centred design assessment process should include the following activities.

- Measurement of human performance and mental comfort in critical tasks.
- Determination of efficiency and effectiveness of human intervention.
- Maintenance of human-centred design test records and assessment data as basis for evaluation and improvement.
- Assessment of ease of maintenance.
- Performance of emergency situation simulations/training in defined intervals and provision of the lessons learnt for enhancement of the system performance and the human awareness/skills.

The human-centred design assessment results should be analysed to support recommendations for design changes, where appropriate, provide rationale for human performance improvements or implement training solutions.

The human-centred design information flow should include sharing with integrated logistics support (ILS) programs where applicable. ILS is a disciplined approach to integrate support considerations into design, to acquire the necessary initial support for the system and to identify life cycle support requirements. The human-centred design program provides the human resource and performance dimension for logistics support requirements and functions. Close coordination between the human-centred design and ILS programs will reduce data redundancies and result in more effective use and sharing of information.

6.6 Enhancement

This stage is to improve system performance with added features to meet growing user demands on the system.

The human-centred design process should include the following activities.

- Collection and analysis of in-service reports to generate updates or lessons learnt for the next version of the system.
- Improvement of the human-centred design process in the context of the wider systems engineering process.

- Communication with stakeholders on proposed improvements.

The result might be to apply a miniature version of the life cycle in order to implement the enhancement.

6.7 Retirement/decommission

This stage is designed to end the existence of the system entity.

The human-centred design process should include the following activities:

- Examine human factors issues related to disposals, recycling, and reuse
- Identify risks and health and safety issues associated with removal from service and destruction of the system.
- Define how users will be re-allocated, dismissed or transferred to other duties.
- Plan the break-up of social structures.
- Debrief and retrospective analysis for the replacement system.

6.8 Outsourcing projects and related human-centred design issues

The human-centred design requirements should be incorporated in system specifications and procurement documents. This is crucial for the system to achieve its objectives for coherent design and consistent performance involving proper function allocation and interactions of hardware, software and human elements in system design and operation.

The outsourcing of subsystems development requiring human operation is common in today's complex system development and enhancement projects. Incorporation of commercial-off-the-shelf (COTS) products as system functions often has cost benefits. System support services are frequently used for contract maintenance.

The success factors are dependent on the collaborative efforts of the acquirers and suppliers, the system integrators and service providers through application of supply-chain management and quality assurance processes. Since human-oriented design involves multi-disciplinary actions, it is sometimes necessary for technical experts to deal with resolution of critical human issues related to outsourcing and procurement needs.

Outsourcing human-centred design projects should consider the following issues.

- Conformance to the human-centred design process in ISO 9241-210 and making available work products such as those described in ISO/IEC TR 25060 (context of use description, user needs report, user requirements specification, user interaction specification, user interface specification, evaluation reports).
- Human-system interface requirements to achieve the level of human performance during system operation and maintenance.
- Maximizing the economical demands on utilization of available human resources, skills and training.
- Staffing implications of the human resources, job classification, skill levels and experience needed for the projects.
- Evaluation for design automation trade-off with human operation in terms of applicability, efficiency and cost implications.
- Potential system safety and health hazard areas involving human-system interactions.
- Quality assurance provisions for procurement contracts.
- Reintegration of all outsourced tasks and projects into the total system model for system optimization.

Human performance testing of COTS products should take advantage of available information from the product manufacturers, records of warranty returns, previous commercial testing and product use experience.

Outsourcing projects should be identified during concept/definition stage of the system life cycle. The procurement contracts should be well established at the completion of the design/development stage. This permits time for subcontractor evaluation, multiple sourcing of preferred suppliers and COTS product assessment for incorporation as system functions to facilitate the system integration process.

7 Human-centred design methods

7.1 Classification of human-centred design activities

Human-centred design activities are classified in ISO/PAS 18152 as follows:

- HS.1 Life cycle involvement activities: in each stage of the system life cycle.
- HS.2 Integrate human factors activities: in business strategy, quality management, authorisation and control, management of HS issues, HF data in trade-off and risk mitigation, user involvement, human-system integration and development and re-use of HF data.
- HS.3 Human-centred design activities*:* context of use, user requirements, produce design solutions, evaluation of use.
- HS.4 Human resources activities*:* human resources strategy, definition of standard competencies and identification of gaps, design of staffing solution and delivery plan, evaluation of human resources system solutions and obtaining feedback.

The methods that can be used to support these activities include the following.

a) Human-centred design analysis methods

Human-centred design analysis methods are used to define system concepts, describe application/mission scenarios, determine functional requirements and assign tasks for appropriate skills allocation. The various analyses provide a means for identifying human-centred design related goals, objectives, critical design issues, and further evaluation needs to meet system performance requirements involving human interactions.

b) Human-centred design methods for design and development

Human-centred design methods for design and development are used to incorporate all necessary human-centred design criteria into the human-system interface design. The human-system interface includes system hardware, software, procedures, work environments and facilities associated with the system functions requiring human interactions. The process is designed to convert the results of the human-centred design analysis activities into design criteria for human factors project development and implementation.

c) Human-centred design methods for test and evaluation

Human-centred design methods for test and evaluation are used to verify human-system interface and procedures to ensure that the system can be operated, maintained, supported and controlled in its intended operating environment by the users. These methods facilitate identification of critical human-centred design issues in operation and maintenance for problem resolution and process improvement.

Annex C provides a summary of practical methods for human-centred design analysis, design and development, as well as test and evaluation.

7.2 Applications of human-centred design methods

The human-centred design methods for general analysis, evaluation and assessment applications are based on systems engineering techniques. They should be used in conjunction with other engineering methods and technical disciplines in system design and implementation. The human factors engineering methods listed in Annex C contribute to the best practices for human-centred design, as shown in Table C.1.

Annex A
(informative)

Examples of HRA methods

There is a distinction between the HRA methods of the first generation and the HRA methods of the second generation.

First generation methods treat human failure in the same way as hardware failure with the output from human tasks substituted for equipment outputs. Human actions are considered in a binary fashion, i.e. as success or failure to achieve the required result from a task. Tasks and subtasks are considered to have an inherent failure probability which is then modified by performance shaping factors which are based on the evaluation of the ergonomic environment. Methods differ in the way in which they estimate the basic human error probabilities (HEP) and incorporate performance shaping factors (PSFs).

HRA procedures of the second generation model and evaluate the role of the context and human decision-making behaviour which can have adverse effects on the system.

Table A.1 provides a description of the various methods and details on how they are applied.

Table A.1 – HRA methods and their application

Method and short description	Level of use
ASEP – Accident Sequence Evaluation Program: simplified version of THERP for pre-assessments (with conservative estimates during pre-assessments). Critical tasks are broken down into subtasks which are arranged on a human performance event tree. HEPs for subtasks are obtained from tables published in NUREG/CR-4772 (US regulatory Commission 1987). Guidance is also given for allowing for PSFs in the HEP. Standardized action decomposition: critical actions and diagnosis of disturbances if applicable. Overall recommendations for commitment on one HEP per critical action; detailed judgment on human-machine interfaces not required. Time-related HEP-diagnosis, given curves are based on an expert consensus. Allows for fast pre-selection of important tasks.	ASEP is used if a quick but not very precise quantitative estimation is needed for screening. This is the case in low power and shutdown states of nuclear power plants for instance where the number of action to assess is large and a time-efficient method is needed. ASEP is a first generation HRA method, allowing for assessment of ergonomic problems in the working environment.

Method and short description	Level of use
ATHEANA – A Technique For Human Error Analysis: thorough analysis of the context and of decision-making provides the system analyst with detailed knowledge about the potential for erroneous human decisions. The method identifies human failure events (HFEs) by considering accident scenarios. HFEs are characterized by unsafe acts i.e. actions (or omissions) which result in degraded plant performance and by the error forcing context (EFC). The EFC includes both PSFs and plant conditions that make human error likely. HFE is quantified by combining probabilities of EFCs, the probability of an unsafe act in the EFC and the probability of an EFC given the unsafe act and additional evidence following the unsafe act. The quantitative estimates are based on expert judgment similar to the SLIM approach.	ATHEANA is used in a number of studies in particular in the nuclear environment. ATHEANA is a second generation HRA method, allowing for thorough qualitative analysis of the influence of the context on human behaviour and decision making. Can be used for analysis of post incident error where error forcing context of the incident occurs.
CAHR – Connectionism Assessment Of Human Reliability: the method requires operational events or other behavioural data to perform its assessment. It consists of: (1) a structured framework for data collection, (2) a method for qualitative analysis of the collected data, and (3) a method for human reliability assessment. For the assessment the method distinguishes the task and the context under which the task needs to be performed, the cognitive demand that the task and the context place on the human, the human compensation mechanisms and the resulting behaviour.	CAHR can be used for either assessing classical ergonomic problems or interrelations of multiple conditions and factors. Applications range from nuclear, automobile, aviation, and air traffic to maritime management. CAHR is a second generation HRA method, allowing thorough qualitative analysis of the influence of the context on human behaviour and decision making in a time efficient manner.

Method and short description	Level of use
CREAM – Cognitive Reliability And Error Analysis Method: The human control mode applicable to the scenario is selected from 4 “contextual control modes” (human reliability is assumed to increase as level of control increases). The context of the task or scenario is described using CREAM’s 9 common performance conditions (CPCs). (CPCs are similar to PSFs.) Potential errors are identified and classified into a number of groups that describe error modes and error causes. For the assessment CREAM uses similar tables to THERP but only after having performed the analysis of the essential contextual control modes.	CREAM is widely used for quick assessments of the context on human performance and provides insights on the level of a screening technique. CREAM is a second generation HRA method, allowing a qualitative analysis of the influence of the context on human behaviour and decision-making and a coarse quantification.
ESAT – Expertensystem zur Aufgaben-Taxonomie (expert system for task taxonomy): PSF-related quantification of discretionary tasks. Determination of a reliability rating (RR, on a scale of 1 to 10) by assessments (“ratings”) of given PSFs. The functional connection between HEP and RR is partly determined by expert assessments (based on generic knowledge on human work performance) and partly by measuring work performances. This method has been applied for the design of cockpits in aviation.	ESAT stems from aviation but is still occasionally used also in other industrial settings like assessing human errors in production. ESAT is a first generation HRA method, allowing for assessment of ergonomic problems in the working environment.
FMEA/FMECA – Failure Modes And Effects Analysis identifies failure modes (i.e. what is done incorrectly) and failure mechanisms (how it is done wrongly or psychological error mechanisms) and its effects. As with equipment, FMEA probabilities error modes occurring can be estimated and the criticality of errors can be estimated by considering their probability of occurrence and the magnitude of the effects.	FMEA and FMECA are commonly used for equipment reliability and extended into human reliability as either a qualitative or quantitative tool. For more detailed guidance see IEC 60812.

Method and short description	Level of use
HCR/ORE (Human Cognitive Reliability / Operator Reliability Experiments): HCR methods recognise that the success or failure of an operator depends on the time available for action. HEP is the fraction of time required for diagnosis and response time available. HCR/ORE was developed on the basis of operator reliability experiments (ORE). For tasks described in procedures, time-related and time-unrelated failures of diagnosis are distinguished. There are 6 HEP-time-curves available (according to the type of reactor and dynamic of failure) normalized on the average time requirement (Median). PSF-related HEP quantification for the time-unrelated failure is performed by considering 8 given error mechanisms. Guidelines for a decision-tree-type PSF-modelling are also given. For tasks that are not represented in procedures, a quick method for assessment of the HEP is offered	The approach was developed because the original HCR (human cognitive reliability model) approach, distinguishing between skill- rule- and knowledge-based behaviour, was proven to not be a valid approach towards human reliability. HCR/ORE requires simulation experiments to be conducted before it can provide valid assessments. Due to the efforts combined with this requirement current use is limited to some nuclear control room actions. HCR/ORE is a first generation HRA method, allowing for assessment of task performance dependent from the time available; ergonomic problems are addressed in a limited way.
HEART/CARA – Human Error Assessment And Reduction Technique: Intended for generic, system-based tasks (e.g. put system X into operation) rather than for elementary tasks (e.g. manipulate switch X). A nominal value for HEP is selected by comparing the task with a list of 8 generically defined tasks for which HEPs are defined. HEP is then modified by a rating for PSFs selected from a list of 38 PSFs. The method received further development into generic task types in air traffic management under the name CARA.	Easily and quickly manageable. Many of the PSF-figures are based on empirical studies; disadvantage: model calibration is insufficient. The technique is hence not suitable for estimating the reliability of Human actions if a high precision in the assessment or a high reliability is required (e.g. actions leading immediately to adverse effects in the system). HEART and its successors are first generation HRA methods, allowing for assessment of task performance in the sense of a more detailed screening rather than a thorough assessment.

Method and short description	Level of use
MERMOS – Méthode d'Evaluation de la Réalisation des Missions Opérateur pour la Sûreté (Method for the evaluation of the realization of an operator's mission regarding safety). MERMOS avoids the term "human error" and distinguishes missions (set of tasks to be performed); mechanisms are established by humans on how to coordinate the mission and probable outcomes of such coordination. Multiple failure paths that lead to mission failure are identified using a process structured by considering strategy, action and diagnosis. Probabilities are assigned to path elements by expert judgment. Data stem from operational experience as well as simulator observations.	MERMOS is used extensively in the French nuclear industry. It was validated several times and received regulatory acceptance. MERMOS is a second generation HRA method, allowing thorough qualitative analysis of the influence of the context on human behaviour and decision making.
SHERPA – Systematic Human Error Reduction And Prediction Approach. Starts with task analysis and classifies bottom level sub-tasks by type (action, retrieval, checking, selecting and communicating). Determine credible error modes for subtask using SHERPA check list for error modes. Consequences are described and the possibility of recovery at a later task noted. Probability and criticality of each error for each subtask are given an ordinal rating (high, medium, low).	First generation method that provides a structured comprehensive means of identifying errors in performing specific tasks and qualitatively rating their importance. Used to seek error reduction strategies. Does not incorporate system or organizational errors.

Method and short description	Level of use
SLIM – Success Likelihood Index Methodology: Experts identify relevant PSFs (e.g. complexity of task) and nominate endpoints on a scale from 1 to 9 (e.g. 1 = simple and 9 = complex). The point on each scale at which ideal performance is expected is noted and used to rescale ratings according to the distance from an ideal value. Each task is rated for each PSF on these scales. A success likelihood index (SLI) is calculated on the basis of an overall sum of weighted PSF ratings and is transformed to a probability scale by applying at least 2 reference-HEPs. Prerequisite: proven reference-HEPs and relevant PSFs are available; PSFs are clearly assessable. The determination of reference-HEPs is problematic and predetermines the results that can be achieved.	SLIM is used if a flexible method is required and no specific data is available. Also PSF-interdependencies are not taken into account. Therefore the results of the method can only provide a screening. SLIM is a first generation HRA method, allowing for assessment of task performance in the sense of a more detailed screening rather than a thorough assessment.
SPAR-H – Standardized Plant Analysis Risk (SPAR) HRA: consists of a two-step process to identify nominal human error probabilities (HEPs), and then modify those HEPs on the basis of summary-level performance-shaping factors (PSFs) and dependence. Significantly, this method required analysts to complete a relatively straightforward worksheet, which was then used to estimate the PSFs and the HEP of interest. SPAR-H has inherent limitations of modelling and analysis that should be clearly understood.	The SPAR-H is a screening method and should not necessarily be preferred over more sophisticated and detailed approaches, such as a technique for human event analysis (ATHEANA) in situations that require detailed analysis of the human performance aspects of an event. SPAR-H allows addressing in a limited way first and second generation HRA issues on the level of screening.
THERP – Technique for Human Error Rate Prediction: this is the standard method for human reliability in respect to ergonomic issues. Produces in-depth task decomposition into elements using THERP taxonomy, errors for elements represented in event tree format. Nominal HEP is assigned to each task element by selecting 'appropriate' HEPs from a data base of around 100 factors. Nominal HEP is modified by multiplier for PSFs if applicable. Dependence between errors for the task elements is modelled. Curves are produced for the probability that a human will respond to a disturbance in a given time are based on an expert consensus.	THERP is used when a thorough assessment of the tasks is required and the overall system dependability relies on critical actions. Decision-making and the influence of a wide spectrum of contextual factors cannot be assessed. THERP is a first generation HRA method, allowing thorough assessment of task performance and providing detailed ergonomic requirements for system design. It is not suitable for assessing decision making or to consider the range of contextual conditions sufficiently.

Annex B
(informative)

Summary of human-oriented design activities and their impact on system dependability

B.1 Overview

This annex gives some examples of human-centred design activities that when used appropriately, will improve system dependability.

B.2 Automation

Table B.1 – Automation

Human-centred design activity	Impact on system dependability
• Provide automation information and operating status and other feedback to system user. • Make features easy to use. • Ensure safe operations within the user's capacity and capability. • Alert user of automation failure or degradation, and potential unsafe modes of operation. • Provide error resistant and error tolerant features that are not unnecessarily difficult to use to prevent unauthorized or accidental access. • Provide means for manual override (with safe-guards)	• Enhancing availability of system functions. • Improved system performance due to automated functions. • Enabling users to carry out the required tasks to avoid increased cognitive demands, extreme workload situations, interruption or distraction imposed on the user. • Simplifying user training needs and requirements for system applications. • Minimizing errors and risk arising from error.

B.3 Design for maintainability

Table B.2 – Design for maintainability

Human-centred design activity	Impact on system dependability
• Build in redundancy where practicable and cost-effective to reduce unscheduled maintenance. • Design for modularity, lowest replaceable unit and throwaway assembly. • Incorporate built-in-test capabilities, remote and self-diagnostic features. • Incorporate quick and easy access to all assembly units requiring maintenance for inspection, removal and replacement. • Minimize the numbers and types of tools and test equipment needed for maintenance. • Incorporate self-healing and self-adjustment features where applicable and practical.	• Improved maintainability. • Improved reliability. • Simplification of maintenance functions. • Enhancing testability, diagnostics, and fault identification. • Reduced maintenance time and logistic support resource requirements.

B.4 Computer-human interface

These activities are based on ISO 9241-110. For more detailed guidance on user interface design, see ISO 9241, Parts 2, 12, 13, 14, 15, 16, 17, 20, 151 and 171.

Table B.3 – Computer-human interface

Human-centred design activity	Impact on system dependability
• Make the interactive system suitable for the task so that it supports the user in the completion of the task. • Make the interactive dialogues self-descriptive so that it is obvious to the users which dialogue they are in, where they are within the dialogue, which actions can be taken and how they can be performed. • Make the interactive dialogues conform with user expectations so that it corresponds to predictable contextual needs of the user and to commonly accepted conventions. • Make the interactive dialogues suitable for learning so that they support and guide the user in learning to use the system. • Make the interactive dialogues controllable so that the user is able to initiate and control the direction and pace of the interaction. • Make the interactive dialogues error-tolerant so that despite evident errors in input, the intended result can be achieved with either no, or minimal, corrective action by the user. • Make the interactive dialogues capable of individualization so that users can modify interaction and presentation of information to suit their individual capabilities and needs.	• Improved system usability and serviceability. • Increased system speed. • Reduced number of errors.

B.5 Incorporation of displays, controls and alarm functions

For more detailed guidance on displays and controls, see ISO 9241, Parts 300, 302, 303, 304, 305, 306, 307, 308, 309, and 920.

Table B.4 – Incorporation of displays, controls and alarm functions

Human-centred design activity	Impact on system dependability
• Make displays and controls legible, identifiable, and distinguishable under all conditions. • Locate controls in a consistent manner in grouping and arrangement for easy access to the user. • Design the control movement and direction in a consistent manner. • Design the controls with sequential operations to follow a fixed pattern. • Design the controls for maintenance and adjustment to be protected to avoid accidental activation. • Design the coding for controls to differentiate among the controls with uniform application of the code throughout the system. • Simplify coding entry and identify error for re-entering codes. • Design alarm functions to be visible and auditable. • Design alarm functions to provide unambiguous and clear indication of the cause for the alert, inform the user of the priority and nature of the problem, and possible responses. • Incorporate alarm input validation to prevent false alarms. • Provide voice communication systems where essential and applicable in alarm and emergency situations.	• Improved maintainability. • Improved testability. • Improved system operation and maintenance tasks. • Reduced number of false alarms. • Improved safety and security in system performance. • Simplifying user training needs and skills requirements.

B.6 Incorporation of input devices

For more detailed guidance on design of input devices, see ISO 9241, Parts 4, 9, 400, 410 and 920.

Table B.5 – Incorporation of input devices

Human factors design activity	Impact on system dependability
• Design of keyboard entry and fixed-function keys. • Design of pointing devices (mouse, joystick and trackball, light pen). • Design of non-pointing devices (touch interactive devices and touch panels, voice activated controls). • Design inter-changeability among input devices	• Improved accessibility. • Improved operability. • Improved usability.

B.7 Environment

For more detailed guidance on workplace environment, see ISO 9241-6.

Table B.6 – Environment

Human-centred design activity	Impact on system dependability
• Modular designs for lowest replaceable units. • User control of workplace environment (ventilation, illumination, temperature, humidity, noise).	• Improved maintainability. • Improved human performance and satisfaction in workplace.

B.8 Safety

Table B.7 – Safety

Human-centred design activity	Impact on system dependability
• Workplace safety for accessibility and operation. • Equipment-related safety for user operation. • Hazard avoidance designs. • Human reliability analysis.	• Improved human performance in a safe environment. • Risk mitigation for degraded system performance. • Statistics on human performance.

B.9 Security

Table B.8 – Security

Human-centred design activity	Impact on system dependability
• System security and authorized access. • Security safeguards and protective measures and controls. • Physical security. • Information security.	• Improved system performance integrity. • Risk reduction.

Annex C
(informative)

Best practices for human-centred design

This annex lists the most important activities in ISO/PAS 18152 that are relevant at each lifecycle stage (together with their reference numbers), and gives examples of methods and techniques that can be used to implement them.

Table C.1 – Examples of methods and techniques that contribute to best practices

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
1.1 Concept	Identify expected context of use of systems (forthcoming needs, trends and expectations) (1.1-1) Analyse the system concept to clarify objectives, their viability and risks (1.1-2)	– Future workshop – Preliminary field visit – Focus groups – Photographic surveys – Simulations of future working environments – In-depth analysis of work and lifestyles
	Describe the objectives which the user or user organization wants to achieve through use of the system (1.1-3)	– Participatory workshops – Field observations and ethnography – Consult stakeholders – Human factors analysis
	Define the scope of the context of use for the system (3.1-1)	– Context of use analysis
1.2 Planning a) General	Develop a plan to achieve and maintain usability throughout the life of the system (2.4-1) Identify the specialist skills required and plan how to provide them (2.4-2)	– Plan to achieve and maintain usability – Plan use of HSI data to mitigate risks
b) User involvement	Identify the HS issues and aspects of the system that require user input (2.6-1) Define a strategy and plan for user involvement (2.6-3) Select and use the most effective method to elicit user input (2.6-4) Customize tools and methods as necessary for particular projects/stages (2.7-4)	– Identify HSI issues and aspects of the system requiring user input – Develop a plan for user involvement – Select and use the most effective methods – Customize tools and methods as necessary

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
c) Risks	Assess the health and well-being risks to the users of the system (1.2-6) Assess the risks to the community and environment arising from human error in the use of the system (1.2-7) Evaluate the current severity of emerging threats to system usability and other HS risks and the effectiveness of mitigation measures (2.5-3) Assess the risks of not involving end users in each evaluation (2.6-2) Plan and manage use of human factors data to mitigate risks related to HS issues (2.5-1) Evaluate the current severity of emerging threats to system usability and other HS risks and the effectiveness of mitigation measures (2.5-3) Take effective mitigation to address risks to system usability (2.5-4)	– Risk analysis (process and product) – HSI program risk analysis
1.3 Understanding needs a) Context of use	Identify and analyse the roles of each group of stakeholders likely to be affected by the system (1.1-4) Describe the characteristics of the users (3.1-3) Describe the cultural environment/ organizational/ management regime (3.1-4) Describe the characteristics of any equipment external to the system and the working environment (3.1-5) Describe the location, workplace equipment and ambient conditions (3.1-6) Decide which goals, behaviours and tasks of the organization influence human resources (4.1-1) Present context and human resources options and constraints to the project stakeholders (1.1-6)	– Successful identification of critical stakeholders – Field observations and ethnography – Participatory workshop – Work context analysis – Context of use analysis – Event data analysis – Contextual enquiry – Visibility diagram – Reach envelope
b) Tasks	Analyse the tasks and work system (3.1-2)	– Task analysis – Cognitive task analysis – Work context analysis – Application/mission analysis – Functional flow diagram – Operational sequence diagram – Flow process chart – Decision/action diagram – Action/information requirements – Timeline – Integrated computer-aided manufacturing definition – Workload analysis – Situation awareness analysis – Link analysis – Human performance reliability analysis
c) Usability needs	Perform research into required system usability (1.1-5)	– Investigate required system usability – Usability benchmarking – Heuristic/expert evaluation – Predetermined time standards

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
d) Design options	Generate design options for each aspect of the system related to its use and its effect on stakeholders (1.2-1) Produce user-centered solutions for each design option (1.2-2)	– Early prototyping and usability evaluation – Develop simulations – Parallel design (tiger testing)
1.4 Requirements a) Context requirements	Analyse the implications of the context of use (3.1-7)	– Define the intended context of use, including boundaries
b) Infrastructure requirements	Identify, specify and produce the infrastructure for the system (1.3-2) Build required competencies into training and awareness programs (1.3-4) Define the global numbers, skills and supporting equipment needed to achieve those tasks (4.1-2)	– Identify staffing requirements and any training or support needed to ensure that users achieve acceptable performance
c) User requirements	Develop an explicit statement of the user requirements for the system (3.2-2) Generate and agree on measurable criteria for the system in its intended context of use (3.2-4)	– Scenarios – Personas – Storyboards – Establish performance and satisfaction goals for specific scenarios of use – Define detailed user interface requirements – Prioritize requirements
1.5 Analysis requirements	Assess the extent to which usability criteria and other HS requirements are likely to be met by the proposed design (2.5-2) Analyse the user requirements (3.2-3) Present these requirements to project stakeholders for use in the development and operation of the system (3.2-5) Identify any staffing gap and communicate requirements to design of staffing solutions (4.2-6)	– Identify and analyse the success of critical stakeholder requirements) – Common industry specification for usability requirements – Environment/organization assessment
2. Design/ development a) General	Generate design options for each aspect of the system related to its use and its effect on stakeholders (1.2-1) Produce user-centred solutions for each design option (1.2-2) Design to enable customization to support specific market and user needs (1.2-3) Distribute functions between the human, machine and organizational elements of the system best able to fulfil each function (3.3-1) Develop a model of the user's work from the requirements, context of use, allocation of function and design constraints for the system (3.3-2) Produce designs for the user-related elements of the system that take into account the user requirements, context of use and human factors data (3.3-3) Produce a description of how the system will be used to support integration of system components (3.3-4)	– Function allocation – Generate design options – Physical ergonomics – Participatory design – User interface guidelines and standards

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
b) Prototyping and evaluation	Develop simulation or trial implementation of key aspects of the system for the purposes of testing with users (1.2-4)	– Prototyping and usability evaluation – Develop prototypes –Develop simulations – Drawing – Mock-up – Scale model – Manikin – CAD environment – Technical, manual and functional evaluation – Use human factors engineering data for evaluation
c) Human resources	Decide which goals and tasks of the organization influence human resources (4.1-1) Define the global numbers, skills and supporting equipment needed to achieve those tasks (4.1-2) Identify current tasking/duty (4.2-1) Analyse gap between existing and future provision (4.2-3) Identify skill requirements for each role (4.2-3) Predict staff wastage between present and future (4.2-4) Calculate the available staffing, by taking into account the working hours, attainable effort and non-availability factor (4.2-5) Identify and allocate the functions to be performed (4.3-1) Specify and produce job designs and competence/ skills required to be delivered (4.3-2) Calculate the required number of personnel (4.3-3) Generate costed options for delivery of training and/or redeployment (4.3-4) Evolve options and constraints into an optimal training implementation plan (4.3.5) Develop and submit to trial a training solution to representative users (4.3-6) Define how users will be re-allocated, dismissed or transferred to other duties (1.5-3)	– Work domain analysis – Task analysis – Participatory design – Workload assessment – Human performance model – Design for alertness – Plan staffing

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
3. Realization/ Implementation	Maintain contact with users and the client organization throughout the definition, development and introduction of a system (1.3-3) Evolve options and constraints into an implementation strategy covering technical, integration and planning and manning issues (1.3-1) Revise design and safety features using feedback from evaluations (3.3-5) Deliver final training solutions to designated staff according to agreed timetable (4.3-7) Collect user input on the usability of the developing system (1.2-5) Test that the system meets the requirements of the users, the tasks and the environment, as defined in its specification (1.3-5) Review the system for adherence to applicable human science knowledge, style guides, standards, guidelines, regulations and legislation (1.4-3)	– Risk analysis (process and product) – User feedback on usability and user experience – Use models and simulation – Guidelines: common industry format for usability reports – Performance measurement – Design criteria checklist
4. Operations	Produce personnel strategy (1.4-1) Review the system for adherence to applicable human science knowledge, style guides, standards, guidelines, regulations and legislation (1.4-3) Deliver training and other forms of awareness-raising to users and support staff (1.4-2) Review health and well-being risks to the users of the system (1.4-5) Review the risks to the community and environment arising from human error in the use of the system (1.4-6) Perform research to refine and consolidate operation and support strategy for the system (1.4-8)	– Work context analysis – Organizational and environmental context analysis
5. Enhancement	Provide means for user feedback (on human issues) (4.4-2) Analyse feedback on the system during delivery and inform the organization of emerging issues (1.3-6) Assess the effect of change on the usability of the system (1.4-4) Take action on issues arising from in-service assessment (1.4-7) Take effective mitigation to address risks to system usability (2.5-4)	– Organizational and environmental context analysis – Risk analysis – User feedback on usability and user experience – Work context analysis – Continuous direct observation – Sampled direct observation – Interviews and questionnaires
6. Retirement	Collect and analyse in-service reports to generate updates or lessons learnt for the next version of the system (1.5-1) Identify risks and health and safety issues associated with removal from service and destruction of the system (1.5-2) Define how users will be re-allocated, dismissed, or transferred to other duties (1.5-3) Plan break-up of social structures (1.5-4) Debriefing and retrospective analysis for replacement system (1.5-5)	
7. Outsourcing	Take into account the stakeholder and user issues in acquisition activities (2.3-1)	– Common industry format

Life cycle stage	Best practices from ISO/PAS 18152 (ISO/PAS 18152 reference number given in brackets)	Example methods and techniques
8. Integration a) Business strategy b) Quality management c) Authorization and control	Contribute to the business case for the system (1.1-7) Define usability as a competitive asset (2.1-1) Set usability, health and safety objectives for systems (2.1-2) Develop user-centred infrastructure (2.1-4) Relate HS issues to business benefits (2.1-5) Define and maintain HCD and HR infrastructure and resources (2.2-3) Increase and maintain awareness of usability (2.2-4) Develop or provide staff with suitable HS skills (2.2-5) Implement the HR strategy that gives the organization a mechanism for implementing and recording lessons learnt (4.1-4) Enable and encourage people and teams to work together to deliver the organization's objectives (4.1-6) Create HR capabilities to meet future system requirements (conduct succession planning) (4.2-7)	– Program risk analysis – Develop and maintain HSI infrastructure and resources – Identify required HSI skills – Provide staff with HSI skills – Establish and communicate a policy on HSI – Maintain an awareness of usability
d) Staffing	Decide how many people are needed to fulfil the strategy and what ranges of competence they need (4.1-3)	

Bibliography

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

HF-STD-001:2002, *Human Factors Design Standard (HFDS), Federal Aviation Administration*

HFDG, 1996, *FAA Human Factors Design Guide – For Acquisition of Commercial-Off-The-Shelf Subsystems, Non-developmental Items, and Development Systems, DOT/FAA/CT-96/1. Federal Aviation Administration*

MIL-HDBK-46855A:1999, *Human Engineering Program Process and Procedures. Department of Defense*

MIL-HDBK-1472F:1998, *Human Engineering Design Criteria. Department of Defense*

MIL-HDBK-1908B:1999, *Definitions of Human Factors Terms. Department of Defense*

WALLACE, D.F.; WINTERS, J.; DUGGER, M.; and LACKIE, J.:2001, "*Human Systems Engineering: Understanding the Process of Engineering the Human into the System"; Naval Surface Warfare Center Dahlgren Division Technical Report NSWCDD/TR-01/101; November, 2001.*

NASA, *Man-Systems Integration Standards, NASA-STD-3000, Volume I and II (1995)*

FAA, *Guidelines for Human Factors Requirements Development, AAR-100 (2004)*

ISO/PAS 18152:2003, *Ergonomics of human-system interaction — Specification for the process assessment of human-system issues*

ISO 6385:2004, *Ergonomic principles in the design of work systems*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 9241-1:1997, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 1: General introduction*

ISO 9241-2:1992, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 2: Guidance on task requirements*

ISO 9241-3:1992, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 3: Visual display requirements W 2008-11-14*

ISO 9241-4:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 4: Keyboard requirements*

ISO 9241-5:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 5: Workstation layout and postural requirements*

ISO 9241-6:1999, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 6: Guidance on the work environment*

ISO 9241-7:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 7: Requirements for display with reflections W 2008-11-14*

ISO 9241-8:1997, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 8: Requirements for displayed colours W 2008-11-14*

ISO 9241-9:2000, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 9: Requirements for non-keyboard input devices*

ISO 9241-11:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability*

ISO 9241-12:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 12: Presentation of information*

ISO 9241-13:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 13: User guidance*

ISO 9241-14:1997, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 14: Menu dialogues*

ISO 9241-15:1997, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 15: Command dialogues*

ISO 9241-16:1999, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 16: Direct manipulation dialogues*

ISO 9241-17:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 17: Form filling dialogues*

ISO 9241-20:2008, *Ergonomics of human-system interaction – Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services*

ISO 9241-110:2006, *Ergonomics of human-system interaction – Part 110: Dialogue principles*

ISO 9241-151:2008, *Ergonomics of human-system interaction – Part 151: Guidance on World Wide Web user interfaces*

ISO 9241-171:2008, *Ergonomics of human-system interaction – Part 171: Guidance on software accessibility*

ISO 9241-210:–, *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*[4]

ISO 9241-300:2008, *Ergonomics of human-system interaction – Part 300: Introduction to electronic visual display requirements*

ISO 9241-302:2008, *Ergonomics of human-system interaction – Part 302: Terminology for electronic visual displays*

ISO 9241-303:2008, *Ergonomics of human-system interaction – Part 303: Requirements for electronic visual displays*

ISO 9241-304:2008, *Ergonomics of human-system interaction – Part 304: User performance test methods for electronic visual displays*

---

4 To be published.

ISO 9241-305:2008, *Ergonomics of human-system interaction – Part 305: Optical laboratory test methods for electronic visual displays*

ISO 9241-306:2008, *Ergonomics of human-system interaction – Part 306: Field assessment methods for electronic visual displays*

ISO 9241-307:2008, *Ergonomics of human-system interaction – Part 307: Analysis and compliance test methods for electronic visual displays*

ISO 9241-308:2008, *Ergonomics of human-system interaction – Part 308: Surface-conduction electron-emitter displays (SED)*

ISO 9241-309:2008, *Ergonomics of human-system interaction – Part 309: Organic light-emitting diode (OLED) displays*

ISO 9241-400:2007, *Ergonomics of human-system interaction – Part 400: Principles and requirements for physical input devices*

ISO 9241-410:2008, *Ergonomics of human system interaction – Part 410: Design criteria for physical input devices*

ISO 9241-920:2009, *Ergonomics of human-system interaction – Part 920: Guidance on tactile and haptic interactions*

ISO 11064-1, *Ergonomic design of control centres – Part 1: Principles for the design of control centres*

ISO 11064-2, *Ergonomic design of control centres – Part 2: Principles for the arrangement of control suites*

ISO 11064-3, *Ergonomic design of control centres – Part 3: Control room layout*

ISO 11064-4, *Ergonomic design of control centres – Part 4: Layout and dimensions of workstations*

ISO 11064-5, *Ergonomic design of control centres – Part 5: Displays and controls*

ISO 11064-6, *Ergonomic design of control centres – Part 6: Environmental requirements for control centres*

ISO 11064-7, *Ergonomic design of control centres – Part 7: Principles for the evaluation of control centres*

ISO/PAS 18152:2003, *Ergonomics of human-system interaction – Specification for the process assessment of human-system issues*

ISO/TR 18529:2000, *Ergonomics – Ergonomics of human-system interaction – Human-centred lifecycle process descriptions*

ISO/IEC 24765:–, *Systems and software engineering – Vocabulary*[5]

5 To be published.

ISO/IEC DIS TR 25060:–, *Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability – General framework for usability-related information*[6]

Human reliability analysis (HRA)

NOTE Titles preceded by method, in acronym form.

ASEP: SWAIN, A.D. (1987) *Accident Sequence Evaluation Program on Human Reliability Analysis Procedure. NUREG/CR-4772. NRC. Washington DC*

ATHEANA: NUREG-1624:2000, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). NRC. Washington DC. Rev. 1*

CAHR: STRÄTER, O.:2005, *Cognition and safety – An Integrated Approach to Systems Design and Performance Assessment. Ashgate. Aldershot. (ISBN 0754643255)*

CREAM: HOLLNAGEL, E.:1998, *Cognitive Reliability and Error Analysis Method – CREAM. Elsevier. New York, Amsterdam. (ISBN 0-08-042848-7)*

ESAT: BRAUSER, K.:1992, *ESAT – Ein neues Verfahren zur Abschätzung der menschlichen Zuverlässigkeit. In: Gärtner, K. (Hrsg.) Menschliche Zuverlässigkeit. DGLR-Bericht 92-04. DGLR. Bonn*

HCR/ORE: MOIENI, P., SPURGIN, A.J. & SINGH, A.:1994, *Advances in Human Reliability Analysis Methodology. Part I: Frameworks, Models and Data. Reliability Engineering and System Safety. Vol.44. Elsevier. p. 27*

KIRWAN, B.:1994, *A Guide To Practical Human Reliability Assessment. CRC*

MERMOS: LE BOT, P., DESMARES, E. & BIEDER, C.:1998, *MERMOS: an EDF project to update Human Reliability Assessment methodologies. In: Lydersen, S., Hansen, G. Sandtorv, H. (1998) Safety and Reliability. ESREL'98, Trondheim/Norway. A. A. Balkema. Rotterdam. p. 767 ff*

SLIM: EMBREY, D., HUMPHREYS, P. ROSA, E.A., KIRWAN, B. & REA, K.:1984, *SLIM-MAUD- An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement. NUREG/CR-3518. NRC. Washington DC*

SPAR-H: BYERS, I.C., GERTMAN, D.I., HILL, S.G., BLACKMAN, H.S., GENTILLON, C.D., HALLBERT, B.P., & HANEY, L.N.:2000, *SPAR HRA Methodology: Comparison with other HRA methods. International Ergonomics – IEA 2000. San Diego. Human Factors and Ergonomics Society. Santa Monica CA. Published by: Mira Digital Publishing. South Jefferson, St. Lois, MO (www.miracd.com)*

THERP: SWAIN, A.D. & GUTTMANN, H. E.:1983, *Handbook of Human Reliability Analysis with emphasis on nuclear power plant applications. Sandia National Laboratories, NUREG/CR-1278. Washington DC*

WILLIAMS, J.C.:1988, *HEART – A data-based method for assessing and reducing human error to improve operational performance. In: Proceedings of the IEEE Conference on Human Factors and Power Plants. Monterey, CA. June 1988. P. 436-450*

———————

6 To be published.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

LIGNES DIRECTRICES RELATIVES AUX FACTEURS HUMAINS DANS LA SÛRETÉ DE FONCTIONNEMENT

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62508 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

La présente édition annule et remplace le CEI/PAS 62508 publié en 2007.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1365/FDIS	56/1373/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente Norme internationale fournit des lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement des systèmes. Elle répond au besoin d'une norme traitant de la sûreté de fonctionnement des systèmes homme-machine.

Elle fournit les lignes directrices relatives à la prise en compte des facteurs humains dans la sûreté de fonctionnement dans toutes les phases du cycle de vie d'un système, y compris les principes ergonomiques de conception et la compréhension des facteurs humains pour les applications de système.

La présente norme présente les différents principes et certains exemples des types de méthodes qu'il est possible d'utiliser.

Il est prévu d'élaborer une norme décrivant de manière plus détaillée les méthodes, notamment la quantification du facteur humain et qui constituera une suite à la publication de la présente norme.

La présente norme apporte des recommandations, mais ne comporte aucune exigence. L'attention est attirée sur l'éventuelle existence d'exigences réglementaires concernant les systèmes entrant dans le domaine d'application de la présente norme.

LIGNES DIRECTRICES RELATIVES AUX FACTEURS HUMAINS DANS LA SÛRETÉ DE FONCTIONNEMENT

1 Domaine d'application

La présente Norme internationale fournit des lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement, ainsi que des méthodes et pratiques de conception centrées sur l'intervention de l'homme et qui peuvent être utilisées tout au long du cycle de vie du système afin d'améliorer les performances de sûreté de fonctionnement. La présente norme décrit des approches qualitatives. Des exemples de méthodes quantitatives sont donnés dans l'Annexe A.

La présente norme internationale s'applique à tous les domaines de l'industrie dans lesquels l'homme et la machine sont en relation. Elle est destinée aux techniciens et à leurs hiérarchies.

La présente norme internationale n'est pas destinée à une utilisation dans le cadre d'une certification, d'une réglementation ou d'un contrat.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60300-1:2003, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

Disponible en anglais seulement.

CEI 60300-2, *Gestion de la sûreté de fonctionnement – Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement*

CEI 60300-3-15, *Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations suivants s'appliquent.

NOTE Certains termes et définitions sont tirés de l'avant-projet de la deuxième édition de la CEI 60050-191, *Vocabulaire Électrotechnique International – Partie 191: Sûreté de fonctionnement*, actuellement à l'étude.

3.1 Termes et définitions

3.1.1
sûreté de fonctionnement
aptitude à fonctionner conformément aux exigences[1]

---

1 Future CEI 60050-191, définition 191-41-26, deuxième édition, à l'étude.

NOTE 1 Les caractéristiques de la sûreté de fonctionnement incluent la disponibilité et ses facteurs influents intrinsèques ou externes, tels que la fiabilité, la tolérance aux pannes, l'aptitude à être remis à niveau, l'intégrité, la sûreté, la maintenabilité, la durabilité et la logistique de maintenance.

NOTE 2 La sûreté de fonctionnement est également utilisée de manière descriptive comme terme général exprimant les caractéristiques de qualité, dans le temps, d'un produit ou d'un service. Elle peut également exprimer un niveau, un degré, une confiance ou une probabilité de satisfaire à un ensemble défini de caractéristiques.

NOTE 3 D'une manière générale, les spécifications des caractéristiques de sûreté de fonctionnement incluent: la fonction du produit, la durée de son aptitude à la fonction et les conditions de stockage, d'utilisation et de maintenance. Il est également possible d'intégrer des exigences en matière de sécurité, d'efficacité et d'économie tout au long du cycle de vie.

3.1.2
ergonomie
facteurs humains
FH
discipline scientifique qui vise la compréhension fondamentale des interactions entre les êtres humains et les autres composantes d'un système, et la mise en œuvre dans la conception de théories, de principes, de données et de méthodes afin d'améliorer le bien-être des êtres humains et l'efficience globale des systèmes

[ISO 6385:2004, définition 2.3, modifiée]

3.1.3
robustesse aux erreurs
aptitude d'un système à limiter la probabilité d'erreurs humaines

3.1.4
tolérance aux pannes
aptitude d'un système ou d'un composant à fonctionner correctement malgré la présence de données erronées

[ISO/CEI 24765:2009, définition 3.1034]

3.1.5
aspects humains
aptitudes, limites et autres caractéristiques humaines liées à la conception, au fonctionnement et à la maintenance de systèmes et/ou de leurs composants, qui affectent l'efficience globale du système

3.1.6
conception centrée sur l'humain
approche de conception et de développement de systèmes ayant pour objectif de rendre les systèmes interactifs mieux utilisables en mettant l'accent sur l'utilisation du système, en prenant en compte les facteurs humains, la connaissance et les techniques de l'ergonomie et de l'aptitude à être utilisable

NOTE 1 Les systèmes utilisables présentent un certain nombre d'avantages, dont une productivité accrue, l'amélioration du bien-être de l'utilisateur, la prévention du stress, une meilleure accessibilité et un risque de préjudice réduit.

NOTE 2 La présente norme utilise l'expression «conception orientée vers l'humain» pour rappeler la nécessité de tenir compte des personnes dans la conception du système. Cependant, elle retient l'expression «conception centrée sur l'humain» utilisée dans les normes ISO pour faire référence aux méthodes et activités spécifiques.

NOTE 3 L'expression «conception centrée sur l'humain» est employée de préférence à l'expression «conception centrée sur l'utilisateur» afin de souligner que la présente norme couvre également les effets sur un grand nombre de parties prenantes, et non simplement les individus considérés généralement comme utilisateurs. Toutefois, dans la pratique, ces termes sont souvent utilisés comme synonymes.

[ISO 9241-210:–, définition 2.7, modifiée][2]

3.1.7
erreur humaine
écart entre l'action humaine réalisée (ou l'inaction) et l'action prévue[3]

3.1.8
probabilité d'erreur humaine
PEH
probabilité de défaillance d'un opérateur à réaliser une tâche qui lui a été attribuée

NOTE 1 Cette probabilité peut reposer sur le rapport entre le nombre moyen d'erreurs survenues dans la réalisation d'une tâche donnée et le nombre total de possibilités d'erreur pour ce type de tâche.

NOTE 2 Les probabilités d'erreur humaine sont exprimées dans une distribution qu'il convient de déterminer en fonction des variations humaines et circonstancielles dans lesquelles la tâche doit être réalisée.

3.1.9
défaillance humaine
écart par rapport à l'action humaine requise pour atteindre l'objectif, quelle que soit la cause de cet écart

NOTE Pour tout système particulier ou toute situation singulière, l'étendue des défaillances humaines constitue la combinaison des erreurs humaines et des violations qui entraînent des défaillances du système et/ou des résultats dangereux.

3.1.10
conception orientée vers l'humain
approche de conception centrée sur l'utilisateur en adaptant les technologies permettant de satisfaire aux exigences de performance humaine, de tenir compte des limites humaines, d'atteindre un certain confort mental et d'améliorer la performance globale du système

3.1.11
fiabilité humaine
aptitude des êtres humains à réaliser une tâche dans des conditions données, dans un délai défini et dans les limites d'acceptation

3.1.12
analyse de fiabilité humaine
AFH
processus systématique d'évaluation de la fiabilité humaine

NOTE Les méthodes d'évaluation peuvent être simplement qualitatives, mais elles peuvent être étendues pour donner des résultats quantitatifs.

3.1.13
faute
faiblesse ou défaillance constatée dans le processus appréciatif ou inférentiel de choix d'un objectif ou de précision des moyens permettant d'atteindre cet objectif, indépendamment du fait que les actions entreprises respectent ou non le plan établi

---

2 A publier.

3 Future CEI 60050-191, définition 191-43-133, deuxième édition, à l'étude.

3.1.14
facteurs de performance
caractéristiques de l'environnement extérieur, de la tâche et des personnes ayant une influence sur les performances individuelles

3.1.15
exigence
besoin ou attente formulés, habituellement implicites ou imposés

[ISO 9000:2005, définition 3.1.2]

NOTE Dans le contexte de la présente norme, il s'agit d'un besoin ou d'une attente qu'il convient qu'un système, un composant du système, un produit ou un service satisfasse ou détienne.

3.1.16
conscience circonstancielle
perception humaine temporelle et spatiale des éléments environnementaux, compréhension de leur signification et projection de leur état dans un avenir proche

3.1.17
système
ensemble d'éléments corrélés ou interactifs

[ISO 9000:2005, 3.2.1]

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un système dispose:

– d'un objet défini exprimé en termes de fonctions prévues;
– de conditions spécifiées de fonctionnement/utilisation; et
– de limites définies.

NOTE 2 La structure d'un système peut être hiérarchique.

[CEI 60300-1:2003, 3.6]

NOTE 3 Pour certains systèmes (les produits de technologie de l'information, par exemple), les données constituent une part importante des éléments du système.

NOTE 4 Les êtres humains peuvent faire partie intégrante d'un système.

3.1.18
violation

écart intentionnel, mais non obligatoirement répréhensible, des pratiques jugées nécessaires

3.2 Abréviations

AFH	Analyse de Fiabilité Humaine
AMDE (FMEA)	Analyse des Mécanismes de Défaillance et de leurs Effets
AMDEC (FMECA)	Analyse des Mécanismes de Défaillance, de leurs Effets et de leur Criticité
CAO	Conception assistée par ordinateur
COTS	Produits du Commerce (*de l'anglais Commercial Off The Shelf*)
CPC	Condition de performance commune
CFE	Contexte de forçage d'erreur
CCH	Conception centrée sur l'humain
EF	Evaluation de Fiabilité
FH	Facteurs Humains
FP	Facteur de Performance
HS	Homme-Système
IHS	Interaction Homme-Système
IPR	Indice de Probabilité de Réussite
IU	Interface Utilisateur

MIPR (SLIM)	Méthode basée sur l'Indice de Probalitité de Réussite
PEH	Probabilité d'Erreur Humaine
RH	Ressources Humaines
SLI	Soutien Logistique Intégré

4 Facteurs humains

4.1 Présentation

Les actions humaines peuvent avoir une influence importante sur la sûreté de fonctionnement de l'ensemble du système et sur la qualité des éléments de sortie. Par conséquent, la prise en compte des aspects humains génère des avantages considérables tels que la prévention des défaillances, l'amélioration de la performance d'un système, l'assurance de la sécurité, le renforcement de la fiabilité et l'amélioration de la rentabilité. Un système nécessitant une interaction humaine implique la présence d'êtres humains, de machines et d'un environnement social et physique dans lequel ils évoluent. La sûreté de fonctionnement du système, ainsi que l'efficacité et l'efficience avec lesquelles les objectifs du système sont atteints, dépendent de chaque composant individuel du système et de leurs interactions (Figure 1).

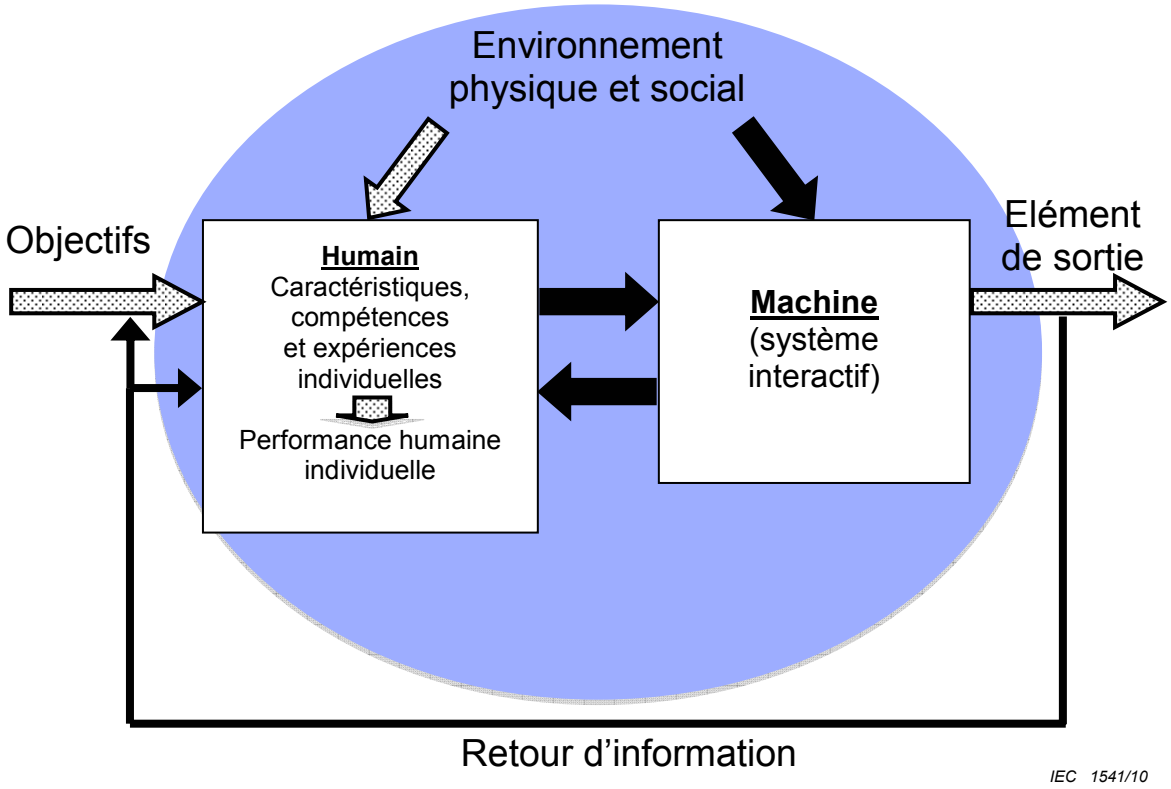

Figure 1 – Composants du système et leurs interactions

Les flèches grises matérialisent les facteurs de performance (FP) (décrits en 4.4).

Les composants illustrés à la Figure 1 se présentent comme suit:

- Objectifs: ce à quoi doit aboutir le système en action (4.2.2).
- Être humain: celui qui réalise la tâche (4.2.3).
- Machine: système interactif conçu pour faciliter la réalisation des objectifs du système en action (4.2.4).

- Environnement: facteurs sociaux et physiques qui peuvent influencer le ou les êtres humains et la machine (4.2.5).
- Élément de sortie: ce qu'il convient d'obtenir avec le niveau requis d'efficacité et d'efficience (4.2.6).
- Retour d'information: qui provient de la machine (4.2.7).

4.2 Composants du système et leurs interactions

4.2.1 Remarques introductives

Le présent paragraphe décrit chacun des composants de la Figure 1.

4.2.2 Objectifs

Le système en action a pour but d'atteindre les objectifs selon une efficacité et une efficience souhaitées.

4.2.3 Êtres humains

Le rôle des êtres humains dans le système consiste à réaliser une tâche ou à interagir avec une machine en vue d'atteindre un objectif défini. L'opérateur humain peut avoir un rôle de surveillance (dans la maîtrise des processus ou dans une salle de contrôle du trafic routier, par exemple) ou un rôle actif (pour résoudre un incident sur une voie de circulation, par exemple).

L'influence humaine peut être négative (des erreurs humaines et des violations, par exemple) ou positive (prévention des défaillances du système ou des problèmes liés au système, par exemple). Les êtres humains peuvent avoir une influence sur le système par leur action ou inaction. Un être humain fait partie intégrante du système (même automatisé) au travers de ses fonctions de conception, de maintenance et de surveillance.

De nombreuses personnes (comme l'indique le Tableau 1) peuvent intervenir dans les différentes phases du cycle de vie d'un système, chacune d'entre elles ayant une influence sur la sûreté de fonctionnement du système par ses actions et décisions.

Tableau 1 – Personnes ayant une influence sur la sûreté de fonctionnement

Poste	Exemples d'influence
Chef de projet	Sensibilisation aux besoins de sûreté de fonctionnement dans les concepts du système
Concepteur	• Prise en compte des facteurs humains en utilisation normale et dans le cas d'une mauvaise utilisation raisonnablement prévisible • Conception en vue de la reconnaissance et du rétablissement du système suite à des conditions de défaillance y compris lorsqu'il existe plusieurs modes de défaillance
Rédacteur de procédures d'exploitation	Établissement des procédures permettant de limiter les défaillances humaines
Chef d'exploitation et superviseur	• Garantie des conditions de travail, des ressources, de la communication, du retour d'information et de la formation appropriés • Motivation des opérateurs, • Garantie de la conformité aux procédures
Opérateur	Observation et consignation dans un rapport des conséquences d'une erreur humaine
Formateur	Mise en évidence, lors de la formation, des situations sujettes aux erreurs
Personnel de maintenance	Compréhension, interprétation et conformité aux procédures

Il convient de tenir compte des performances humaines, y compris les forces et limites, ainsi que le potentiel des êtres humains à améliorer ou à détériorer l'exploitation d'un système lors de la prise en considération de la sûreté de fonctionnement de l'ensemble du système. Même si cela semble alourdir la charge de travail et les implications financières, le coût de la défaillance peut s'avérer plus lourd, si la sûreté de fonctionnement de l'ensemble du système n'est pas prise en compte. Les possibles conséquences néfastes des défaillances humaines (comprenant les erreurs, étourderies, défaillances, violations ou actes de malveillance) sont particulièrement importantes lorsque l'être humain fait partie intégrante d'un système complexe ayant des applications critiques, sécuritaires ou vitales. L'erreur humaine peut également avoir de graves conséquences dans les environnements financiers et du commerce électronique.

Pour plus de détails sur les caractéristiques humaines, voir 4.3.

4.2.4 Machine (système interactif)

La machine est conçue pour atteindre des objectifs fonctionnels et de performance au sein des environnements dans lesquels elle doit fonctionner.

Au cours de l'exploitation, la machine reçoit de l'être humain, par le biais de ses commandes, des éléments d'entrée et fournit un élément de sortie qui traduit la réalisation de la tâche par le système. L'élément de sortie est souvent extrait afin de fournir un retour d'information à l'être humain sur le fonctionnement de la machine.

Pour que l'ensemble du système fonctionne de manière efficiente et efficace, l'interface et l'interaction entre la machine et les personnes qui l'utilisent à tous les stades du cycle de vie

(de la conception à la mise au rebut) doivent tenir compte des facteurs humains. Cela comprend les caractéristiques humaines fondamentales associées aux compétences et à l'expérience spécifiques, et les tâches à réaliser. En particulier, il convient de faciliter l'interaction homme-machine (c'est-à-dire les tâches, les affichages et les commandes) et d'assurer des niveaux acceptables de confort mental.

4.2.5 Environnement social et physique

4.2.5.1 Environnement social

La structure organisationnelle, les flux de travaux et les facteurs sociaux qui en résultent influencent les performances de l'être humain et du système et doivent être conçus pour faciliter l'efficacité et la fiabilité des performances humaines. Une structure organisationnelle est caractérisée par le transfert des tâches (délégation), la compétence de décision, les voies d'information, de communication et de décision, ainsi que par le nombre de niveaux hiérarchiques. Le déroulement du travail est caractérisé, par exemple, par la méthode de flux de travaux, le travail posté, le temps de travail et la planification et l'exécution du travail.

D'autres facteurs, comme le comportement de l'encadrement, la participation, la culture de sûreté et le climat social peuvent également avoir une influence sur la motivation et le comportement du personnel lors de l'utilisation du système.

4.2.5.2 Environnement physique

Les facteurs liés à l'environnement physique ayant un impact sur les personnes et, par conséquent, sur la fiabilité du système, comprennent la lumière, le bruit, les vibrations mécaniques, le climat, l'hygiène, l'humidité, la pression atmosphérique, les gaz toxiques et les rayonnements. Les facteurs environnementaux peuvent avoir une influence directe sur les aptitudes des êtres humains (par exemple, le bruit, les gaz toxiques, etc.). Ils peuvent également influencer les interactions entre les personnes et la machine (les vibrations mécaniques, par exemple) ou la machine elle-même (les vents latéraux sur une voiture qui roule, par exemple). Toutefois, outre leurs effets négatifs, ils peuvent également fournir un retour d'information permettant d'améliorer l'aptitude du personnel à interagir de manière efficace avec la machine (bruit/vibration du moteur d'une voiture qui roule, par exemple).

Certains facteurs de l'environnement physique peuvent nécessiter que les personnes utilisent des équipements de protection (appareil respiratoire, par exemple). Certaines limites humaines individuelles peuvent impliquer l'utilisation de technologies d'assistance (lunettes pour la vision de près ou dispositifs d'entrée spécialisés, par exemple). Ces éléments peuvent avoir un impact sur leurs aptitudes et doivent être pris en compte lors de la conception.

4.2.6 Élément de sortie

Il convient d'atteindre les objectifs de la tâche avec le niveau requis d'efficacité et d'efficience.

4.2.7 Retour d'information de la machine vers la personne

Un retour d'information approprié de la machine est une caractéristique importante d'une conception fiable. La personne a accès au retour d'information relatif à l'élément d'entrée provenant de la machine par le biais de signaux sonores, visuels et tactiles. Le retour d'information relatif à l'élément de sortie du système dans son ensemble donne des informations sur l'atteinte des objectifs.

Le retour d'information est important pour plusieurs raisons. Il permet à une personne de corriger tout comportement indésirable de la machine ou de l'ensemble du système afin d'améliorer les performances ou de corriger les actions non souhaitées. De plus, l'absence de retour d'information approprié peut être source d'erreurs. Par exemple, lorsqu'un ordinateur met du temps à fournir un retour d'information visuel à la suite de l'utilisation du bouton de suppression, l'opérateur répète souvent l'action. Le retour d'information peut également

permettre de réaliser une tâche de manière plus précise, par exemple, la réponse de la pédale de frein d'un véhicule peut aider le conducteur à freiner en douceur. Le retour d'information provenant de la machine et du système facilite également la conscience circonstancielle. Dans certaines circonstances, le retour d'information peut donner lieu à une modification des objectifs.

4.3 Caractéristiques humaines

4.3.1 Remarques introductives

Les êtres humains disposent d'un ensemble de caractéristiques physiques, cognitives et psychologiques qui varient d'une personne à l'autre (4.5.2). Ces caractéristiques se traduisent par des limites fondamentales des aptitudes humaines dont il faut tenir compte lors de la conception des systèmes. Une formation et une expérience appropriées permettent aux personnes de travailler de manière plus efficace, mais uniquement dans le cadre de leurs limites.

La conception de la machine et l'environnement physique et social ont une influence sur la fiabilité et les performances humaines (4.5.1). Pour assurer que les conditions de travail offrent une sûreté de fonctionnement élevée, il convient de concevoir le système de manière à maintenir dans des limites acceptables le stress lié au travail, à son environnement et à la conception technique.

4.3.2 Limites humaines

Il convient que la conception tienne compte des limites humaines.

a) Limites physiques

- Contraintes anthropométriques et biomécaniques.
- Contraintes sensorielles (l'éventail des signaux qui peuvent être perçus et différenciés, par exemple).

b) Limites cognitives

- La durée nécessaire entre la perception d'un signal et une action en réponse. Elle peut être comprise entre quelques centaines de millisecondes pour les actions fondées sur la compétence pour lesquelles la réponse est quasi automatique (et pas raisonnée) et plusieurs secondes, voire minutes, lorsqu'il est nécessaire de procéder à un raisonnement et une analyse.
- Limites de la mémoire à court terme. Seuls 5 à 7 éléments d'information peuvent être conservés dans la mémoire à court terme. Pour des quantités d'informations plus importantes, des modèles mentaux sont construits.
- Limites de la quantité d'informations qui peut être traitée en une fois (mémoire de travail).
- L'inaptitude à se concentrer de manière efficace sur plusieurs tâches à la fois ou à traiter des informations en parallèle.
- L'éventualité de perte de conscience circonstancielle à la suite d'actions reposant sur une perception erronée de la réalité.

c) Limites psychologiques

- Baisse des performances en raison d'une fatigue physique ou mentale ou de l'ennui.
- Tendance à prendre des décisions et à réaliser des actions de manière émotionnelle plutôt que raisonnée, notamment dans des situations de stress.

Etant donné que ces caractéristiques humaines ne peuvent pas être conçues hors du système, la répartition des tâches entre les personnes et le reste d'un système et la

conception des systèmes et interfaces techniques doivent être prises en compte. Il convient de tenir compte des forces relatives des êtres humains et des machines (4.4.3).

4.3.3 Comparaison homme - machine

Il convient que l'allocation des activités et des tâches d'exploitation entre l'être humain et la machine tienne compte des forces relatives de chacun d'eux.

a) Forces de l'être humain

- Aptitude de perception des signaux lumineux ou sonores.
- Aptitude d'improvisation et d'utilisation des procédures flexibles.
- Aptitude de mémorisation d'une très grande quantité d'informations pendant de longues périodes et à se souvenir de faits pertinents au moment opportun.
- Aptitude de raisonnement inductif.
- Aptitude de jugement.

b) Forces de la machine

- Aptitude de détection de petites quantités et d'un large éventail de signaux visuels et sonores.
- Aptitude de réponse rapide aux signaux de commande et aptitude à exercer un effort important de manière progressive et précise.
- Aptitude de réalisation de tâches répétitives et routinières de manière cohérente et précise.
- Aptitude d'enregistrement rapide, puis de suppression totale des informations.
- Aptitude de raisonnement déductif, notamment la puissance de calcul.
- Aptitude de traitement d'opérations extrêmement complexes et de réalisation de plusieurs tâches simultanément.

Il existe des différences importantes entre l'être humain et la machine.

- A l'inverse de l'être humain, la machine peut être modifiée, mise à niveau et sa conception peut être revue. Les êtres humains naissent avec des différences génétiques naturelles modelées par l'environnement. Les aptitudes ou capacités naturelles sont développées par l'éducation et la formation.
- Les machines peuvent être fabriquées de manière à fournir l'élément de sortie exact et à reproduire une opération précise. Les êtres humains sont tous différents, tant du point de vue des caractéristiques sensorielles, cognitives, physiques et des performances. Certains aspects particuliers des performances humaines peuvent être nivelés de manière plus importante par la sélection et la formation.

4.4 Facteurs de performance humaine

4.4.1 Généralité

Les performances et la fiabilité des personnes au sein d'un système varient en fonction de nombreuses conditions internes et externes qui diffèrent d'une personne à l'autre et d'un instant à l'autre. Les facteurs qui influencent l'aptitude des êtres humains à accomplir une tâche de manière fiable sont appelés facteurs de performance (également appelés contexte d'utilisation).

La Figure 1 présente les types de facteurs de performance par des flèches grises.

La Figure 2 donne des exemples permettant de distinguer les facteurs de performance externes et internes.

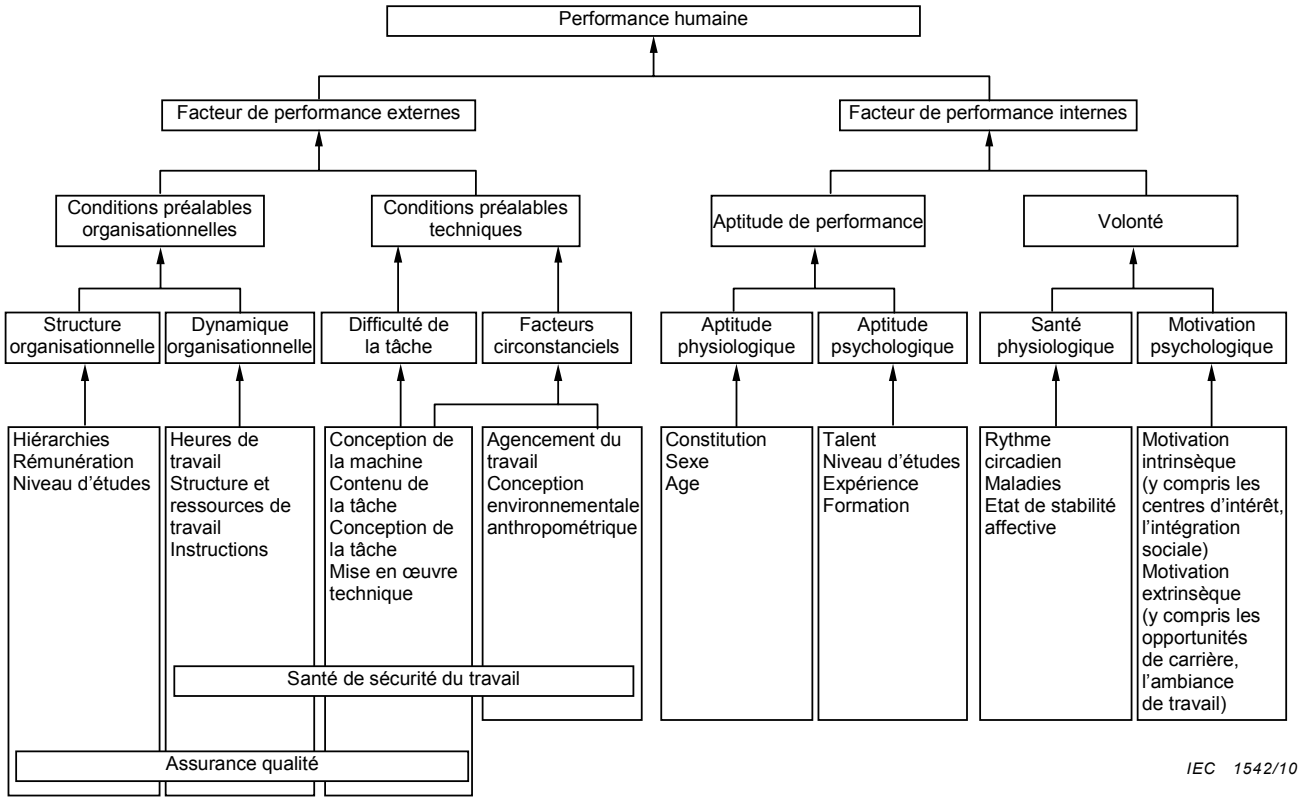

Figure 2 – Facteurs de performance humaine

4.4.2 Facteurs de performance externes

Les facteurs de performance externes résultent de conditions préalables organisationnelles et techniques. Dans la plupart des cas, les conditions préalables organisationnelles (4.2.5.1) ne peuvent être décrites que du point de vue qualitatif. Par ailleurs, les conditions préalables techniques, y compris la conception de la machine (4.2.4) et les facteurs environnementaux (4.2.5.2) ne peuvent, le plus souvent, être décrites que du point de vue quantitatif.

La prise en compte des facteurs de performance externes dans la conception a un effet positif sur les performances.

4.4.3 Facteurs de performance internes

Les facteurs de performance internes peuvent être classés en aptitude de performance et en volonté. Il s'agit de facteurs issus de fluctuations physiologiques et psychologiques dont font l'objet les personnes et se présentent sous la forme de «caractéristiques, compétences et expérience individuelles» dans la Figure 1.

Ils comprennent les limites humaines (4.3.2) et les différences de taille, de force, de talent, de compétence, d'expérience et de connaissance, ainsi que les fluctuations psychologiques et les facteurs de motivation.

4.5 Analyse de fiabilité humaine (AFH)

4.5.1 Présentation

L'analyse de fiabilité humaine fait partie intégrante de l'analyse globale de la fiabilité d'un système technique. Elle implique les activités suivantes:

- Identification du potentiel de défaillance humaine.
- Analyse des sources d'erreur et des causes de violations, afin de pouvoir définir des contre-mesures appropriées.
- Le cas échéant, quantification de la fiabilité humaine de manière à pouvoir quantifier la fiabilité de l'ensemble du système.
- Décision sur la nécessité d'apporter des améliorations.

4.5.2 Identification du potentiel d'erreur humaine

En règle générale, le rôle des êtres humains dans le système consiste à recevoir un élément d'entrée (des instructions par exemple) ou des informations par l'intermédiaire d'un processus sensoriel. Cet élément d'entrée fait alors l'objet d'un processus cognitif faisant appel à des connaissances, à la mémoire ou à la formation afin de prendre une décision quant à la manière de répondre. La décision qui en résulte est mise en œuvre par un processus d'action moteur impliquant l'utilisation des muscles concernés. Souvent, l'action génère un retour d'information qui fournit des éléments d'entrée supplémentaires susceptibles de confirmer l'exactitude de l'action ou d'indiquer un problème auquel il faudra remédier (Figure 3). Cela s'applique si la tâche implique l'exploitation d'une machine, le suivi de procédures, la conception d'équipements ou de procédures, ou encore la réalisation d'une tâche de gestion ou de supervision.

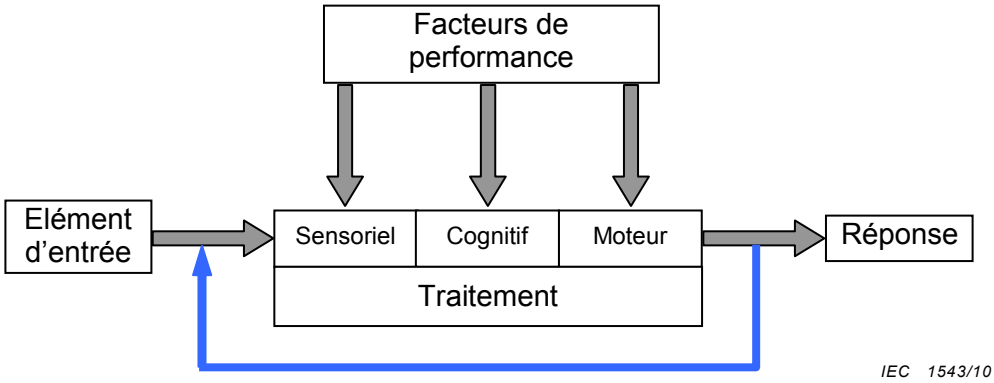

Figure 3 – Modèle simplifié de traitement des informations par l'être humain

Dans la Figure 3, l'élément d'entrée comprend les objectifs de la tâche, l'environnement et le retour d'information.

Le traitement des informations et la prise de décision font souvent appel à la mémoire et peuvent nécessiter d'autres informations externes. Des erreurs peuvent se produire à tous les stades de ce processus cognitif, le potentiel d'erreur pouvant être identifié en considérant chaque stade cognitif un par un afin de déterminer où des problèmes peuvent survenir. Le potentiel d'erreurs humaines peut également être identifié par une Analyse des Modes de Défaillance et de leurs Effets (AMDE) qui débute par une analyse de la tâche et qui identifie les erreurs possibles à chaque étape du déroulement, puis détermine comment ces erreurs peuvent se produire (voir l'Annexe A).

4.5.3 Analyse des défaillances humaines afin de définir des contre-mesures

Une bonne compréhension des causes des défaillances humaines et de la manière dont celles-ci se produisent permet de définir des contre-mesures appropriées et d'améliorer la sûreté de fonctionnement du système.

Les défaillances humaines peuvent être classées en violations et erreurs. Les violations sont des écarts par rapport à une voie correcte connue. Elles se produisent en général lorsqu'il y a une recherche non intentionnelle d'un comportement incorrect (pour un gain de temps à

moindre effort ou pour une reconnaissance par ses pairs, par exemple). Des règles peuvent être enfreintes lorsque la personne estime qu'il existe un meilleur moyen d'atteindre son objectif, tente de dissimuler des erreurs ou d'assister des collègues. Les violations sont rarement malveillantes.

On parle d'erreurs lorsqu'une séquence prévue d'activités mentales ou physiques ne parvient pas à obtenir les résultats prévus. Ceci peut se produire en raison du caractère inapproprié de la planification ou de la non exécution des activités dans le respect de cette dernière. Cette distinction entraîne une classification des erreurs en fautes, étourderies et défaillances.

Un autre type d'erreur concerne une action correcte réalisée par un individu mais qui génère une performance incorrecte. Ces erreurs peuvent également être divisées en deux groupes:

- Les étourderies qui sont des erreurs d'exécution se produisant souvent dans le cadre de tâches connues et routinières réalisées de façon automatique avec peu de réflexion (la dactylographie ou la conduite, par exemple).
- Les défaillances de la mémoire ou les défaillances cognitives (perte d'une place dans une liste, par exemple), ainsi que les défaillances qui peuvent se produire en cas de réalisation accidentelle d'une procédure connue au lieu d'une nouvelle procédure requise.

La classification est un point de départ utile pour l'analyse des causes de défaillance humaine. Les approches de conception suivantes peuvent être adoptées lors de la constatation ou de la suspicion de problèmes.

Pour limiter les violations, les raisons pour lesquelles les personnes peuvent agir de manière incorrecte doivent être identifiées et les comportements corrects doivent être «récompensés» contrairement aux comportements incorrects. Par exemple, la probabilité de violation est plus faible lorsque la manière la plus facile est la manière correcte de réalisation.

Les fautes sont réduites en tenant compte des limites humaines inhérentes dans la conception, puis en s'assurant que les personnes ont les connaissances et les compétences nécessaires à la réalisation de la tâche et qu'elles disposent d'un délai suffisant pour mener un raisonnement correct. Des instructions claires, des affichages et des commandes intuitifs et des aide-mémoire permettent de limiter les fautes.

Il est plus difficile de limiter les étourderies et les défaillances lorsque les personnes ont de bonnes intentions, les erreurs se produisant souvent dans le cadre d'activités automatiques que l'individu ne contrôle pas consciemment. Les conceptions qui entretiennent et contrôlent la conscience circonstancielle, répondant aux attentes mentales inconscientes et signalant très tôt qu'une erreur s'est produite, peuvent aider à corriger les étourderies et les défaillances avant qu'elles compromettent la sûreté de fonctionnement globale.

L'Article A.1 énumère un certain nombre de méthodes AFH qui incluent des techniques d'analyse des mécanismes et des causes des défaillances humaines qui sont ensuite examinées afin de définir des contre-mesures. Il est également possible de réduire tous les types de défaillances humaines en considérant les facteurs de performance dans la conception du système et de ses composants, et en adoptant une conception visant à améliorer les performances humaines.

4.5.4 Quantification de la fiabilité humaine

Lorsque la fiabilité d'un système doit être quantifiée, il peut être judicieux d'accorder également de l'importance à la probabilité d'erreur humaine. Un certain nombre de méthodes différentes peuvent être appliquées dans ce but. Ces méthodes sont répertoriées et brièvement décrites dans l'Annexe A. D'une manière générale, les probabilités s'appliquent aux étourderies, aux défaillances et aux fautes, en tenant compte des facteurs de performance. Les violations malveillantes sont normalement exclues de l'analyse (c'est-à-dire, les personnes sont supposées bien intentionnées mais peuvent commettre des étourderies, des défaillances et des fautes).

4.6 Systèmes critiques

Un système critique est un système informatique, électronique, mécanique ou électromécanique dont la défaillance peut provoquer des dommages importants tels que des blessures ou la mort de personnes, une avarie importante du matériel ou une perte financière considérable. Lors de la conception des systèmes critiques, il est particulièrement important de tenir compte du fonctionnement normal, mais également du fonctionnement dans les conditions de défaillance possibles dans lesquelles l'opérateur peut prendre des décisions en état de stress. Il est essentiel d'envisager la manière dont l'opérateur peut répondre dans l'éventail le plus large possible des situations anormales, et de concevoir l'interface en vue de limiter toute mauvaise interprétation possible.

Les systèmes critiques sont généralement conçus pour limiter ou exclure toute intervention de l'homme. Toutefois, lorsqu'une intervention de l'homme se révèle nécessaire, elle doit habituellement être correcte, rapide et décisive afin d'interrompre ou de prévenir toute évolution ultérieure de conditions défavorables.

D'une façon générale, il existe trois types de situations anormales dans lesquelles le facteur humain est un élément critique. Ces situations ne sont pas exclusives et certains cas peuvent évoluer d'une situation à une autre:

a) dans une situation d'urgence, l'aptitude de décision de l'être humain diminue et les informations peuvent être mal interprétées;

b) dans des situations normales ou anormales, dans lesquelles l'opérateur n'a pas conscience de l'influence de ses actions. Dans ce cas, l'opérateur n'est pas dans une situation de stress, pouvant ainsi ne pas accorder une attention appropriée et contribuer de ce fait au préjudice d'une certaine manière;

c) situations dans lesquelles l'opérateur ne peut connaître les résultats et doit être aidé dans la prise de décisions et le suivi des décisions prises (éventuellement sur de très longues périodes).

Dans ces situations, les activités ci-dessous permettent d'augmenter la prise de décisions appropriées:

- en reconnaissant le potentiel d'erreur accru et les conséquences des erreurs d'un individu dans le cas de systèmes fortement automatisés;
- en simulant des situations d'urgence avec des prototypes d'interface permettant d'évaluer la compréhension humaine et en utilisant le retour d'information obtenu pour améliorer ces interfaces;
- s'il existe un risque de confusion, en formant les opérateurs à la manière de répondre à la situation;
- en sélectionnant un personnel capable de s'adapter de manière efficace aux environnements contraignants de fonctionnement multi-tâches;
- en formant régulièrement les opérateurs à la gestion manuelle du système dans des conditions de défaillance possibles;
- en mettant en place les moyens de répondre à la suffisance/au manque de considération, tels que la sélection du personnel, les procédures de contrôle, l'existence d'un système de sécurité comportemental, etc.;
- en intégrant des procédures et des outils de modélisation et de prise de décisions lorsque la situation ne permet pas de connaître à l'avance les risques encourus et lorsque les opérateurs doivent agir avec une forte incertitude (par exemple, dans les secteurs de la finance, de la défense, de l'exploration, de l'élimination des déchets, etc.).

4.7 Lignes directrices pour la conception centrée sur l'humain

Les lignes directrices suivantes pour la conception centrée sur l'humain, si elles sont appliquées correctement, contribuent à améliorer la fiabilité humaine et la sûreté de fonctionnement du système.

a) Aptitude à l'emploi

- Rendre la conception durable, fiable et applicable pour l'utilisation prévue.
- Allouer les fonctions de manière appropriée entre les personnes et la technologie.
- Adapter les caractéristiques physiques, cognitives et psychologiques des utilisateurs.
- Procéder à un essai avec les utilisateurs.

b) Simplicité

- La conception doit être aussi simple que possible.
- Limiter les besoins en formation.
- Rendre les fonctions évidentes.

c) Tolérance et résistance aux erreurs

- Rendre le système tolérant aux erreurs.
- Prévoir la conception de sorte qu'il ne soit pas possible de commettre des erreurs.
- Prévoir une conception à sûreté intégrée.

d) Cohérence

- Faire en sorte que la conception soit en accord avec l'expérience de l'utilisateur, avec les objets de la vie réelle et avec des systèmes analogues.

e) Normalisation

- Utiliser un matériel et des logiciels normalisés, le cas échéant.
- Conserver des interfaces identiques pour des fonctions identiques.
- Assurer l'uniformité des commandes, des affichages, des marquages, du codage, de l'étiquetage et de la disposition.
- Caractériser la présentation.
- Normaliser la terminologie, l'aspect et les textures (sensations).
- Faire en sorte que les équipements analogues du point de vue fonctionnel soient interchangeables.

f) Perspective centrée sur l'utilisateur

- Comprendre les rôles, les responsabilités, les décisions et les objectifs de l'utilisateur.
- Fournir un retour d'information régulier et informatif.
- Utiliser des termes et des images familiers.
- Concevoir en fonction des aptitudes de l'utilisateur.
- Optimiser les performances et la satisfaction des utilisateurs.
- Limiter les exigences en matière de formation.
- Faciliter le transfert de compétences.
- S'adapter à la diversité physique.

g) Maintenabilité et logistique de maintenance

- Conception visant à faciliter le démontage et le remontage.
- Prévoir des outils spécialisés, si nécessaire.
- Prévoir un soutien logistique, le cas échéant.
- Conception d'outils communs.
- Faire en sorte que la conception soit facile d'entretien.

L'Annexe B récapitule l'influence de la conception ergonomique et son impact sur la sûreté de fonctionnement du système dans des situations particulières.

4.8 Processus de conception centrée sur l'humain

4.8.1 Principes de la conception centrée sur l'humain dans le processus de conception

La conception orientée vers l'humain implique le processus d'ingénierie de l'ensemble du système pour répondre aux besoins de l'opérateur humain et des autres parties prenantes. Il s'agit d'optimiser les capacités et les performances globales du système en fonctionnement.

Quel que soit le processus de conception ainsi que l'allocation des responsabilités et des rôles adoptée, il convient que l'intégration d'une approche orientée vers l'humain respecte les principes de conception centrée sur l'humain énoncés ci-après (et décrits de façon plus complète dans l'ISO 9241-210):

a) La conception est basée sur une compréhension explicite des utilisateurs, des tâches et des environnements.

b) Les utilisateurs sont impliqués tout au long de la conception et du développement.

c) La conception est dirigée et affinée par l'évaluation centrée sur l'utilisateur.

d) Le processus est itératif.

e) La conception tient compte de l'expérience de l'utilisateur dans son ensemble (y compris de la manière dont il s'adapte à la tâche, à l'environnement de travail, au soutien, à la formation et à l'utilisation à long terme).

f) L'équipe de conception dispose de compétences et de points de vue pluridisciplinaires.

4.8.2 Activités de conception centrée sur l'humain

Cinq activités liées de conception centrée sur l'humain doivent être mises en place au cours du projet de développement d'un système (décrit dans l'ISO/FDIS 9241-210). Ces activités ont lieu tout au long du projet et varient tant dans la forme qu'au niveau du contenu, selon l'avancée du projet.

a) Planifier les activités de conception orientée vers l'humain.

b) Analyser, comprendre et préciser le contexte d'utilisation.

c) Analyser les besoins et spécifier les exigences utilisateur.

d) S'appuyer sur les connaissances actuelles des facteurs humains pour produire des solutions répondant à ces exigences.

e) Comparer les solutions de conception aux exigences et au retour d'information de l'utilisateur, et modifier les unes et/ou les autres en conséquence.

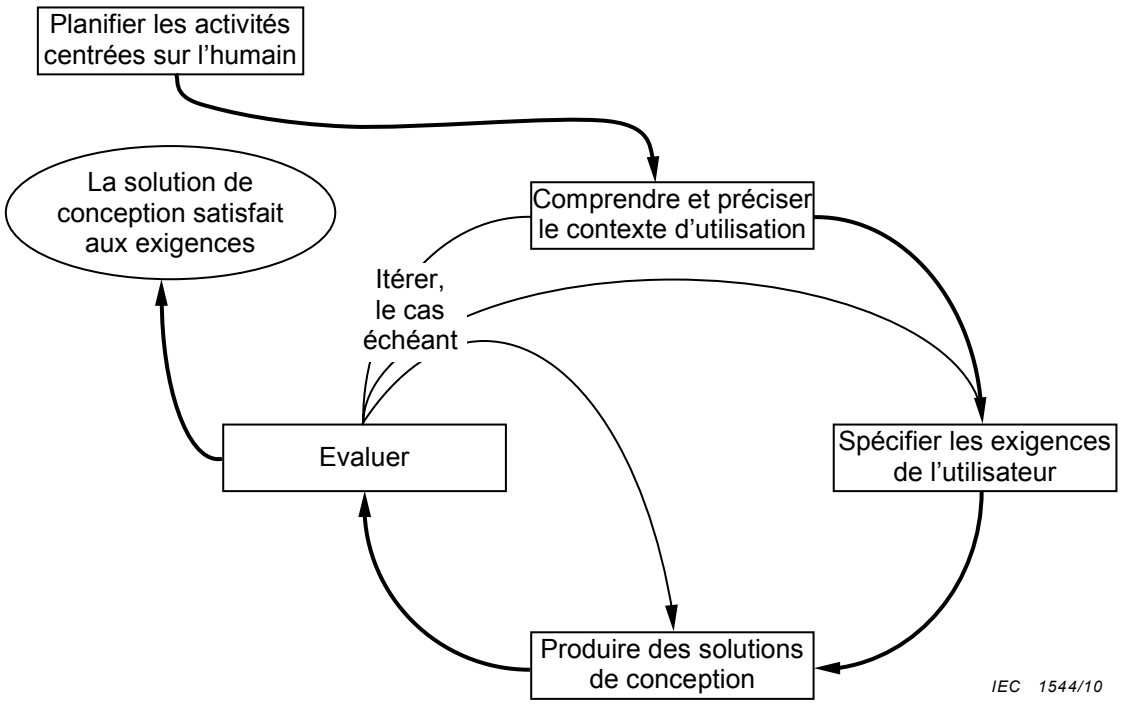

Figure 4 – Activités de conception centrée sur l'humain

Dans la pratique, ces activités peuvent se chevaucher ou être réalisées séparément. Les activités ultérieures peuvent également modifier les hypothèses formulées aux stades antérieurs. La Figure 4 (issue de l'ISO 9241-210) illustre leur interdépendance.

5 Conception orientée vers l'humain dans le cycle de vie du système

5.1 Présentation

La prise en compte des aspects humains dans l'ingénierie des systèmes a pour objet d'incorporer les intérêts et les besoins des individus et/ou des groupes qui vont travailler avec le système. Cette approche présente les avantages suivants:

- Les projets anticipent et répondent aux questions et aux risques liés à l'interaction homme-système.
- La planification du cycle de vie et l'attribution des ressources du système sont prévues pour faire face de manière rentable aux risques liés aux facteurs humains.
- Les besoins des parties prenantes dans le système sont transmis à l'organisation de développement.
- La sûreté de fonctionnement de l'ensemble du système est améliorée.

L'approche de conception orientée vers l'humain implique l'application de méthodes de conception centrée sur l'humain dans le cycle de vie du système, tout en tenant compte du caractère variable des performances et de la fiabilité des êtres humains.

Il convient de concevoir les systèmes de manière à limiter le potentiel d'erreur humaine et à réduire l'impact des erreurs susceptibles de se produire. Pour atteindre une fiabilité humaine acceptable, le processus de conception doit tenir compte de tous les aspects humains pertinents, tels que:

- clarifier et définir les exigences pour tous les utilisateurs, personnels impliqués dans la maintenance et autres parties prenantes;

- définir les contextes d'utilisation et de maintenance du système, notamment les caractéristiques des utilisateurs, les tâches et les environnements de travail;
- définir les exigences en matière de performance humaine et de confort mental nécessaires pour atteindre les objectifs du système durant toutes les phases du cycle de vie;
- identifier le potentiel d'erreur humaine par des opérateurs, du personnel impliqué dans la maintenance et des autres personnes faisant partie du système, au cours des différentes phases du cycle de vie.

La conception orientée vers l'humain repose sur une base de connaissances des facteurs humains applicable aux conceptions centrées sur l'utilisateur, robustes et tolérantes aux erreurs, en adaptant les technologies appropriées afin de limiter les difficultés à satisfaire aux exigences de performance humaines et améliorer l'interaction homme-système.

Cette approche de conception orientée vers l'humain permet non seulement d'améliorer la fiabilité humaine, mais présente également d'autres avantages importants, selon la liste suivante:

- productivité augmentée, performances améliorées et plus grande satisfaction de l'utilisateur;
- erreurs de conception et d'exploitation réduites;
- procédures simplifiées d'exploitation et de maintenance du système;
- délai d'assistance technique réduit;
- besoins limités de formation professionnelle particulière;
- risques d'accidents graves limités;
- limitation des coûts et réduction des coûts liés au cycle de vie.

5.2 Cycle de vie du système

Il convient d'intégrer les aspects humains dans le processus d'ingénierie et le cycle de vie des systèmes. Le concept de cycle de vie du système adapté de la CEI 60300-3-15 est illustré à la Figure 5 afin d'identifier l'influence essentielle de la conception orientée vers l'humain dans le cycle de vie du système. Les étapes du cycle de vie du système sont brièvement décrites ci-dessous:

– L'étape de *Faisabilité/Définition* consiste à identifier les besoins du marché, définir/identifier l'environnement d'application/calendrier d'exécution opérationnels, définir les exigences système préliminaires et à confirmer les solutions de conception réalisables par la production de spécifications techniques pour la conception du système. Les activités de processus impliquent la définition et l'analyse d'exigences, la conception architecturale et la conception/évaluation fonctionnelles afin de définir des spécifications système de haut niveau. Les facteurs humains à prendre en compte à ce stade sont la variabilité des performances et la fiabilité des personnes qui utiliseront le système. Il convient que les activités de conception centrée sur l'humain commencent par un plan contenant toutes les exigences.

– L'étape de *Conception/Développement* consiste à planifier et à réaliser les solutions de conception d'ingénierie retenues pour la réalisation des fonctions du système. Cette étape résulte en une prestation appropriée relative au développement du système, comprenant la modélisation, la construction de prototypes, l'évaluation des risques et l'identification de l'interface des éléments du système et des sous-systèmes. A ce stade, il est indispensable d'accorder une attention continue à la variabilité des opérateurs. Il convient également d'identifier les besoins de maintenance à ce stade afin d'assurer un accès approprié dans la conception initiale. Il convient de tenir compte de la variabilité des performances et de la fiabilité des personnes qui procèdent aux opérations de maintenance.

– L'étape de *Réalisation/Mise en œuvre* consiste à exécuter les décisions "achat ou fabrication" pour l'acquisition et la mise en place des éléments de sous-systèmes. Les

prestations de réalisation traitent d'activités telles que les applications technologiques, la fabrication, le conditionnement et l'approvisionnement en fournitures de manière à assurer la transposition complète de la conception du système en éléments de produits ou de sous-systèmes spécifiés. Les produits ou éléments réalisés peuvent combiner des fonctions matérielles et logicielles. La mise en œuvre inclut des activités telles que l'intégration des fonctions du système, la vérification des sous-systèmes et l'installation du système. A ce stade, il convient de former les opérateurs et les personnes qui assurent la maintenance du système.

– L'étape d'*Exploitation/Maintenance* permet la mise en place du système pour la fourniture du service et de maintenir la capacité opérationnelle du système grâce à la maintenance. Les activités de processus incluent l'exploitation et le maintien du système en service conformément à ses exigences de performance, la formation des opérateurs et du personnel de maintenance afin de pérenniser les compétences et qualifications, l'interface client destinée à établir une relation de service, la tenue d'enregistrements portant sur l'état de performance du système et le compte rendu des défaillances afin de déclencher les actions correctives et préventives dans les délais impartis.

– L'étape d'*Amélioration* consiste à améliorer la performance du système par l'ajout de fonctionnalités afin de satisfaire aux demandes nouvelles des utilisateurs concernant le système. Les activités de processus incluent une mise à jour logicielle, l'ajout de matériel(s), la réparation et la remise en état, la formation professionnelle, la simplification des procédures afin d'améliorer l'efficacité opérationnelle, la gestion de l'obsolescence, la restructuration organisationnelle de manière à renforcer la convenance et à accroître la plus-value pour le client. Il convient de réexaminer tous les facteurs humains considérés dans les étapes précédentes afin de réaliser toutes les améliorations possibles en fonction des connaissances du fonctionnement du système.

– L'étape de *Retrait/Démantèlement* consiste à mettre fin à l'existence du système. Au terme du service du système au client, le système peut être démonté, réinstallé pour une autre utilisation ou éliminé, dans toute la mesure du possible sans affecter les environnements. Il convient de prendre en compte les caractéristiques physiques et mentales des opérateurs affectés à la mise au rebut et au processus de recyclage.

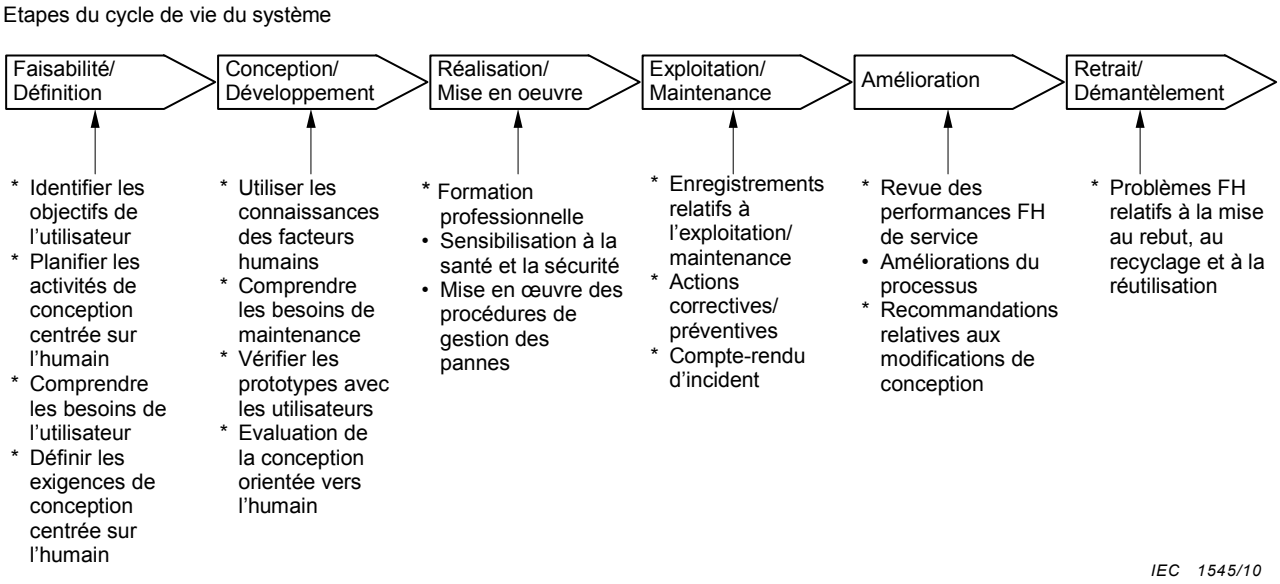

Figure 5 – Aspects humains du cycle de vie du système

5.3 Intégration de la conception orientée vers l'humain dans l'ingénierie des systèmes

La conception orientée vers l'humain est intégrée dans l'ingénierie des systèmes tout au long du cycle de vie du système, notamment au cours des étapes de conception/développement, de réalisation/mise en œuvre et d'exploitation/maintenance. C'est au cours de ces étapes que

la conception orientée vers l'humain a le plus d'influence sur les tâches d'ingénierie des systèmes liées aux améliorations de la conception, aux fonctions de sécurité, aux impacts de l'automatisation, aux compromis de performance homme-système, à la facilité d'utilisation et à la charge de travail.

Les principales activités sont répertoriées ci-dessous:

a) Compréhension totale et exhaustive des besoins des utilisateurs et des organismes utilisateurs.

b) Identification des risques liés à la sûreté de fonctionnement découlant de l'intervention de l'homme dans le système (erreurs intempestives ou comportement humain potentiellement malveillant).

c) Identification des facteurs qui influencent les performances humaines (voir 4.5).

d) Application des connaissances des facteurs humains à la conception afin d'obtenir des performances humaines optimales à moindre risque.

e) Itération des solutions de conception proposées et intégration du retour d'information provenant des utilisateurs dans la conception.

Ces activités sont décrites de manière plus détaillée dans les articles suivants. Il convient que les ressources allouées aux activités de conception centrée sur l'humain soient fonction des avantages probables liés à la réalisation des activités à des étapes particulières du cycle de vie, et des risques associés si ces activités ne sont pas réalisées. Il convient que les risques à prendre en compte incluent la possibilité de ne pas satisfaire aux exigences de fiabilité, de sûreté de fonctionnement ou autres besoins des parties prenantes, les implications opérationnelles et professionnelles et les coûts connexes d'une re-fabrication inévitable. Les meilleures pratiques sont présentées ci-dessous et dans l'Annexe C.

6 Conception orientée vers l'humain à chaque étape du cycle de vie

6.1 Présentation

L'Annexe C fournit une liste des activités nécessaires à la mise en œuvre de la conception orientée vers l'humain à chaque étape du cycle de vie du système. Ces activités sont récapitulées dans le présent article.

6.2 Etape de faisabilité/définition

6.2.1 Faisabilité

En phase de faisabilité, il est important de bien comprendre les objectifs que l'utilisateur ou l'organisme utilisateur souhaite atteindre par l'utilisation du système, d'évaluer leur viabilité et d'identifier tous les risques susceptibles d'être intégrés dans les spécifications et d'être considérés lors de la conception. Il convient de spécifier les exigences de sûreté de fonctionnement du système, étant donné qu'elles peuvent avoir un impact sur les rôles de l'être humain au sein du système.

6.2.2 Planification de la conception centrée sur l'humain

Un plan de conception centrée sur l'humain est un élément essentiel permettant d'établir une stratégie de gestion de l'effort de conception centrée sur l'humain afin de prendre en charge le développement et l'exploitation du système. L'objectif est d'apporter une réponse aux problèmes rencontrés lors de la conception centrée sur l'humain afin d'améliorer la performance de l'ensemble du système et de réduire les coûts de développement et ceux liés au cycle de vie. Cela est obtenu en optimisant les performances humaines lorsque le système fonctionne et est maintenu dans l'environnement opérationnel. Il convient que la planification comprenne les activités suivantes:

- Déduire les objectifs des activités centrées sur l'humain, à partir des objectifs organisationnels globaux du système.
- Définir les ressources consacrées à l'utilisation des méthodes de conception centrée sur l'humain. Il convient qu'elles dépendent du niveau de risque qui serait induit par le projet à chaque étape si les méthodes centrées sur l'humain n'étaient pas utilisées.
- Spécifier à quel moment et de quelle manière les activités centrées sur l'humain s'intègrent dans le cycle de vie de l'ensemble du système, et la façon d'utiliser l'élément d'entrée généré par les activités dans le cycle de vie du système.
- Décider des méthodes à inclure et de la manière de les associer dans le cycle de vie.
- Permettre des itérations, le cas échéant.
- Identifier la nécessité d'implication de l'utilisateur et les frais associés.
- Définir les éléments de sortie et les critères de réussite de chaque activité.
- Identifier les compétences nécessaires et prévoir les moyens de les fournir.

Il convient de développer un plan de conception centrée sur l'humain dès l'étape de faisabilité/définition du cycle de vie du système afin d'optimiser son efficacité à influencer la définition du système et le développement du cadre. Il convient que le plan de conception centrée sur l'humain fasse partie intégrante du plan de l'ensemble du système.

6.2.3 Compréhension des besoins

Il convient d'identifier les rôles de chaque groupe de parties prenantes susceptible d'être affecté par le système (y compris les groupes d'utilisateurs et le personnel de maintenance) et d'analyser les tâches qu'ils doivent réaliser. Il convient d'évaluer l'importance de la facilité d'utilisation et de performances humaines sans erreur. Il convient d'identifier le contexte général d'utilisation prévue du système, y compris les facteurs environnementaux (voir 4.2.5.2) ainsi que les structures organisationnelles, les tâches et les flux de travaux (voir 4.2.5.1). Il peut s'avérer nécessaire de visiter le site d'exploitation afin d'obtenir ce type d'informations.

6.2.4 Exigences du système

L'intégration de questions spécifiques à l'être humain dans les exigences du système implique:

- de fournir des éléments d'entrée de conception centrée sur l'humain afin de développer les spécifications du système;
- d'inclure les exigences de conception centrée sur l'humain dans le processus d'assurance de qualité;
- d'inclure les exigences de conception centrée sur l'humain pour l'externalisation et la sous-traitance;
- d'établir des procédures orientées vers l'humain pour l'exploitation et la maintenance du système.

Il s'agit d'obtenir un système centré sur l'humain, résistant et tolérant aux pannes, adapté et utilisable, afin d'assurer l'efficacité de son exploitation.

- Il convient d'établir les exigences utilisateur en partenariat avec les utilisateurs potentiels.
- Il convient d'établir le comportement et les performances prévus du système en fonction des utilisateurs.

6.2.5 Exigences de conception centrée sur l'humain

L'analyse des exigences centrées sur l'humain fournit les informations nécessaires et les données pertinentes pour les activités suivantes:

- détermination des questions liées à la conception centrée sur l'humain dans l'application du système et le scénario de fonctionnement;
- intégration des principes de conception centrée sur l'humain dans le contexte du système;
- ajustement du projet de conception centrée sur l'humain afin de satisfaire aux exigences du système.

Il convient que les exigences de conception centrée sur l'humain comprennent les éléments suivants:

- rôles et responsabilités de l'opérateur et du personnel de maintenance;
- interfaces homme-système influençant l'efficience et l'efficacité des performances de l'utilisateur;
- spécification du contexte d'utilisation du système, y compris les facteurs environnementaux (voir 4.2.5.2) ainsi que les structures organisationnelles, les tâches et les flux de travaux (voir 4.2.5.1);
- des systèmes de mesure de la performance du système, y compris les performances de l'opérateur/du personnel de maintenance;
- les exigences en matière de confort mental et de satisfaction de l'utilisateur;
- la conception de l'architecture du système affectant les interactions entre l'homme et le système;
- l'environnement d'application du système ayant un impact sur les ressources et les exigences liées à l'humain.

Afin d'obtenir un retour d'information, il convient de présenter les exigences de conception centrée sur l'humain aux parties prenantes concernées. Il est possible de s'appuyer sur des scénarios d'utilisation pour présenter ces exigences. En effet, ces scénarios présentent l'avantage d'être relativement faciles à appliquer et peuvent être aisément appréhendés par d'autres parties prenantes du projet.

Il convient de mener l'analyse des exigences de conception centrée sur l'humain conjointement avec le plan de conception centrée sur l'humain au cours de l'étape de faisabilité/définition du cycle de vie du système. Cela permet de faciliter le processus d'ajustement afin de répondre aux besoins spécifiques du projet dans la définition du système. Le processus d'ajustement du projet est présenté dans la CEI 60300-2.

6.3 Conception/développement

Dans la conception du système, l'analyse de conception centrée sur l'humain est menée au cours de l'étape de conception/développement du cycle de vie du système. L'objectif est d'assurer que

- les exigences du système reflètent correctement les aptitudes et limites homme-système,
- les caractéristiques de performance homme-système donnent des informations pertinentes permettant d'identifier les options et alternatives de conception,
- la fiabilité humaine et les autres risques en matière de sûreté de fonctionnement du système liés à l'être humain sont identifiés, évalués et correctement résolus dans la conception.

Il convient que les spécifications du système et que les procédures d'exploitation et de maintenance tiennent compte des éléments suivants:

- les performances humaines, telles que les aptitudes et les limites humaines (voir 4.3.3), la charge de travail, l'allocation des fonctions, la conception matérielle et logicielle, les aides à la décision, les contraintes environnementales et la performance de l'équipe par rapport à celle de l'individu;

- les besoins en formation, tels la durée et l'efficacité de la formation, le perfectionnement des compétences, les outils et équipements de formation et la formation intégrée;
- les exigences en matière de recrutement, telles les niveaux de recrutement, la composition de l'équipe et la structure organisationnelle;
- la sélection du personnel, telle le niveau de compétence minimal, les compétences particulières, l'expertise et l'expérience;
- les risques liés à la santé et la sécurité pouvant apparaître à chaque étape du cycle de vie. Les points soulevés portent sur les matériaux et situations dangereux, la conception du système et des équipements pour une exploitation sûre, les influences biomédicales, les équipements de protection et les exigences en matière d'avertissement et d'alarme.

Il convient que la conception du système tienne compte de la nécessité pour les êtres humains d'être capables de déceler, de diagnostiquer et de corriger les pannes en cours de fonctionnement, y compris les complexités du système en cas de défaillances multiples.

Il convient de revoir le système en cohérence avec les connaissances scientifiques applicables en matière de facteurs humains, les usages, les normes, les lignes directrices, les réglementations et la législation. Il convient que les utilisateurs évaluent les prototypes afin d'affiner l'aptitude du système de développement à être utilisé. Il convient de soumettre le système à essai dans le cadre d'une procédure de vérification et de validation afin d'assurer qu'il satisfait aux exigences vis-à-vis de l'utilisateur, des tâches et de l'environnement, telles que définies dans sa spécification. A cet effet, il est possible d'utiliser un prototype évoluant dans un environnement de travail simulé afin de soumettre à essai la manière dont l'être humain interagit avec la conception proposée. Dans le cas de systèmes et/ou composants plus complexes, où les interactions humaines sont particulièrement importantes, il convient de soumettre le système à essai lors des exploitations initiales.

6.4 Réalisation/mise en œuvre

A ce stade, le produit est fabriqué, les composants du système sont assemblés et le produit est mis en place pour l'application et l'exploitation.

La conception centrée sur l'humain inclut les activités suivantes:

- Revue des interactions homme-machine à la lumière de l'expérience acquise.
- Évaluation des risques plus détaillée, notamment les risques liés à la fiabilité humaine de l'étape exploitation/maintenance.
- Formation professionnelle dans les domaines nécessaires à l'utilisation du système.
- Sensibilisation à la santé et la sécurité.
- Mise en œuvre de procédures de gestion des pannes.
- Revue de conformité avec la réglementation.
- Soumettre le système définitif à essai afin d'assurer qu'il satisfait aux exigences orientées vers l'humain.

6.5 Exploitation/maintenance

Une conception adaptée permet de réduire les erreurs d'exploitation et de maintenance, mais non de les éliminer. Il est important de consigner les erreurs dans un rapport de manière à pouvoir les examiner et à apporter des améliorations. Ceci exige une culture axée sur la consignation des erreurs en toute liberté sans crainte de représailles, et sur la compréhension des causes d'erreur sous-jacentes, ainsi que des conditions susceptibles de provoquer des erreurs.
Il convient de prévoir une simulation et/ou formation périodique qui répondent aux situations d'urgence, et d'appliquer les enseignements établis afin d'améliorer les performances du système, ainsi que la sensibilisation et les compétences des êtres humains.

En phase d'exploitation/maintenance, l'évaluation de la conception centrée sur l'humain consiste à vérifier que les considérations liées à cette conception ont été correctement intégrées dans le système pour des performances opérationnelles efficaces. La conception centrée sur l'humain est évaluée en soumettant le système à essai et en vérifiant la performance obtenue. Il s'agit de démontrer la conformité aux exigences de conception centrée sur l'humain dans un environnement d'application. Il convient que l'évaluation de la conception centrée sur l'humain intègre les activités suivantes:

- Mesure de la performance et du confort mental de l'opérateur dans des tâches critiques.
- Détermination de l'efficience et de l'efficacité de l'intervention de l'homme.
- Maintien des enregistrements d'essai de conception centrée sur l'humain et des données d'évaluation comme base d'évaluation et d'amélioration.
- Évaluation de la facilité de maintenance.
- Réalisation de simulations/formations liées aux situations d'urgence à intervalles définis et application des enseignements établis afin d'améliorer la performance du système, ainsi que la sensibilisation/les compétences des êtres humains.

Il convient d'analyser les résultats de l'évaluation de la conception centrée sur l'humain de manière à appuyer les recommandations en faveur de modifications de conception, le cas échéant, justifier les principes permettant d'améliorer les performances de l'homme ou mettre en œuvre des solutions de formation.

Le cas échéant, il convient que le flux d'informations de conception centrée sur l'humain soit associé à des programmes de soutien logistique intégré (SLI). Le SLI est une approche rigoureuse permettant d'intégrer des considérations en matière de soutien dans la conception, afin d'obtenir le soutien initial nécessaire pour le système et d'identifier les exigences en matière de soutien du cycle de vie. Le programme de conception centrée sur l'humain fournit les ressources et performances humaines nécessaires pour les exigences et fonctions de soutien logistique. Une coordination rapprochée entre la conception centrée sur l'humain et les programmes SLI permet de réduire les redondances de données et d'augmenter l'efficacité d'utilisation et de partage des informations.

6.6 Amélioration

Cette étape consiste à améliorer la performance du système par l'ajout de fonctionnalités pour satisfaire aux demandes croissantes des utilisateurs concernant le système.

Il convient que le processus de conception centrée sur l'humain intègre les activités suivantes:

- Collecte et analyse des rapports internes afin de générer des mises à jour ou établir des enseignements pour la version suivante du système.
- Amélioration du processus de conception centrée sur l'humain dans le contexte du processus plus large d'ingénierie des systèmes.
- Communication avec les parties prenantes quant aux améliorations proposées.

Le résultat peut consister à appliquer une version réduite du cycle de vie afin de mettre en œuvre l'amélioration.

6.7 Retrait/Démantèlement

Cette étape consiste à mettre fin à l'existence de l'entité système.

Il convient que le processus de conception centrée sur l'humain intègre les activités suivantes:

- Examen des questions liées aux facteurs humains quant à la mise au rebut, au recyclage et à la réutilisation.
- Identification des risques et des problèmes de santé et de sécurité liés à la mise hors service et à la destruction du système.
- Détermination de la manière dont les utilisateurs seront réaffectés, écartés ou transférés vers d'autres activités.
- Planification de la fin des structures sociales.
- Compte rendu et analyse rétrospective pour le système de remplacement.

6.8 Projets de sous-traitance et questions connexes liées à la conception centrée sur l'humain

Il convient d'intégrer les exigences de conception centrée sur l'humain dans les spécifications du système et les documents d'approvisionnement. Cela est essentiel pour que le système puisse atteindre ses objectifs de cohérence de conception et de conformité des performances, notamment en matière d'allocation des fonctions et d'interaction des éléments matériels, logiciels et humains dans la conception et l'exploitation du système.

Actuellement, dans le cadre de projets de développement et d'amélioration de systèmes complexes, il est fréquent de faire appel à des sous-traitants pour assurer le développement des sous-systèmes nécessitant l'intervention d'un opérateur. L'intégration de produits du commerce (COTS) comme fonctions du système présente souvent des avantages en matière de coûts. Les services de soutien d'un système sont souvent utilisés pour la maintenance contractuelle.

Les facteurs de réussite dépendent de la collaboration des acquéreurs et des fournisseurs, des intégrateurs de système et des fournisseurs de service en appliquant un processus de gestion de la chaîne d'approvisionnement et d'assurance qualité. Étant donné que la conception orientée vers l'humain implique des actions pluridisciplinaires, les experts techniques doivent parfois régler des questions d'ordre humain critiques liées aux besoins de sous-traitance et d'approvisionnement.

Il convient que la sous-traitance des projets de conception centrée sur l'humain tienne compte des questions suivantes:

- La conformité au processus de conception centrée sur l'humain défini dans l'ISO 9241-210 et mise à disposition de produits tels que ceux décrits dans l'ISO/CEI TR 25060[4] (contexte de description d'utilisation, compte rendu des besoins de l'utilisateur, spécification des exigences utilisateur, spécification d'interaction de l'utilisateur et d'interface utilisateur, rapports d'évaluation).
- Les exigences d'interface homme-système permettant d'atteindre le niveau d'aptitude de la personne lors de l'exploitation et de la maintenance du système.
- L'optimisation des contraintes économiques relatives à l'usage des ressources humaines, des compétences et des formations disponibles.
- Les implications en matière des effectifs des ressources humaines, de classification des emplois, de niveaux de compétence et d'expérience nécessaires aux projets.
- L'évaluation du compromis d'automatisation de la conception avec l'ergonomie en termes d'applicabilité, d'efficacité et de coûts.
- Les dangers potentiels liés à la sûreté du système et à la santé impliquant les interactions homme-système.
- Les dispositions relatives à l'assurance qualité pour les contrats d'approvisionnement.

---

4 To be published.

- La réintégration de toutes les tâches et tous les projets externalisés dans l'ensemble du modèle pour optimiser le système.

Il convient que l'aptitude humaine à soumettre les produits COTS à essai bénéficie des informations disponibles provenant des fabricants du produit, des dossiers de retours sous garantie, des précédents essais commerciaux et de l'expérience d'utilisation du produit.

Il convient d'identifier les projets de sous-traitance à l'étape de faisabilité/définition du cycle de vie du système. Il convient de bien établir les contrats d'approvisionnement à l'issue de l'étape de conception/développement. Cela permet d'évaluer les sous-traitants, de proposer plusieurs fournisseurs préférentiels et d'évaluer le produit du commerce en vue d'une intégration comme fonctions du système afin de faciliter le processus d'intégration du système.

7 Méthodes de conception centrée sur l'humain

7.1 Classification des activités de conception centrée sur l'humain

Les activités de conception centrée sur l'humain sont classées dans l'ISO/PAS 18152 comme suit:

- HS.1 Activités d'implication du cycle de vie: à chaque étape du cycle de vie du système.

- HS.2 Intégration des activités liées aux facteurs humains: dans la stratégie d'entreprise, le management de la qualité, l'autorisation et le contrôle, la gestion des problèmes homme-système, les données ergonomiques dans la réduction des compromis et des risques, l'implication de l'utilisateur, l'intégration homme-système et le développement et la réutilisation des données ergonomiques.

- HS.3. Activités de conception centrée sur l'humain: contexte d'utilisation, exigences utilisateur, génération de solutions de conception, évaluation de l'utilisation.

- HS.4 Activités liées aux ressources humaines: stratégie de ressources humaines, définition des compétences normalisées et identification des écarts, conception d'une solution de recrutement et d'un plan de livraison, évaluation des solutions liées au système de ressources humaines et obtention d'un retour d'information.

Les méthodes pouvant être appliquées pour prendre en charge ces activités comprennent les suivantes:

a) Méthodes d'analyse de conception centrée sur l'humain

Les méthodes d'analyse de conception centrée sur l'humain permettent de définir les concepts du système, de décrire les scénarios de l'application/de la mission, de déterminer des exigences fonctionnelles et d'attribuer des tâches en fonction de l'allocation appropriée des compétences. Les différentes analyses permettent d'identifier les objectifs liés à la conception centrée sur l'humain, les problèmes de conception critiques et d'autres besoins d'évaluation permettant de satisfaire aux exigences de performance du système impliquant des interactions humaines.

b) Méthodes de conception centrée sur l'humain pour la conception et le développement

Les méthodes de conception centrée sur l'humain pour la conception et le développement permettent d'intégrer tous les critères nécessaires de conception centrée sur l'humain dans la conception d'interfaces homme-système. L'interface homme-système est composée de matériel, de logiciels, de procédures, d'environnements de travail et d'équipements associés aux fonctions système exigeant des interactions humaines. Le processus consiste à convertir

les résultats des activités d'analyse de la conception centrée sur l'humain en critères de conception destinés au développement et à la mise en œuvre du projet ergonomique.

c) Méthodes de conception centrée sur l'humain pour les essais et l'évaluation

Les méthodes de conception centrée sur l'humain pour les essais et l'évaluation permettent de vérifier l'interface homme-système, ainsi que les procédures visant à assurer que le système peut être exploité, maintenu, pris en charge et contrôlé par les utilisateurs dans son environnement d'exploitation prévu. Ces méthodes permettent d'identifier facilement les problèmes critiques de conception centrée sur l'humain dans le cadre de l'exploitation et de la maintenance, afin de résoudre les problèmes et d'améliorer le processus.

L'Annexe C propose un récapitulatif des méthodes pratiques d'analyse de conception centrée sur l'humain, de conception et développement, ainsi que d'essai et d'évaluation.

7.2 Applications des méthodes de conception centrée sur l'humain

Les méthodes de conception centrée sur l'humain destinées aux applications générales d'analyse, d'évaluation et d'estimation reposent sur des techniques d'ingénierie des systèmes. Il convient de les utiliser avec d'autres méthodes d'ingénierie et disciplines techniques dans la conception et la mise en œuvre du système. Les méthodes ergonomiques figurant dans l'Annexe C participent aux meilleures pratiques de conception centrée sur l'humain présentées dans le Tableau C.1.

Annexe A
(informative)

Exemples de méthodes AFH

Il existe une distinction entre les méthodes AFH de première et de deuxième générations.

Les méthodes de première génération traitent les défaillances humaines comme des défaillances matérielles, l'élément de sortie issu des tâches humaines remplaçant les éléments de sortie générés par l'équipement. Les actions humaines sont considérées de manière binaire, c'est-à-dire en termes de réussite ou d'échec à obtenir le résultat requis à la suite de la réalisation d'une tâche. Les tâches et sous-tâches sont supposées faire l'objet d'une probabilité de défaillance inhérente, modifiée ensuite par les facteurs de performance reposant sur l'évaluation de l'environnement ergonomique. Les méthodes diffèrent dans la manière dont elles permettent d'estimer les probabilités d'erreur humaine (PEH) fondamentales et intègrent les facteurs de performance (FP).

Les procédures AFH de deuxième génération modélisent et évaluent le rôle du contexte et le comportement de prise de décision de l'être humain qui peuvent avoir des effets néfastes sur le système.

Le Tableau A.1 fournit une description des différentes méthodes ainsi que leurs applications.

Tableau A.1 – Méthodes AFH et leurs applications

Méthode et brève description	Niveau d'utilisation
ASEP – Accident Sequence Evaluation Program: version simplifiée du THERP pour des évaluations préalables (avec estimations prudentes) Les tâches critiques sont divisées en sous-tâches représentées sur un arbre d'événements de performances de l'être humain. Les PEH correspondant aux sous-tâches sont obtenues à partir de tableaux publiés dans le NUREG/CR-4772 (Commission réglementaire américaine de 1987). Des lignes directrices sont également données pour tenir compte des facteurs de performance dans les PEH. Décomposition normalisée de l'action: actions critiques et diagnostic des perturbations, le cas échéant. Recommandations globales en faveur d'une PEH par action critique. Jugement détaillé des interfaces homme-machine non requis. Diagnostic PEH temporel, les courbes données reposent sur un consensus d'experts. Permet une rapide sélection préalable des tâches importantes.	L'ASEP est utilisé en cas de nécessité d'estimation quantitative rapide mais pas nécessairement précise (sélection). C'est le cas des états à faible puissance et à l'arrêt de centrales nucléaires, par exemple, où le nombre d'actions d'évaluation est important et nécessite de recourir à une méthode qui permet de gagner du temps. L'ASEP est une méthode AFH de première génération, permettant d'évaluer les problèmes ergonomiques dans l'environnement de travail.

Méthode et brève description	Niveau d'utilisation
ATHEANA – A Technique for Human Error Analysis: une analyse approfondie du contexte et de la prise de décision fournit à l'analyste système des informations détaillées sur le potentiel de prise de décisions erronées de l'être humain. La méthode permet d'identifier les événements de défaillance humaine (EDH) en s'appuyant sur des scénarios d'accident. Les EDH se caractérisent par des actions dangereuses, c'est-à-dire des actions (ou des omissions) se traduisant par une diminution de la performance de l'installation et par un contexte de forçage d'erreur (CFE). Le CFE comporte des conditions liées aux facteurs de performance et à l'installation qui rendent les erreurs humaines possibles. L'EDH est quantifié en combinant les probabilités de CFE, la probabilité de réaliser une action dangereuse dans le CFE et la probabilité d'un CFE, compte tenu de l'action dangereuse et des éléments de preuve supplémentaires qui en résultent. Les estimations quantitatives reposent sur une expertise analogue à l'approche SLIM.	ATHEANA est utilisée dans un certain nombre d'études, en particulier dans le domaine nucléaire. ATHEANA est une méthode AFH de deuxième génération, permettant de procéder à une analyse qualitative approfondie de l'influence du contexte sur le comportement humain et la prise de décision. Elle peut être utilisée pour analyser l'erreur qui fait suite à l'incident, en cas de conditions de forçage d'erreur de l'incident.
CAHR – Connectionism Assessment of Human Reliability: la méthode requiert des événements opérationnels ou d'autres données comportementales permettant de procéder à son évaluation. Elle est composée: (1) d'un cadre structuré de collecte des données, (2) d'une méthode d'analyse qualitative des données collectées et (3) d'une méthode d'évaluation de la fiabilité humaine. Pour l'évaluation, la méthode distingue la tâche et le contexte dans lequel la tâche doit être réalisée, la demande cognitive que la tâche et le contexte exigent de l'être humain, les mécanismes de compensation humaine et le comportement qui en résulte.	La méthode CAHR peut être utilisée pour évaluer les problèmes ergonomiques classiques ou les relations réciproques qu'entretiennent plusieurs conditions et facteurs. L'éventail des applications s'étend du nucléaire, de l'automobile, de l'aéronautique, de la gestion du trafic aérien au domaine maritime. CAHR est une méthode AFH de deuxième génération, permettant de procéder à une analyse qualitative rapide et approfondie de l'influence du contexte sur le comportement humain et la prise de décision.

Méthode et brève description	Niveau d'utilisation
CREAM – Cognitive Reliability and Error Analysis Method: Le mode de contrôle humain applicable au scénario est sélectionné à partir de 4 «modes de contrôle contextuels» (la fiabilité humaine est supposée augmenter à mesure de l'augmentation du niveau de contrôle). Le contexte de la tâche ou du scénario est décrit à l'aide de 9 conditions de performance communes (ou CPC) de CREAM. (Les CPC sont analogues aux facteurs de performance). Les erreurs potentielles sont identifiées et classées en un certain nombre de groupes décrivant les modes et les causes de l'erreur. Pour l'évaluation, CREAM utilise des tableaux analogues à THERP, mais uniquement après avoir procédé à l'analyse des modes de contrôle contextuels essentiels.	CREAM est largement utilisée pour évaluer rapidement l'influence du contexte sur l'aptitude à la fonction de l'être humain et donne un aperçu du niveau d'une technique de sélection. CREAM est une méthode AFH de deuxième génération, permettant de procéder à une analyse qualitative de l'influence du contexte sur le comportement humain, la prise de décision et une quantification ordinaire.
ESAT – Expertensystem zur Aufgaben-Taxonomie (Expert system for task taxonomy): Quantification des tâches discrétionnaires liée à un facteur de performance. Détermination du niveau de fiabilité (sur une échelle de 1 à 10) par évaluation («appréciations») des facteurs de performance donnés. Le rapport fonctionnel entre la PEH et le niveau de fiabilité est déterminé d'une part par des expertises (en fonction des connaissances génériques sur les performances au travail de l'être humain) et d'autre part par mesure des performances au travail. Méthode appliquée pour la conception de cockpits d'avion	La méthode ESAT est issue de l'aviation et est toujours utilisée occasionnellement dans d'autres secteurs de l'industrie, pour l'évaluation des erreurs humaines en production. L'ESAT est une méthode AFH de première génération, permettant d'évaluer les problèmes ergonomiques dans l'environnement de travail.
AMDE/AMDEC – L'Analyse des Modes De Défaillance et de leurs effets permet d'identifier les modes de défaillance (c'est-à-dire ce qui n'est pas réalisé correctement) ainsi que les mécanismes de défaillance (les raisons d'une mauvaise réalisation ou les mécanismes psychologiques d'erreur) et leurs effets. A l'instar des équipements, les modes d'erreurs de probabilités AMDE peuvent être estimés, la criticité des erreurs pouvant être évaluée en tenant compte de leur probabilité d'occurrence et de l'amplitude de leurs effets	Les méthodes AMDE et AMDEC sont couramment utilisées pour déterminer la fiabilité des équipements. Elles sont ensuite utilisées comme des outils qualitatifs ou quantitatifs pour évaluer la fiabilité humaine. Pour de plus amples informations, voir la CEI 60812.

Méthode et brève description	Niveau d'utilisation
HCR/ORE (Human Cognitive Reliability / Operator Reliability Experiments): Les méthodes HCR établissent que la réussite ou l'échec d'un opérateur dépend de la durée disponible pour réaliser l'action. La PEH est la fraction de temps qui dépasse la durée disponible et nécessaire pour le diagnostic et la réponse. La méthode HCR/ORE a été développée sur la base des expériences de fiabilité de l'opérateur (ORE). Les tâches décrites dans les procédures font la distinction entre les défaillances de diagnostic qui sont liées à la durée et celles qui ne le sont pas. Six courbes de temps PEH sont disponibles (en fonction du type de réacteur et de la dynamique de la défaillance). Elles sont normalisées en fonction des exigences de durée moyenne (médiane). Quantification PEH liée au facteur de performance des défaillances qui ne sont pas liées à la durée en tenant compte de 8 mécanismes d'erreur donnés. Des lignes directrices pour une modélisation de facteur de performance reposant sur un type d'arbre de décision sont également données. Pour les tâches qui ne sont pas représentées dans les procédures, une méthode rapide d'évaluation de la PEH est proposée.	L'approche a été développée car il a été démontré que la méthode HCR initiale (modèle de fiabilité cognitive humaine), qui faisait la distinction entre les comportements reposant sur les compétences, les règles et les connaissances, n'était pas une approche valide pour déterminer la fiabilité humaine. La méthode HCR/ORE nécessite de procéder à des expériences de simulation avant de fournir des évaluations valides. Compte tenu des efforts liés à cette exigence, l'utilisation de cette méthode est limitée à certaines actions réalisées dans des salles de contrôle nucléaires. La méthode HCR/ORE est une méthode AFH de première génération, permettant d'évaluer les performances d'une tâche en fonction du temps disponible. Les problèmes ergonomiques sont résolus de manière limitée.
HEART/CARA – Human Error Assessment and Reduction Technique: destinée aux tâches génériques basées sur le système (mise en exploitation du système X, par exemple) plutôt qu'aux tâches élémentaires (manipulation du commutateur X, par exemple). Une valeur nominale de la PEH est choisie en comparant la tâche à une liste de 8 tâches définies de manière générique pour lesquelles des PEH sont définies. La PEH est alors modifiée par appréciation des facteurs de performance sélectionnés dans une liste de 38 facteurs de performance. La méthode a été développée en types de tâches génériques dans le domaine de la gestion du trafic aérien sous le nom de CARA	Peut être aisément et rapidement gérée. La plupart des caractéristiques des facteurs de performance reposent sur des études empiriques. Inconvénient: l'étalonnage du modèle est insuffisant. La technique ne permet donc pas d'estimer la fiabilité des actions humaines en cas de besoin d'une évaluation très précise ou d'une fiabilité élevée (des actions donnant immédiatement lieu à des effets néfastes dans le système, par exemple). La méthode HEART et celles qui lui ont succédé sont des méthodes AFH de première génération. Elles permettent d'évaluer les performances d'une tâche en réalisant une sélection plus détaillée plutôt qu'une évaluation approfondie.

Méthode et brève description	Niveau d'utilisation
MERMOS – Méthode d'Evaluation de la Réalisation des Missions Opérateur pour la Sûreté (Method for the Evaluation of the Realization of an Operator's Mission regarding Safety). La méthode MERMOS proscrit le terme «erreur humaine». Elle est composée de missions (ensemble des tâches à réaliser), les êtres humains établissant les mécanismes de coordination de la mission et des résultats probables qu'implique ce type de coordination. Plusieurs voies de défaillance, se traduisant par un échec de la mission, sont identifiées à l'aide d'un processus structuré autour d'une stratégie, d'une action et d'un diagnostic. Des probabilités sont attribuées par expertise aux éléments de la voie. Les données sont issues de l'expérience opérationnelle et des observations du simulateur.	MERMOS est exclusivement utilisée dans l'industrie française du nucléaire; elle a fait l'objet d'un certain nombre de validations et a obtenu une acceptation réglementaire. MERMOS est une méthode AFH de deuxième génération, permettant de procéder à une analyse qualitative approfondie de l'influence du contexte sur le comportement humain et la prise de décision.
SHERPA – Systematic Human Error Reduction and Prediction Approach. Commence par une analyse des tâches et classe les sous-tâches de niveau inférieur par type (action, extraction, vérification, sélection, communication). Détermine les modes d'erreur plausibles des sous-tâches à l'aide de la liste de contrôle SHERPA des modes d'erreur. Les conséquences sont présentées, et la possibilité de reprise au niveau d'une tâche ultérieure est notée. La probabilité et la criticité de chaque erreur de chaque sous-tâche sont données dans l'ordre ordinal (élevée, moyenne, basse).	Méthode de première génération offrant un moyen complet et structuré d'identification des erreurs dans la réalisation de tâches particulières et de les classer du point de vue qualitatif en fonction de leur importance. Utilisée pour rechercher des stratégies de réduction des erreurs. N'intègre pas les erreurs système ou organisationnelles.

Méthode et brève description	Niveau d'utilisation
SLIM – Success Likelihood Index Methodology: Les experts identifient les facteurs de performance pertinents (la complexité d'une tâche, par exemple) et fixent des points limites sur une échelle allant de 1 à 9 (par exemple, 1 = simple et 9 = complexe). Le point désigné sur chaque échelle auquel des performances idéales sont affectées est enregistré et utilisé pour remettre à l'échelle les appréciations par rapport à la valeur idéale. Chaque tâche est appréciée selon chaque facteur de performance de ces échelles. Un indice de probabilité de succès (IPS) est calculé sur la base d'une somme globale d'appréciations de facteurs de performance pondérées, puis est transformé en échelle de probabilité en appliquant au moins 2 PEH de référence. Condition préalable: des PEH de référence éprouvées et des facteurs de performance pertinents sont disponibles, ces derniers pouvant être clairement évalués. La détermination des PEH de référence est problématique et prédétermine les résultats qu'il est possible d'obtenir.	SLIM est utilisée si une méthode souple est nécessaire et qu'aucune donnée particulière n'est disponible. De même, les interdépendances entre facteurs de performance ne sont pas prises en compte. Par conséquent, la méthode ne peut générer des résultats qu'au niveau de qualité d'une sélection. La méthode SLIM est une méthode AFH de première génération. Elle permet d'évaluer les performances d'une tâche en réalisant une sélection plus détaillée plutôt qu'une évaluation approfondie.
SPAR-H – Standardized Plant Analysis Risk (SPAR) AFH: composée d'un processus en deux étapes visant à identifier les probabilités d'erreur humaine nominales (PEH), puis à modifier ces PEH sur la base de facteurs de performance de niveau général et d'une dépendance. De manière plus significative pour cette méthode, les analystes renseignent une fiche technique relativement simple, qui est ensuite utilisée pour estimer les facteurs de performance et la PEH considérée. La méthode SPAR-H comporte des limites de modélisation et d'analyse inhérentes qu'il convient de clairement appréhender.	La méthode SPAR-H fait partie d'un ensemble de méthodes de sélection. Il convient de ne pas nécessairement la préférer à d'autres approches plus sophistiquées et détaillées (la méthode ATHEANA, par exemple), dans des situations nécessitant une analyse détaillée des aspects liés aux performances humaines d'un événement. La méthode SPAR-H permet de résoudre, de manière limitée, les problèmes AFH de première et deuxième génération au niveau de la sélection.

Méthode et brève description	Niveau d'utilisation
THERP – Technique for Human Error Rate Prediction: méthode normalisée de détermination de la fiabilité humaine concernant les problèmes ergonomiques. Décomposition approfondie des tâches en éléments à l'aide de la taxinomie THERP, erreurs liées aux éléments représentés sous forme d'arbre d'événements. PEH nominale attribuée à chaque élément de tâche en sélectionnant des PEH «appropriées» dans une base de données contenant environ 100 facteurs. PEH nominale modifiée par un multiplicateur de facteurs de performance, le cas échéant. La dépendance entre les erreurs des éléments de tâches est modélisée. Les courbes de probabilité qu'un être humain réponde à une perturbation dans un temps donné reposent sur un consensus d'experts.	La méthode THERP est utilisée si une évaluation approfondie des tâches est nécessaire et si la sûreté de fonctionnement de l'ensemble du système repose sur des actions critiques. La prise de décision et l'influence d'un large éventail de facteurs contextuels ne peuvent pas être évaluées. THERP est une méthode AFH de première génération. Elle permet d'évaluer de manière approfondie les performances d'une tâche et de fournir des exigences détaillées en matière d'ergonomie pour concevoir le système. Elle n'est pas adaptée à l'évaluation de la prise de décision, ni à la prise en compte suffisante de la plage de conditions contextuelles.

Annexe B
(informative)

Récapitulatif des activités de conception orientée vers l'humain et de leur impact sur la sûreté de fonctionnement du système

B.1 Présentation

La présente annexe donne quelques exemples d'activités de conception centrée sur l'humain permettant d'améliorer la sûreté de fonctionnement du système, si elles sont correctement utilisées.

B.2 Automatisation

Tableau B.1 – Automatisation

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Donne des informations relatives à l'automatisation, l'état de fonctionnement et autre retour d'information à l'utilisateur du système. • Facilite l'utilisation des fonctionnalités. • Assure une exploitation en toute sécurité en fonction de la capacité et des compétences de l'utilisateur. • Alerte l'utilisateur d'une défaillance ou d'une dégradation de l'automatisation, et de modes de fonctionnement potentiellement dangereux. • Indique les fonctionnalités résistantes et tolérantes aux erreurs afin de prévenir tout accès non autorisé ou accidentel, et dont l'utilisation n'est pas nécessairement difficile. • Fournit les moyens de procéder à une annulation manuelle (avec des protecteurs).	• Amélioration de la disponibilité des fonctions du système. • Amélioration des performances du système grâce aux fonctions automatisées. • Permettre aux utilisateurs de réaliser les tâches requises en évitant l'augmentation des demandes cognitives, les charges de travail importantes, l'interruption ou l'inattention de l'utilisateur. • Simplification des besoins de formation de l'utilisateur et des exigences liées aux applications système. • Limitation des erreurs et des risques découlant d'une erreur.

B.3 Conception de la maintenabilité

Tableau B.2 – Conception de la maintenabilité

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Intègre une redondance lorsque cela est justifié et rentable pour limiter les cas de maintenance non planifiée. • Permet en termes de modularité, de concevoir des unités plus petites remplaçables et des ensembles jetables. • Incorpore des capacités d'essai intégrées et des caractéristiques de télédiagnostic et d'autodiagnostic. • Intègre un accès rapide et facile à tous les éléments d'installation devant faire l'objet d'opérations de maintenance dans le cadre de l'inspection, de la dépose et du remplacement. • Limite le nombre et les types d'outils et d'équipements d'essai nécessaires à la maintenance. • Intègre des caractéristiques de réparation et de réglage automatiques, dans la mesure du possible.	• Maintenabilité améliorée • Fiabilité améliorée. • Simplification des fonctions de maintenance • Amélioration de la testabilité, des diagnostics et de l'identification des pannes. • Exigences limitées en matière de durée de maintenance et de ressources de soutien logistique

B.4 Interface homme-ordinateur

Ces activités reposent sur l'ISO 9241-110. Pour de plus amples informations sur la conception de l'interface utilisateur, voir l'ISO 9241, Parties 2, 12, 13, 14, 15, 16, 17, 20, 151 et 171.

Tableau B.3 – Interface homme-ordinateur

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Adapter le système interactif à la tâche de manière à aider l'utilisateur à réaliser celle-ci. • Rendre les boîtes de dialogue interactives auto-descriptives, de sorte que les utilisateurs puissent savoir exactement dans quelle boîte de dialogue ils se trouvent, où ils se trouvent à l'intérieur de la boîte de dialogue, les actions qu'ils peuvent réaliser et la manière dont ils peuvent les réaliser. • Adapter les boîtes de dialogue interactives aux attentes de l'utilisateur, de sorte qu'elles répondent à ses besoins contextuels prévisibles et aux conventions communément acceptées. • Adapter les boîtes de dialogue interactives à l'apprentissage, de sorte qu'elles aident et guident l'utilisateur tout au long de son apprentissage du système. • Rendre les boîtes de dialogue interactives contrôlables, de sorte que l'utilisateur puisse lancer et contrôler l'orientation et l'allure de l'interaction. • Rendre les boîtes de dialogue interactives tolérantes aux erreurs, de sorte que, malgré la présence d'erreurs d'entrée manifestes, il soit possible d'obtenir le résultat prévu avec peu, voire pas, d'action corrective de la part de l'utilisateur. • Rendre les boîtes de dialogue interactives capables d'individualisation, de sorte que les utilisateurs puissent modifier l'interaction et la présentation des informations en fonction de leurs aptitudes et besoins individuels.	• Facilité et aptitude à l'emploi du système améliorées. • Augmentation de la vitesse de fonctionnement du système. • Réduction du nombre d'erreurs.

B.5 Incorporation des fonctions d'affichage, de contrôle et d'alarme

Pour de plus amples informations sur l'affichage et les commandes, voir l'ISO 9241, Parties 300, 302, 303, 304, 305, 306, 307, 308, 309 et 920.

Tableau B.4 – Incorporation des fonctions d'affichage, de commande et d'alarme

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Faire en sorte que l'affichage et les commandes soient lisibles, identifiables et visibles, quelles que soient les conditions. • Placer les commandes de manière cohérente en les regroupant et en les disposant pour que l'utilisateur puisse y accéder aisément. • Concevoir le déplacement et le sens de la commande de manière cohérente. • Concevoir les commandes en fonction d'opérations séquentielles afin de suivre un modèle fixe. • Concevoir les commandes de maintenance et d'ajustement à protéger afin d'éviter toute activation accidentelle. • Concevoir le codage des commandes à distinguer, avec une application uniforme du code dans tout le système. • Simplifier le codage de l'entrée et identifier l'erreur afin d'entrer de nouveau les codes. • Concevoir les fonctions d'alarme de manière visible et audible. • Concevoir les fonctions d'alarme de manière à fournir une indication claire et sans ambiguïté de la cause de l'alerte, et informer l'utilisateur de la priorité et de la nature du problème, et des réponses possibles. • Intégrer une validation d'entrée d'alarme afin d'éviter les fausses alarmes. • Prévoir des systèmes de communication vocale, si cela est essentiel, et pouvant être utilisés en cas d'alarme et de situation d'urgence	• Maintenabilité améliorée. • Testabilité améliorée. • Tâches d'exploitation et de maintenance du système améliorées. • Nombre de fausses alarmes réduit. • Sûreté et sécurité des performances du système améliorées. • Simplification des besoins de formation de l'utilisateur et des exigences en matière de compétences.

B.6 Incorporation de dispositifs d'entrée

Pour de plus amples informations sur la conception des dispositifs d'entrée, voir l'ISO 9241, Parties 4, 9, 400, 410 et 920.

Tableau B.5 – Incorporation de dispositifs d'entrée

Activité de conception ergonomique	Impact sur la sûreté de fonctionnement du système
• Conception de la saisie manuelle et des touches à fonction fixe. • Conception de dispositifs de pointage (souris, joystick et boule de commande, crayon optique). • Conception de dispositifs autres que les dispositifs de pointage (dispositifs interactifs tactiles et écrans tactiles, commandes vocales). • Interchangeabilité des dispositifs d'entrée	• Accessibilité améliorée. • Exploitabilité améliorée. • Utilisabilité améliorée.

B.7 Environnement

Pour de plus amples informations sur l'environnement de travail, voir l'ISO 9241-6.

Tableau B.6 – Environnement

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Conceptions modulaires des plus petites unités remplaçables. • Contrôle par l'utilisateur de l'environnement de travail (ventilation, éclairage, température, humidité, bruit).	• Maintenabilité améliorée • Performances humaines améliorées et satisfaction sur le lieu de travail

B.8 Sécurité

Tableau B.7 – Sécurité

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Sécurité du lieu de travail en matière d'accessibilité et d'exploitation. • Sécurité de l'équipement en regard de son utilisation par l'opérateur. • Conceptions permettant d'éviter les dangers. • Analyse de fiabilité humaine.	• Performances humaines améliorées dans un environnement sûr. • Atténuation des risques de dégradation de la performance du système. • Statistiques sur les performances humaines.

B.9 Sûreté

Tableau B.8 – Sûreté

Activité de conception centrée sur l'humain	Impact sur la sûreté de fonctionnement du système
• Sûreté du système et accès autorisé. • Sauvegardes de sûreté et mesures et commandes de protection. • Sûreté physique. • Sûreté des informations.	• Intégrité améliorée de l'aptitude à la fonction du système. • Réduction des risques.

Annexe C
(informative)

Meilleures pratiques liées à la conception centrée sur l'humain

La présente annexe répertorie les activités les plus importantes de l'ISO/PAS 18152 correspondant à chaque étape du cycle de vie (avec leurs numéros de référence) et donne des exemples de méthodes et techniques qui peuvent être utilisées pour les mettre en œuvre.

Tableau C.1 – Exemples de méthodes et techniques contribuant aux meilleures pratiques

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
1.1 Concept	Identifier le contexte prévu d'utilisation des systèmes (besoins, tendances et attentes à venir) (1.1-1) Analyser le concept du système pour clarifier les objectifs, leur viabilité et leurs risques (1.1-2)	– Atelier du futur – Visite préliminaire sur le site – Groupes de discussion – Enquêtes photographique – Simulations d'environnements de travail ultérieur – Analyse approfondie du travail et des modes de vie
	Décrire les objectifs que l'utilisateur ou l'organisme utilisateur souhaite atteindre à l'aide du système (1.1-3)	– Ateliers participatifs – Études sur le terrain et ethnographie – Consultation des parties prenantes – Analyse ergonomique
	Définir la portée du contexte d'utilisation du système (3.1-1)	– Contexte de l'analyse des modes d'utilisation
1.2 Planification a) Généralités	Développer un plan permettant d'obtenir et de conserver l'aptitude à utiliser le système tout au long du cycle de vie du système (2.4-1) Identifier les compétences requises et prévoir les moyens de les fournir (2.4-2)	– Plan permettant d'obtenir et de conserver l'aptitude à utiliser le système – Plan d'utilisation des données IHS afin de limiter les risques
b) Implication de l'utilisateur	Identifier les problèmes homme-système et les aspects du système nécessitant une saisie par l'utilisateur (2.6-1) Définir une stratégie et un plan d'implication de l'utilisateur (2.6-3) Sélectionner et utiliser la méthode la plus efficace pour obtenir une saisie par l'utilisateur (2.6-4) Personnaliser les outils et méthodes pour les projets/étapes particuliers, si nécessaire (2.7-4)	– Identifier les problèmes IHS et les aspects du système nécessitant une saisie par l'utilisateur – Elaborer un plan d'implication de l'utilisateur – Sélectionner et utiliser les méthodes les plus efficaces – Personnaliser les outils et les méthodes, si nécessaire
c) Risques	Évaluer les risques pour la santé et le bien-être des utilisateurs du système (1.2-6) Évaluer les risques qu'encourent la communauté et l'environnement à la suite d'une erreur humaine dans l'utilisation du système (1.2-7) Évaluer la gravité des menaces émergentes sur l'aptitude à l'utilisation du système et les autres risques homme-système et l'efficacité des mesures d'atténuation (2.5-3) Évaluer les risques liés à la non-implication des utilisateurs finaux dans chaque évaluation (2.6-2)	– Analyse des risques (processus et produit) – Analyse des risques liés au programme IHS

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
	Planifier et gérer l'utilisation des données ergonomiques afin d'atténuer les risques liés aux problèmes homme-système (2.5-1) Évaluer la gravité des menaces émergentes sur l'aptitude à l'utilisation du système et les autres risques homme-système et l'efficacité des mesures d'atténuation (2.5-3) Prendre des mesures d'atténuation efficaces pour résoudre les risques vis-à-vis de l'aptitude du système à être utilisé (2.5-4)	
1.3 Compréhension des besoins a) Contexte d'utilisation	Identifier et analyser les rôles de chaque groupe de parties prenantes susceptible d'être affecté par le système (1.1-4) Décrire les caractéristiques des utilisateurs (3.1-3) Décrire le régime culturel/environnemental/ organisationnel/opérationnel (3.1-4) Décrire les caractéristiques des équipements extérieurs au système et à l'environnement de travail (3.1-5) Décrire l'emplacement, les équipements de travail et les conditions ambiantes (3.1-6) Décider des objectifs, des comportements et des tâches de l'organisation qui influencent les ressources humaines (4.1-1) Présenter les options et contraintes liées au contexte et aux ressources humaines aux parties prenantes du projet (1.1-6)	– Identification réussie des parties prenantes critiques – Études sur le terrain et ethnographie – Atelier participatif – Analyse du contexte de travail – Contexte de l'analyse des modes d'utilisation – Analyse des données d'événement – Enquête contextuelle – Diagramme de visibilité – Enveloppe de portée
b) Tâches	Analyser les tâches et le système en action (3.1-2)	– Analyse des tâches – Analyse cognitive des tâches – Analyse du contexte de travail – Analyse de l'application/de la mission – Organigramme fonctionnel – Diagramme séquentiel opérationnel – Diagramme de flux – Diagramme de décision/ d'action – Exigences en matière d'action / informations – Délai – Définition intégrée de fabrication assistée par ordinateur – Analyse de la charge de travail – Analyse de la conscience circonstancielle – Analyse de liens – Analyse de fiabilité des performances humaines
c) Besoins en matière d'aptitude à l'utilisation du système	Procéder à une recherche de l'aptitude à l'utilisation requise pour le système (1.1-5)	– Rechercher l'aptitude à l'utilisation requise pour le système – Référence en matière d'aptitude à l'utilisation du système – Évaluation heuristique/ d'expert – Temps de référence prédéterminés

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
d) Options de conception	Générer des options de conception pour chaque aspect du système lié à son utilisation et à son effet sur les parties prenantes (1.2-1) Produire des solutions centrées sur l'utilisateur pour chaque option de conception (1.2-2)	– Évaluation anticipée du prototype et de l'aptitude à l'utilisation du système – Développer des simulations – Conception parallèle (essais en équipes)
1.4 Exigences a) Exigences du contexte	Analyser les implications du contexte d'utilisation (3.1-7)	– Définir le contexte d'utilisation prévu, y compris ses limites
b) Exigences en matière d'infrastructure	Identifier, spécifier et générer l'infrastructure du système (1.3-2) Etablir les compétences requises dans le cadre de programmes de formation et de sensibilisation (1.3-4) Définir le nombre, les compétences et les équipements de soutien généraux nécessaires à la réalisation de ces tâches (4.1-2)	– Identifier les exigences en matière de recrutement et la formation ou le soutien permettant de garantir les performances acceptables des utilisateurs
c) Exigences utilisateur	Elaborer un état explicite des exigences utilisateur pour le système (3.2-2) Générer et convenir des critères de mesure pour le système dans le cadre de son contexte d'utilisation prévu (3.2-4)	– Scénarios – Personnes – Scénarios illustrés – Établir les objectifs de performance et de satisfaction de scénarios d'utilisation spécifiques – Définir les exigences détaillées en matière d'interface utilisateur – Hiérarchiser les exigences
1.5 Exigences en matière d'analyse	Évaluer dans quelle mesure la conception proposée est susceptible de respecter les critères d'aptitude à l'utilisation du système et les autres exigences HS (2.5-2) Analyser les exigences utilisateur (3.2-3) Présenter ces exigences aux parties prenantes du projet pour qu'elles les utilisent dans le développement et l'exploitation du système (3.2-5) Identifier tous les écarts de recrutement et communiquer les exigences pour concevoir des solutions de recrutement (4.2-6)	– Identifier et analyser les exigences critiques de réussite imposées par les parties prenantes – Spécification commune de l'industrie pour les exigences en matière d'aptitude à l'utilisation du système – Évaluation de l'environnement /organisation

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
2. Conception/développement a) Généralités	Générer des options de conception pour chaque aspect du système lié à son utilisation et à son effet sur les parties prenantes (1.2-1) Produire des solutions centrées sur l'utilisateur pour chaque option de conception (1.2-2) Conception permettant de personnaliser et de prendre en charge les besoins spécifiques du marché et de l'utilisateur (1.2-3) Répartir les fonctions entre l'être humain, la machine et les éléments organisationnels du système les mieux adaptés à la réalisation de chaque fonction (3.3-1) Développer un modèle de travail utilisateur à partir des exigences, du contexte d'utilisation, de l'allocation de fonction et des contraintes de conception du système (3.3-2) Générer des conceptions pour les éléments liés à l'utilisateur du système tenant compte des exigences utilisateur, du contexte d'utilisation et des données ergonomiques (3.3-3) Décrire la manière dont le système sera utilisé afin de prendre en charge l'intégration des composants du système (3.3-4)	– Allocation de fonction – Générer des options de conception – Ergonomie physique – Conception participative – Lignes directrices et normes de l'interface utilisateur
b) Prototype et évaluation	Développer une simulation ou une mise en œuvre d'essais des aspects essentiels du système pour procéder à des essais avec les utilisateurs (1.2-4)	– Évaluation du prototype et de l'aptitude à l'utilisation du système – Développer des prototypes – Développer des simulations – Dessin – Maquette – Modèle réduit – Mannequin – Environnement CAO – Évaluation technique, manuelle et fonctionnelle – Utilisation de données d'ingénierie ergonomique pour évaluation

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
c) Ressources humaines	Décider des objectifs et des tâches de l'organisation qui influencent les ressources humaines (4.1-1) Définir le nombre, les compétences et les équipements de soutien généraux nécessaires à la réalisation de ces tâches (4.1-2) Identifier l'attribution des tâches/obligations en cours (4.2-1) Analyser l'écart entre la disposition existante et la disposition future (4.2-3) Identifier les exigences en matière de compétence pour chaque rôle (4.2-3) Prévoir les changements de personnel entre le présent et le futur (4.2-4) Déterminer le personnel disponible, en tenant compte des heures de travail, de l'effort réalisable et du facteur de non-disponibilité (4.2-5) Identifier et allouer les fonctions à exécuter (4.3-1) Préciser et concevoir les tâches et les compétences requises à assurer (4.3-2) Calculer le nombre de personnes requis (4.3-3) Générer des options chiffrées de formation et/ou redéploiement (4.3-4) Élaborer des options et des contraintes dans le cadre d'un plan optimal de mise en œuvre de formation (4.3.5) Développer et soumettre à essai la solution de formation pour les utilisateurs représentatifs (4.3-6) Définir la manière dont les utilisateurs seront réaffectés, écartés ou transférés vers d'autres activités (1.5-3)	– Analyse du domaine de travail – Analyse des tâches – Conception participative – Évaluation de la charge de travail – Modèle de performance humaine – Conception intégrant la vigilance – Prévoir le recrutement
3. Réalisation/mise en œuvre	Maintenir le contact avec les utilisateurs et l'organisme client tout au long de la définition, du développement et de l'introduction d'un système (1.3-3) Élaborer les options et les contraintes dans le cadre d'une stratégie de mise en œuvre couvrant les questions liées à la technique, à l'intégration, à la planification et au recrutement (1.3-1) Revoir les caractéristiques de conception et de sécurité à l'aide du retour d'information à l'issue des évaluations (3.3-5) Proposer des solutions de formation définitives au personnel désigné en fonction d'un calendrier convenu (4.3-7) Collecter des informations utilisateur relatives à l'aptitude à l'utilisation du système de développement (1.2-5) Vérifier que le système satisfait aux exigences des utilisateurs, aux tâches et à l'environnement, comme indiqué dans sa spécification (1.3-5) Vérifier que le système est conforme aux connaissances applicables en matière de sciences humaines, aux usages, aux normes, aux lignes directrices, aux réglementations et à la législation (1.4-3)	– Analyse des risques (processus et produit) – Retour d'information de l'utilisateur sur l'aptitude à l'utilisation du système et l'expérience de l'utilisateur – Utiliser les modèles et la simulation – Lignes directrices: format commun a l'industrie pour les rapports d'aptitude à l'utilisation du système – Mesure des performances – Liste de contrôle des critères de conception

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
4. Opérations	Générer une stratégie de personnel (1.4-1) Vérifier que le système est conforme aux connaissances applicables en matière de sciences humaines, aux usages, aux normes, aux lignes directrices, aux réglementations et à la législation (1.4-3) Proposer une formation et d'autres formes de sensibilisation aux utilisateurs et au personnel administratif (1.4-2) Evaluer les risques pour la santé et le bien-être des utilisateurs du système (1.4-5) Examiner les risques qu'encourent la communauté et l'environnement à la suite d'une erreur humaine dans l'utilisation du système (1.4-6) Procéder à une recherche visant à affiner et consolider l'opération et la stratégie de soutien du système (1.4-8)	– Analyse du contexte de travail – Analyse du contexte organisationnel et environnemental
5. Amélioration	Donner les moyens d'un retour d'information de l'utilisateur (sur les questions humaines) (4.4-2) Analyser le retour d'information sur le système lors de la livraison et informer l'organisation des questions émergeantes (1.3-6) Evaluer les effets de la modification sur l'aptitude à l'utilisation du système (1.4-4) Prendre des mesures pour les problèmes découlant de l'évaluation en service (1.4-7) Prendre des mesures d'atténuation efficaces pour résoudre les risques liés à l'aptitude à l'utilisation du système	– Analyse du contexte organisationnel et environnemental – Analyse des risques – Retour d'information de l'utilisateur sur l'aptitude à l'utilisation du système et l'expérience de l'utilisateur – Analyse du contexte de travail – Observation directe continue – Observation directe échantillonnée – Entretiens et questionnaires
6. Retrait	Collecter et analyser des rapports internes afin de générer des mises à jour ou établir des enseignements pour la version suivante du système (1.5-1) Identifier les risques et les problèmes de santé et de sécurité liés à la mise hors service et à la destruction du système (1.5-2) Définir la manière dont les utilisateurs seront réaffectés, écartés ou transférés vers d'autres activités (1.5-3) Planifier la décomposition des structures sociales (1.5-4) Compte rendu et analyse rétrospective pour le système de remplacement (1.5-5)	
7. Sous-traitance	Tenir compte des problèmes des parties prenantes et de l'utilisateur dans les activités d'acquisition (2.3-1)	– Format commun de l'industrie

Etape du cycle de vie	Meilleures pratiques issues de l'ISO 18152 (numéro de référence de l'ISO 18152 entre parenthèses)	Exemples de méthodes et techniques
8. Intégration a) Stratégie d'entreprise b) Management de la qualité c) Autorisation et contrôle	Contribuer à l'analyse de rentabilité du système (1.1-7) Définir l'aptitude à l'utilisation du système comme un actif compétitif (2.1-1) Définir les objectifs d'aptitude à l'utilisation, de santé et de sécurité des systèmes (2.1-2) Développer une infrastructure centrée sur l'utilisateur (2.1-4) Associer les problèmes homme-système aux bénéfices de l'entreprise (2.1-5) Définir et maintenir une infrastructure et des ressources CCO et RH (2.2-3) Augmenter et maintenir la sensibilisation à l'aptitude à l'utilisation du système (2.2-4) Développer ou fournir les compétences HS appropriées au personnel (2.2-5) Mettre en œuvre la stratégie de ressources humaines permettant à l'organisation de mettre en œuvre et d'enregistrer les enseignements établis (4.1-4) Inciter et encourager les personnes et les équipes à travailler ensemble afin d'atteindre les objectifs de l'organisation (4.1-6) Créer des capacités de ressources humaines pour satisfaire aux exigences à venir du système (mener un plan de relève) (4.2-7)	– Programmer une analyse des risques – Développer et maintenir une infrastructure et des ressources IHS – Identifier les compétences IHS requises – Apporter les compétences IHS au personnel – Établir et communiquer une politique IHS – Maintenir la sensibilisation à l'aptitude à l'utilisation du système
d) Recrutement	Décider du nombre de personnes nécessaires pour respecter la stratégie, et de l'éventail des compétences dont elles ont besoin (4.1-3)	

Bibliographie

CEI 60812:2009, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

HF-STD-001:2002, *Human Factors Design Standard (HFDS), Federal Aviation Administration*

HFDG, 1996, *FAA Human Factors Design Guide – For Acquisition of Commercial-Off-The-Shelf Subsystems, Non-developmental Items, and Development Systems, DOT/FAA/CT-96/1. Federal Aviation Administration*

MIL-HDBK-46855A:1999, *Human Engineering Program Process and Procedures. Department of Defense*

MIL-HDBK-1472F:1998, *Human Engineering Design Criteria. Department of Defense*

MIL-HDBK-1908B:1999, *Definitions of Human Factors Terms. Department of Defense*

WALLACE, D.F.; WINTERS, J.; DUGGER, M.; and LACKIE, J.:2001, "*Human Systems Engineering: Understanding the Process of Engineering the Human into the System"; Naval Surface Warfare Center Dahlgren Division Technical Report NSWCDD/TR-01/101; November, 2001.*

NASA, *Man-Systems Integration Standards, NASA-STD-3000, Volume I and II (1995)*

FAA, *Guidelines for Human Factors Requirements Development, AAR-100 (2004)*

ISO/PAS 18152:2003, *Ergonomie de l'interaction homme-système – Spécification pour l'évaluation de processus des aspects homme-système*

ISO 6385:2004, *Principes ergonomiques de la conception des systèmes de travail*

ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

ISO 9241-1:1997, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 1: Introduction générale*

ISO 9241-2:1992, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 2: Guide général concernant les exigences des tâches*

ISO 9241-3:1992, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 3: Exigences relatives aux écrans de visualisation*

ISO 9241-4:1998, *Ergonomie de l'interaction homme-système – Partie 4: Exigences relatives aux claviers*

ISO 9241-5:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 5: Aménagement du poste de travail et exigences relatives aux postures*

ISO 9241-6:1999, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 6: Guide général relatif à l'environnement de travail*

ISO 9241-7:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 7: Exigences d'affichage concernant les réflexions*

ISO 9241-8:1997, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 8: Exigences relatives aux couleurs affichées*

ISO 9241-9:2000, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 9: Exigences relatives aux dispositifs d'entrée autres que les claviers*

ISO 9241-11:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 11: Lignes directrices relatives à l'utilisabilité*

ISO 9241-12:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 12: Présentation de l'information*

ISO 9241-13:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 13: Guidage de l'utilisateur*

ISO 9241-14:1997, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 14: Dialogues de type menu*

ISO 9241-15:1997, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 15: Dialogues de type langage de commande*

ISO 9241-16:1999, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 16: Dialogues de type manipulation directe*

ISO 9241-17:1998, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) – Partie 17: Dialogues de type remplissage de formulaires*

ISO 9241-20:2008, *Ergonomie de l'interaction homme-système – Partie 20: Lignes directrices sur l'accessibilité de l'équipement et des services des technologies de l'information et de la communication (TIC)*

ISO 9241-110:2006, *Ergonomie de l'interaction homme-système – Partie 110: Principes de dialogue*

ISO 9241-151:2008, *Ergonomie de l'interaction homme-système – Partie 151: Lignes directrices relatives aux interfaces utilisateurs Web*

ISO 9241-171:2008, *Ergonomie de l'interaction homme-système – Partie 171: Lignes directrices relatives à l'accessibilité aux logiciels*

ISO 9241-210:– , *Ergonomie de l'interaction homme-système – Partie 210: Conception centrée sur l'humain pour les systèmes interactifs*[5]

ISO 9241-300:2008, *Ergonomie de l'interaction homme-système – Partie 300: Introduction aux exigences et techniques de mesure relatives aux écrans de visualisation électroniques*

ISO 9241-302:2008, *Ergonomie de l'interaction homme-système – Partie 302: Terminologie relative aux écrans de visualisation électroniques*

---

5 To be published.

ISO 9241-303:2008, *Ergonomie de l'interaction homme-système – Partie 303: Exigences relatives aux écrans de visualisation électroniques*

ISO 9241-304:2008, *Ergonomie de l'interaction homme-système – Partie 304: Méthodes d'essai de la performance de l'utilisateur pour écrans de visualisation électroniques*

ISO 9241-305:2008, *Ergonomie de l'interaction homme-système – Partie 305: Méthodes d'essai de laboratoire optique pour écrans de visualisation électroniques*

ISO 9241-306:2008, *Ergonomie de l'interaction homme-système – Partie 306: Méthodes d'appréciation sur le terrain des écrans de visualisation électroniques*

ISO 9241-307:2008, *Ergonomie de l'interaction homme-système – Partie 307: Méthodes d'essai d'analyse et de conformité pour écrans de visualisation électroniques*

ISO 9241-308:2008, *Ergonomie de l'interaction homme-système – Partie 308: Écrans à émission d'électrons par conduction de surface (SED)*

ISO 9241-309:2008, *Ergonomie de l'interaction homme-système – Partie 309: Écrans à diodes électroluminescentes organiques (OLED)*

ISO 9241-400:2007, *Ergonomie de l'interaction homme-système – Ergonomie de l'interaction homme-système – Partie 400: Principes directeurs, introduction et exigences générales de conception*

ISO 9241-410:2008, *Ergonomie de l'interaction homme-système – Partie 410: Critères de conception pour des dispositifs d'entrée physiques*

ISO 9241-920:2009, *Ergonomie de l'interaction homme-système* – Partie 920: Lignes directrices relatives aux interactions tactiles et haptiques

ISO 11064-1, *Conception ergonomique des centres de commande – Partie 1: Principes pour la conception des centres de commande*

ISO 11064-2, *Conception ergonomique des centres de commande – Partie 2: Principes pour l'aménagement de la salle de commande et de ses annexes*

ISO 11064-3, *Conception ergonomique des centres de commande – Partie 3: Agencement de la salle de commande*

ISO 11064-4, *Conception ergonomique des centres de commande – Partie 4: Agencement et dimensionnement du poste de travail*

ISO 11064-5, *Conception ergonomique des centres de commande – Partie 5: Dispositifs d'affichage et commandes*

ISO 11064-6, *Conception ergonomique des centres de commande – Partie 6: Exigences relatives à l'environnement pour les centres de commande*

ISO 11064-7, *Conception ergonomique des centres de commande – Partie 7: Principes pour l'évaluation des centres de commande*

ISO/PAS 18152:2003, *Ergonomie de l'interaction homme-système – Spécification pour l'évaluation de processus des aspects homme-système*

ISO/TR 18529:2000, *Ergonomie – Ergonomie de l'interaction homme/système – Descriptions des processus cycle de vie centrées sur l'opérateur humain*

ISO/CEI 24765:–, *Ingénierie des systèmes et du logiciel – Vocabulaire*[6]

ISO/CEI DIS TR 25060:–, *Common Industry Format (CIF) for Usability – General Framework for Usability-related Information*[7]

Analyse de fiabilité humaine (AFH)

NOTE Les titres sont précédés par la méthode, en acronyme.

ASEP: SWAIN, A.D. (1987) *Accident Sequence Evaluation Program on Human Reliability Analysis Procedure. NUREG/CR-4772. NRC. Washington DC*

ATHEANA: NUREG-1624:2000, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). NRC. Washington DC. Rev. 1*

CAHR: STRÄTER, O.:2005, *Cognition and safety – An Integrated Approach to Systems Design and Performance Assessment. Ashgate. Aldershot. (ISBN 0754643255)*

CREAM. HOLLNAGEL, E.:1998, *Cognitive Reliability and Error Analysis Method – CREAM. Elsevier. New York, Amsterdam. (ISBN 0-08-042848-7)*

ESAT: BRAUSER, K.:1992, *ESAT- Ein neues Verfahren zur Abschätzung der menschlichen Zuverlässigkeit. In: Gärtner, K. (Hrsg.) Menschliche Zuverlässigkeit. DGLR-Bericht 92-04. DGLR. Bonn*

HCR/ORE: MOIENI, P., SPURGIN, A.J. & SINGH, A.:1994, *Advances in Human Reliability Analysis Methodology. Part I: Frameworks, Models and Data. Reliability Engineering and System Safety. Vol.44. Elsevier. p. 27*

KIRWAN, B.:1994, *A Guide To Practical Human Reliability Assessment. CRC*

MERMOS: LE BOT, P., DESMARES, E. & BIEDER, C.:1998, *MERMOS: an EDF project to update Human Reliability Assessment methodologies. In: Lydersen, S., Hansen, G. Sandtorv, H. (1998) Safety and Reliability. ESREL'98, Trondheim/Norway. A. A. Balkema. Rotterdam. p. 767 ff*

SLIM: EMBREY, D., HUMPHREYS, P. ROSA, E.A., KIRWAN, B. & REA, K.:1984, *SLIM-MAUD- An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement. NUREG/CR-3518. NRC. Washington DC*

SPAR-H: BYERS, I.C., GERTMAN, D.I., HILL, S.G., BLACKMAN, H.S., GENTILLON, C.D., HALLBERT, B.P., & HANEY, L.N.:2000, *SPAR HRA Methodology: Comparison with other HRA methods. International Ergonomics – IEA 2000. San Diego. Human Factors and Ergonomics Society. Santa Monica CA. Published by: Mira Digital Publishing. South Jefferson, St. Lois, MO (www.miracd.com)*

THERP: SWAIN, A.D. & GUTTMANN, H. E.:1983, *Handbook of Human Reliability Analysis with emphasis on nuclear power plant applications. Sandia National Laboratories, NUREG/CR-1278. Washington DC*

---

6 To be published.

7 To be published.

WILLIAMS, J.C.:1988, *HEART – A data-based method for assessing and reducing human error to improve operational performance. In: Proceedings of the IEEE Conference on Human Factors and Power Plants. Monterey, CA. June 1988. P. 436-450*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch