



BSI Standards Publication

DRAFT FOR DEVELOPMENT

Human reliability – Guide to the fundamental considerations

This publication is not to be regarded as a British Standard. See Foreword for further information.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2010

ISBN 978 0 580 53865 0

ICS 03.020

The following BSI reference relates to the work on this standard:
Committee reference DS/1

Publication history

First published April 2010

Amendments issued since publication

Date	Text affected
------	---------------

Contents

Foreword *ii*

Introduction *1*

1 Scope *1*

2 Normative references *2*

3 Terms, definitions and abbreviations *2*

4 Human performance *4*

5 Human reliability assessment (HRA) *6*

Annexes

Annex A (informative) Case studies using qualitative methods *21*

Annex B (informative) Case study using quantitative methods *28*

Annex C (normative) Influences on the preconditions of human performance *42*

Annex D (normative) Human reliability assessment (HRA) process *43*

Bibliography *44*

List of figures

Figure A.1 – Chlorine case study hierarchical task analysis (HTA) *26*

Figure B.1 – Operator action tree for ESD failure scenario *34*

Figure C.1 – Influences on the preconditions of human performance *42*

Figure D.1 – Human reliability assessment (HRA) process *43*

List of tables

Table A.1 – Example from multiple activity chart (MAC) for drilling activities *21*

Table A.2 – Sample of traditional and specialized guidewords for analysis drilling *22*

Table A.3 – Driller's HAZOP: extract *23*

Table A.4 – Sample human error analysis (HEA) table *27*

Table B.1 – APJ results for ESD scenario *33*

Table B.2 – SLIM-based ERA *36*

Table B.3 – HEART generic categories *38*

Table B.4 – HEART EPCs *39*

Table B.5 – Results table *40*

Table B.6 – Relative contributions *40*

Table B.7 – A subset of HEART remedial measures *41*

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 44, an inside back cover and a back cover.

Foreword

Publishing information

This Draft for Development is published by BSI and came into effect on 30 April 2010. It was prepared by Technical Committee DS/1, *Dependability and terotechnology*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature so that information and experience of its practical application can be obtained.

A review of this Draft for Development will be carried out not later than 2 years after its publication.

Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development, will be made in an announcement in the appropriate issue of Update Standards.

According to the replies received, the responsible BSI Committee will judge whether the Draft for Development can be converted into a British Standard or what other action should be taken.

Observations which it is felt should receive attention before the official call for comments will be welcomed.

These should be sent to the Secretary of BSI Technical Committee DS/1 at British Standards House, 389 Chiswick High Road, London W4 4AL.

Use of this document

As a guide, this Draft for Development takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

As a Draft for Development, this document is of a provisional nature. It should not be quoted as if it were a British Standard.

Presentational conventions

The provisions in this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a Draft for Development cannot confer immunity from legal obligations.

Introduction

Human performance can be analysed by the application of human reliability assessment programmes to minimize the risk of human errors leading to undesirable events. However, it should be remembered that the role of the human in system performance can be beneficial with the ability to mitigate failures and minimize the loss of product or plant availability or threats to safety. Regardless of what a company (or undertaking) designs, manufactures, constructs, installs, operates or maintains, human error has an effect upon life cycle efficiency, profits, safety and market share.

Engineers are aware that the technological complexity and scale of industrial process demand that increased attention be placed on the contribution of the human. This is necessary if the dependability inherent in the design is not to be frustrated by human error.

There is a need to increase awareness of human performance with respect to the following.

- a) What is human error?
- b) How is human reliability measured?
- c) What factors influence human error and how can these be addressed in process and product design?
- d) When is the best time to consider the contribution required from the human in process, system design and development, and who should do it?
- e) What role can ergonomics play in optimizing human performance?

The main purpose of this Draft for Development is to improve the awareness of risks of human error as part of a wider goal of improving dependability and reducing risk.

1 Scope

This Draft for Development gives guidance to engineers and managers on the basic concepts of human reliability, in the context of industrial processes and products. The principles of human performance are introduced to explain how human errors arise and how improved operational competence can be achieved. A range of techniques for qualitative and quantitative assessment and improvement of human reliability are provided.

The application of these guidelines and techniques can help to optimize human performance in process/product design through the inclusion of human reliability considerations throughout the product life cycle.

NOTE 1 It is not intended to provide engineers with the competence to solve all human reliability problems, but to provide an awareness of their potential to exist. The appropriate and timely involvement of specialists can then be provided for in the design and development programme.

NOTE 2 Case studies using qualitative and quantitative methods are given in Annex A and Annex B respectively.

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.

BS 4778-3.2:1991, *Quality vocabulary – Part 3: Availability, reliability and maintainability terms – Section 3.2: Glossary of international terms* [IEC 60050-191:1990]

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this Draft for Development, the terms and definitions given in BS 4778-3.2:1991 and the following apply.

3.1.1 ergonomics

application of scientific information concerning humans to the design of objects, systems and environments for human use

3.1.2 human error probability

HEP

probability that an error will occur when a given task is performed

3.1.3 human factors

discipline concerned with work systems, including designing machines, operations and work environments so that they match human capacities and limitations

NOTE Human factors is the general term that includes human factors engineering, procedures, training, selection and any technical work related to the human factor in man-machine systems. In common parlance the term tends to be used interchangeably with human engineering, human factors engineering and ergonomics.

3.1.4 human reliability assessment

HRA

process designed to identify, quantify and minimize human errors

3.1.5 performance shaping factor

PSF

factor that can affect human ability to perform tasks as required

NOTE PSFs are also known as “precursors to human error”.

EXAMPLES

Training, environment, workload, fatigue, stress, alcohol and drugs, and individual differences.

3.1.6 task analysis

analytical process for determining the specific behaviours required of the human components in a man-machine system

NOTE Task analysis involves determining the detailed performance required of humans and equipment and the effects of environmental conditions, malfunctions and other unexpected events on both. Within each task to be performed by human, behavioural steps are analysed in terms of:

- a) the sensory signals and related perceptions;*
- b) the decisions, memory storage and other mental processes; and*
- c) the required responses.*

3.2 Abbreviations

For the purposes of this Draft for Development the following abbreviations apply.

APJ	absolute probability judgement
ASEP	accident sequence evaluation programme
CCR	central control room
DCU	distributed control unit
EEM	external error mode
EFD	engineering flow diagram
EOP	emergency operating procedure
EPC	error producing condition
ERA	error reduction analysis
ERM	error reduction measure
ERS	error reduction strategy
ESD	emergency shutdown
HAZOP	hazard and operability study
HCR	human cognitive reliability
HEA	human error analysis
HEART	human error assessment and reduction technique
HEP	human error probability
HRA	human reliability assessment
HRM	human resource management
HRP	human reliability probability
HTA	hierarchical task analysis
MAC	multiple activity chart
P&ID	piping and instrumentation drawing
PCT	paired comparisons technique
PEM	psychological error mechanism
PRA	probabilistic risk assessment
PSF	performance shaping factor
PTW	permit-to-work
QA	quality assurance
SHERPA	systematic human error reduction and prediction approach
SLI	success likelihood index
SLIM	success likelihood index method
SLIM-MAUD	SLIM using multi-attribute utility decomposition
SLIM-SARAH	SLIM with systematic approach to the reliability assessment of humans
THERP	technique for human error rate prediction
TRC	time reliability curve
VDU	visual display unit

4 Human performance

4.1 Overview of human performance

Investigation of the capabilities and limitations of human beings has progressed for many years and a considerable body of data has been accumulated, which provides guidance on optimizing human performance. This is particularly true in the field of anthropometrics and general physiology, with comprehensive guidelines available to designers of industrial systems. Account should be taken of the ability of humans to achieve the tasks allocated to them by designers and managers of systems.

Human reliability has a major impact on safety and life cycle costs, particularly maintenance costs, which include a significant contribution from maintenance-induced equipment failure.

There tends to be overemphasis on human error, because of possible consequences. However, one reason for retaining the human element in systems that could conceivably be fully automated is to deal with unpredictable or improbable circumstances, including equipment failure. It is their ability to mitigate the consequences of failure or restore system operation that is often overlooked in designing for the human interactions. As a consequence, the full potential of human involvement is seldom, if ever, achieved.

Comprehensive consideration of human involvement in processes and products starts at the design stage and continues throughout the life of the product or service. Some of the factors involved in human performance optimization are as follows.

- a) Modelling of human behaviour.
- b) Classification of behavioural components.
- c) Classification of human error.
- d) Human reliability analysis.
- e) Human task analysis.
- f) Human error data.
- g) Human reliability assessment.
- h) Human factors design database.

The use of risk and task analysis techniques is probably the most important aid to understanding how operators/maintainers are expected to interact with the system and to identifying the potential problems. The techniques provide guidance in other areas, including personnel selection criteria, training needs and the provision of operating/maintenance procedures. These techniques can provide powerful guidance to improving human reliability if correctly programmed into the design process.

4.2 Performance shaping factors

All factors that affect human ability to perform work reliably are called performance shaping factors (PSFs). Figure C.1 illustrates different factors that influence human performance. In this figure it is possible to distinguish between external and internal PSFs.

External PSFs are created by the organizational and technical preconditions. In many cases the organizational preconditions can only be described verbally. The technical preconditions in most cases, however, can be defined numerically (e.g. noise).

Internal PSFs are given by the capacity and the readiness of human performance. They are individual factors created by physiological and psychological capacities, fitness and willingness and can therefore not be precalculated.

In all cases the resulting human performance is influenced by both external and internal PSFs, as shown by the arrows in Figure C.1.

4.3 Human error causes

Human error results from a mismatch of the capabilities of the human with those required to achieve the activity/task. Studies have demonstrated that in human-machine systems, human error is often the overriding contributor to actual or potential system failures.

Most errors are unintentional; a combination of circumstances resulting in an error. Some, such as operating the wrong control due to labelling difficulties or failure to respond to a critical alarm because of sensory overload due to multiple alarms are within the scope of ergonomics to eliminate. Others, such as missing a step in a procedure, are more difficult but can be examined and possibly identified using human factors engineering techniques and a solution proposed.

Some work situations are obviously error-prone in the sense that the ergonomics are so poor that errors are likely to occur. Such situations involve demands on humans that are not compatible with their capabilities and limitations and are accident-prone. These situations could result in injury to people or damage to equipment and facilities. The potential for human error can arise from:

a) non ergonomic situation factors such as:

- 1) inadequate layout;
- 2) control elements outside the humans handling capability;
- 3) uncomfortable posture conditions;
- 4) inadequate design for the operating environment e.g. glare on instrument panels.

NOTE These are some of the direct influences on human performance but there are many other factors to be considered, which influence human behaviour indirectly such as fear of radiation or toxins.

b) difficult tasks that overtax human abilities such as:

- 1) complex tasks, i.e. too much to do simultaneously in too short a time frame;
- 2) a task design that is not adapted to the demands of the system;
- 3) possibilities of technical realization that do not consider the human interaction;
- 4) insufficient feedback.

c) organizational dynamics not adapted to human demands such as:

- 1) working periods which are too long;
- 2) a work structure which preconditions operator competence.

As well as these examples of error-prone situations, error-prone persons should be considered. By taking all of the known factors into consideration, however it is more cost-effective to look for accident-prone situations than to look for accident-prone people.

4.4 Human error probability (HEP)

In a given situation it is possible to define human error quantitatively as a probability (HEP), which may be measured subsequently by observation. It is the relation of the number, n , of the observed errors to the total number, N , of the opportunities for error in a given situation:

$$\text{HEP} = \frac{\text{number of errors occurred}}{\text{number of opportunities for errors to occur}} = \frac{n}{N}$$

Thus, if the intention is to buy a cup of coffee from a vending machine and on average tea is accidentally purchased on one occasion in a hundred the HEP is 0.01.

In this context, human reliability is equally defined as “the probability of successful performance of the human activities for either a reliable or an available system” (human reliability probability, HRP). It is the mathematical complement to human error, i.e.:

$$\text{HRP} = 1 - \text{HEP}$$

5 Human reliability assessment (HRA)

5.1 General

There are three basic functions which HRA techniques generally fulfil.

- a) To determine what can go wrong in a task where system misuse, malfunction or failure can occur. This qualitative analysis requires an analysis of the task itself to see how it will be performed. It also requires an analysis of human error or task failure potential that also can lead, alone or in conjunction with other hardware/software/environmental events, to overall system failure.
- b) The second basic function of HRA is quantifying how likely human errors are and hence what the overall probability of task success failure/success will be. A wide range of approaches for human reliability quantification exist. Once numerical estimates of human reliability have been derived and integrated into the overall system reliability analysis, the importance of individual errors or tasks to system reliability can be determined quantitatively.
- c) The third function of HRA, and of ergonomics in general, is that of error reduction. Errors that are found to have a significant impact on reliability or risk may need to be reduced in their likelihood or eradicated entirely.

Figure D.1 shows a generalized model called the HRA process, which embodies these three main functions. There are nine parts to the HRA process, each one described briefly in the form of a question, as follows.

- 1) **Problem definition**
What types of human involvements are to be investigated/assessed? (See 5.2.)
- 2) **Task analysis**
How will the task be performed and what type of aids will be needed to support performance? (See 5.3.)
- 3) **Human error analysis (HEA)**
How can task performance fail: what errors can occur and how can they be recovered? (See 5.4.)
- 4) **Representation**
How can these errors or task performance failures be integrated with other hardware, software and environmental events to enable overall system failure likelihoods to be calculated? (See 5.5.)
- 5) **Screening**
Are there any errors or tasks that do not require detailed quantification? (See 5.6.)
- 6) **Quantification**
How likely are individual errors and failures of tasks? (See 5.7.)
- 7) **Impact assessment**
Which errors or tasks are most important, i.e. which ones have the highest contribution to reliability or risk? (See 5.8.)
- 8) **Error reduction**
How can higher human reliability be achieved? (See 5.9.)
- 9) **Documentation**
What details of the HRA need to be documented? (See 5.10.)

In practice the HRA process proceeds step-wise although sometimes with parts (e.g. tasks analysis and error identification) proceeding in parallel with one another.

5.2 Problem definition

Prior to the use of formal techniques, the problem areas being addressed should be defined and this, to a large extent, amounts to scoping the HRA. The Project Manager should decide the area of focus of the HRA, asking questions such as:

- a) Will the HRA look at emergency operations only or normal and maintenance tasks also?
- b) Is quantification of error probabilities required? (This is not always necessary.)
- c) Will the HRA be used to determine error reduction measures (ERMs)?

Overall, the study should focus on the major anticipated vulnerabilities to human error. These can sometimes be identified by reviewing similar plant PRAs, or accident/incident records, or by looking at those systems that are critical to system performance and which themselves require or can be directly influenced by operator action. Once the area of focus has been defined, the next step is to analyse the task.

5.3 Task analysis

The study of what an operator (or team of operators) is required to do, in terms of actions and/or cognitive processes, to achieve a system goal is known as task analysis. There are many forms of task analysis but their primary purpose for HRA includes the following.

- a) Describe the operator goals.
- b) Describe the correct sequences of actions and legitimate variations.
- c) Note critical operator interactions with the system via controls and displays, including critical system feedback to the operator(s) indicating success or failure, and including use of procedures and communications.

If task analysis is not carried out there is a very real danger of underestimating human error potential in a system if task analysis is not carried out, i.e. if the assessor were to make a judgement of what error(s) could occur without formally analysing and describing the task. Task analysis forces the assessor to systematically consider the various aspects of the task and should lead to more robust and comprehensive error identification and quantification. Task analysis is therefore not merely a preliminary to error identification, but should be seen as an integral and important part of the HRA process.

There are a number of useful methods of task analysis for HRA purposes:

- 1) Hierarchical task analysis (HTA) maps out, in a hierarchical flowchart, the overall goal of a task, the major actions necessary and sufficient to fulfil that task and the operations (usually actions) required to achieve those tasks. The HTA should also contain plans which state when tasks should be carried out. The sequence specified in the plans can be strict, contingent upon signals from the operator interface (e.g. alarms, temperature/pressure instrument levels, etc.), a matter of choice for the operator, or a combination of these plan types. HTAs are most readily applicable to operations which have relatively stable goal structures, e.g. normal operations, maintenance/calibration/testing activities or textbook fault conditions that have highly specified and unambiguous procedures.
- 2) Tabular approach of which there are two useful forms.
 - i) Tabular scenario analysis which tracks the shifting goals and changes of system status as an event progresses. Tabular analysis of this kind is only used for detailed analysis of event-driven scenarios. An advantage of this approach over the others is that operator expectations and other more cognitive (knowledge-based) events can be estimated and tracked as the scenario proceeds, based on the known indications that will occur and will be presented to the operator(s).
 - ii) Tabular task analysis which focuses on the information given to operators so that they know whether task performance is proceeding adequately or not. This approach is useful for detailed analyses of tasks carried out in normal operation or under maintenance conditions, particularly where there is a strong reliance on information displays.
- 3) Timeline analysis, in which operator involvements in tasks are noted in terms of their respective durations, so that total time to goal achievement (finishing all tasks) is derived.

Without some type of formal task analysis the assessor is at risk of either not knowing what is being assessed, or of working in a vague, non-auditable and unsystematic way. Just as analysis of the hardware functions of a plant should be based upon system specifications and drawings, HRA should always be based upon a formal and documented task analysis. The minimum analysis suggested is a sequential task analysis, which details the overall goal structure and sequence of operations. For more detailed analysis, e.g. of sensitive human errors, an HTA and possibly a tabular task analysis should be carried out for operations involving relatively stable goal structures and tabular scenario analysis for event-driven scenarios.

Wherever possible, the analyst should base the task analysis on field observations and interviews with operators who carry out the tasks and not rely solely on documentation such as procedures and training manuals. The way tasks are actually carried out in industry may differ substantially from the ways specified in the documentation. Sometimes access to operators and observation of the tasks themselves may not be possible and the assessor could have to rely on documentation. However, in such circumstances, operator experience of similar or prototype plants or systems should be taken into account.

5.4 Human error analysis (HEA)

5.4.1 HEA goals

The accuracy of HRA is critically dependent upon comprehensive identification of significant errors or operator interventions necessary for adequate system performance and safety. This is because if such errors and/or actions are not identified in the first place then the accuracy of representation, quantification and error reduction could be irrelevant and may continue to underestimate the risk potential of a system.

The primary consideration in HRA is comprehensive identification of significant human error potential and operator action requirements. This is the principal goal of HEA and task analysis.

A secondary goal of HEA is robust error reduction. This requires an understanding of the major factors affecting performance linked to error reduction (training, procedures, controls and displays) which are causes that dictate why the error occurred and how it occurred in terms of the mechanisms of operator functioning. If risk is undesirably high then a proportion of such assessments would probably also highlight human error as the main problem area to be solved. The logical step is to reduce human error likelihood but to do this without actually understanding or modelling what causes the error and how it manifests itself could lead to an ineffective solution, erroneously accredited with reducing the HEP. Clearly the reduction of human error requires a proper understanding of the human error itself, rather than a simple gross level description such as "operator presses wrong button" (e.g. there are several reasons why such an error could occur: inadequate training, inappropriate operator procedure, inadequate labelling or layout and workspace design, each of which may have a different ergonomics solution).

Useful human error identification techniques should therefore address the following.

- a) External error mode EEM identification
All human errors can be categorized into these descriptions. They are the levels of description that are put into the reliability assessment, e.g. operator fails to respond to alarm "error of omission", or "not done".
- b) Identification of performance shaping factors PSFs, i.e. why the error can occur.
These are factors that affect performance and can be usefully considered during the human error identification phase, although frequently they are not identified until the quantification phase.
- c) Psychological error mechanism PEM, i.e. how it happens.
These descriptions define, in psychologically and/or ergonomically meaningful terms, how the error actually can occur in terms of operator functioning e.g. "failure to respond" could be due to a misinterpretation of the signal, or due to reduced capabilities.

The distinction between the EEM and the error mechanism is particularly important if error reduction is required. Knowing the error mechanism, effective error reduction mechanisms can be more easily specified.

Some basic useful techniques in the area of HEA include the following.

- 1) A checklist of EEMs (see 5.4.2).
- 2) A list of PEMs (see 5.4.3).
- 3) A list of PSFs (see 5.4.4).
- 4) An HEA tabular approach for carrying out HEA systematically and auditably (see 5.4.5).

These can be supplemented by other more sophisticated techniques but they tend to be proprietary systems. The approaches in 5.4.2, 5.4.3, 5.4.4 and 5.4.5 are in the public domain and, although they require ingenuity in their application by the assessor, they are relatively straightforward and can be used effectively in HEA.

5.4.2 External error modes (EEM)

The following is a list of useful EEMs that can be used as prompts by any assessor to aid in the identification of human errors.

- a) Action omitted.
- b) Action too early.
- c) Action too late.
- d) Information not obtained/transmitted.
- e) Wrong information obtained/transmitted.

Human errors can generally be identified and described using these simple descriptions (e.g. "operator fails to respond to alarm" would be a case of "action omitted").

- 1) Action too much.
- 2) Action too little.
- 3) Action too long.
- 4) Action too short.

- 5) Action in wrong direction.
- 6) Right action on wrong object.
- 7) Wrong action on right object.
- 8) Wrong action on wrong object.

As a general consideration on how human error contributes to system failure, the following important operator involvements should be considered.

- i) Maintenance and other errors that could render safety systems unavailable in the event of an accident sequence (e.g. system inadvertently left off-line after corrective maintenance).
- ii) Actions that could initiate a fault or accident sequence.
- iii) Failure of actions that are required to stop the accident sequence (e.g. activation of safety systems; shutdown).
- iv) Actions or decisions that could make the situation worse (e.g. misdiagnosis during a fault sequence).
- v) Actions which can recover the system from failure and stop the accident sequence or mitigate its consequences (e.g. restoration of safety systems; evacuation).

A technique that can utilize EEMs is the hazard and operability (HAZOP) technique. This technique involves a small group of engineers, operators, safety assessors and human factors experts, led by a chairperson, considering the task steps and task environments, step-by-step. At each step the question is asked with reference to the EEMs, "what could go wrong?" Potential errors are thus identified and their consequences assessed and recommendations noted. The HAZOP approach is a powerful, if resource intensive, technique for HEA.

5.4.3 Psychological error mechanisms (PEMs)

The following are the major PEMs used in HRA.

- a) Failure to consider special circumstances:
A task is similar to other tasks but special circumstances prevail which are ignored and the task is carried out inappropriately.
- b) Short cut invoked:
A wrong intention is formed based on familiar cues which activate a short cut or inappropriate rule.
- c) Stereotype takeover:
Owing to a strong habit, actions are diverted along some familiar but unintended pathway.
- d) Need for information not prompted:
Failure of external or internal cues to prompt need to search for information.
- e) Misinterpretation:
Response is based on wrong apprehension of information such as misreading of text or an instrument, or misunderstanding of a verbal message.
- f) Assumption:
Response is inappropriately based on information supplied by the operator (by recall, guesses, etc.) which does not correspond with information available from outside.