

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

Per conto di AICQ CN¹ - Autore Giovanni Mattana - Consigliere di Giunta AICQ CN –Presidente della Commissione IEC per la Fidatezza



IEC 62508

Edition 1.0 2010-06

**INTERNATIONAL
STANDARD**

**NORME
INTERNATIONALE**

Guidance on human aspects of dependability

Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement

¹ marzo 2012 -RIPRODUZIONE VIETATA SENZA IL CONSENSO DI AICQ CENTRONORD E DELL'AUTORE

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

L'INDICE DEI CONTENUTI DELLA NORMA

FOREWORD

INTRODUCTION

1 Scope

2 Normative references

3 Terms, definitions and abbreviations

4 Human aspects

5 Human-oriented design in the system lifecycle

6 Human-oriented design at each life cycle stage

7 Human-centered design methods

Annex A (informative) Examples of HRA methods.

Annex B (informative) Summary of human-oriented design activities and their impact on system dependability

Annex C (informative) Best practices for human-centered design.

Bibliography.

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

4 Human aspects

4.1 Overview

4.2 Components of the system and their interactions

4.2.1 Introductory remark

4.2.2 Goals

4.2.3 Humans

4.2.4 Machine (interactive system)

4.2.5 Social and physical environment

4.2.6 Output

4.2.7 Feedback from the machine to the person

4.3 Human characteristics

4.3.1 Introductory remark

4.3.2 Human limitations

4.3.3 Comparison of humans and machines

4.4 Human performance shaping factors

4.4.1 External performance shaping factors

4.4.2 Internal performance shaping factors

4.5 Human reliability analysis (HRA)

4.5.1 Overview

4.5.2 Identifying the potential for human error

4.5.3 Analysing human failures to define countermeasures

4.5.4 Quantification of human reliability

4.6 Critical systems

4.7 Human-centred design guidelines

4.8 Human-centred design process

4.8.1 Human-centred design principles within the design process

4.8.2 Human-centred design activities

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

5 Human-oriented design in the system lifecycle

5.1 Overview

5.2 The system life cycle

5.3 Integrating human-oriented design in systems engineering

6 Human-oriented design at each life cycle stage

6.1 Overview

6.2 Concept/definition stage

6.2.1 Concept

6.2.2 Human-centred design planning

6.2.3 Understanding needs

6.2.4 System requirements

6.2.5 Human-centred design requirements

6.3 Design/development

6.4 Realization/implementation

6.5 Operation/maintenance

6.6 Enhancement

6.7 Retirement/decommission

6.8 Outsourcing projects and related human-centred design issues

7 Human-centred design methods

7.1 Classification of human-centred design activities

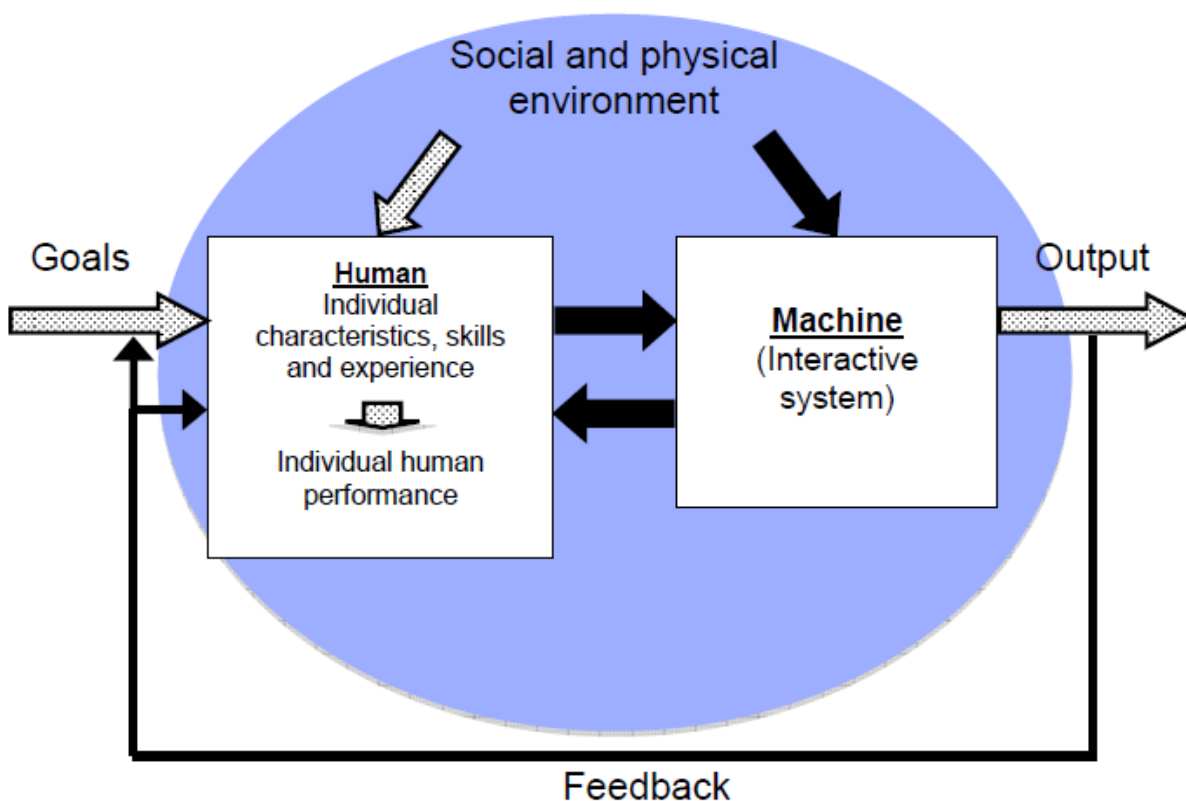
7.2 Applications of human-centred design methods

Annex A (informative) Examples of HRA methods

Annex B (informative) Summary of human-oriented design activities and their impact on system dependability

Annex C (informative) Best practices for human-centred design

Components of the system and their interactions



GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

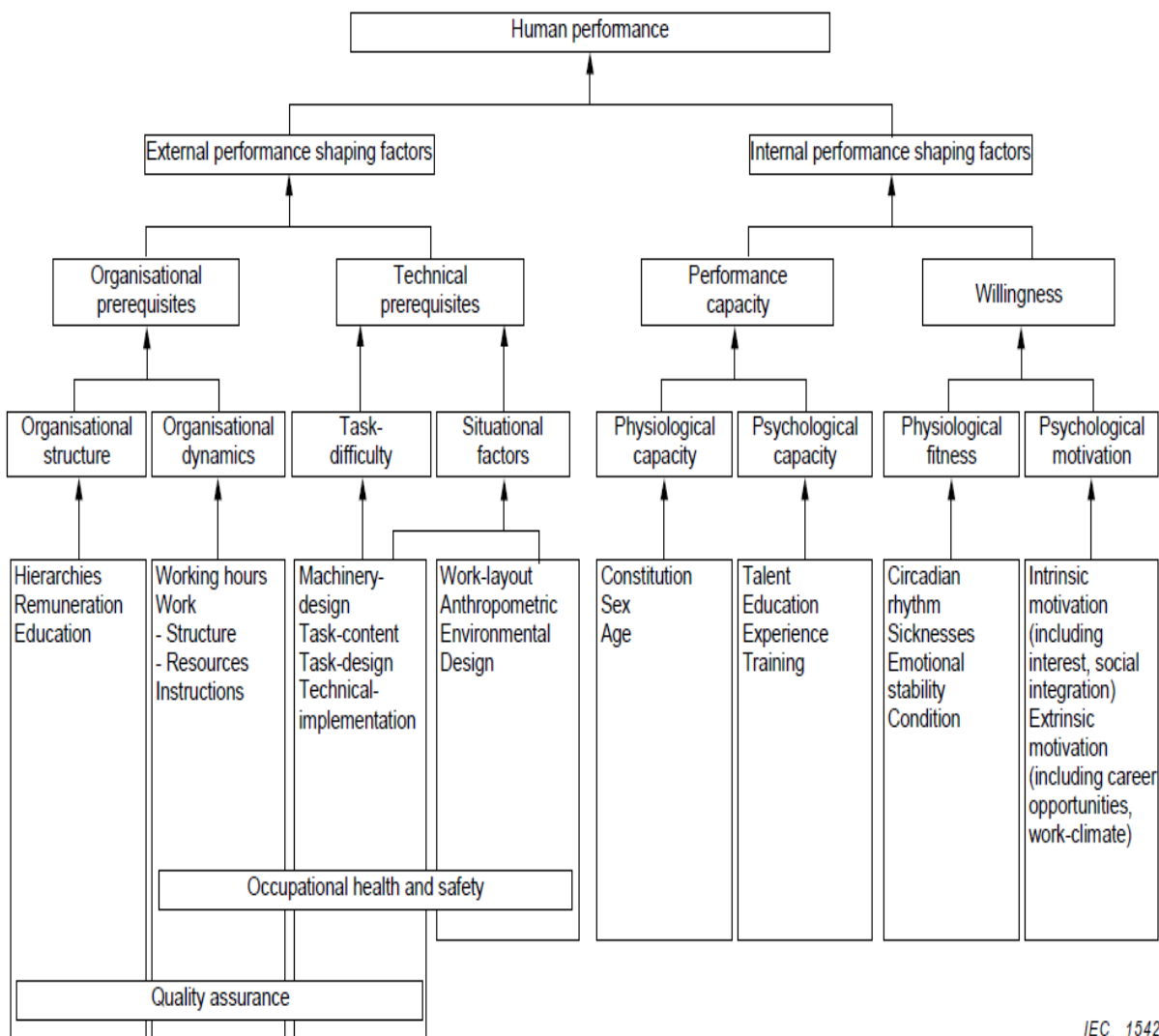
La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

Table 1 – People who influence dependability

Job function	Examples of influence
Project manager	Awareness of dependability needs in system concepts
Designer	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Figure 2 – Human performance shaping factors



IEC 1542/10

Simple model of human information processing

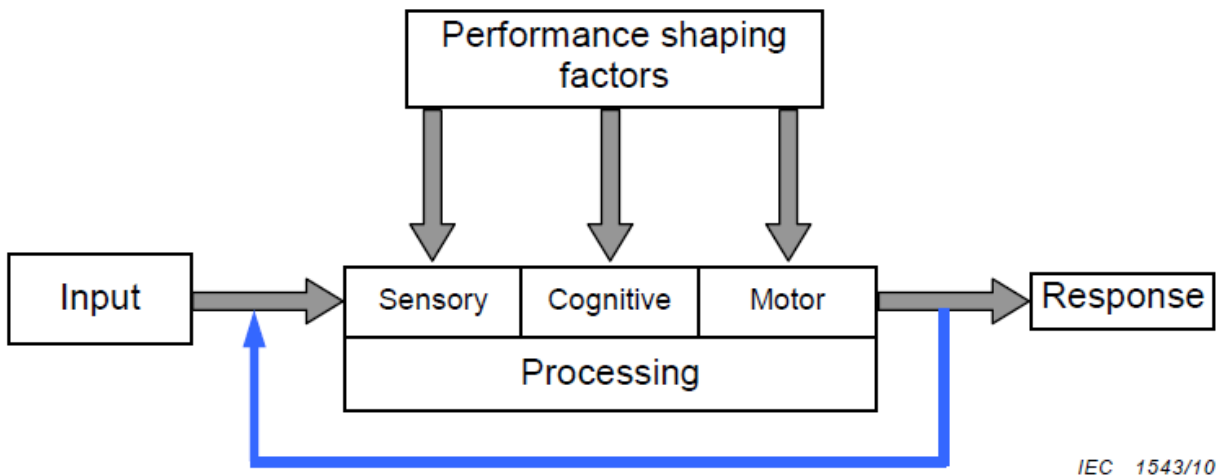
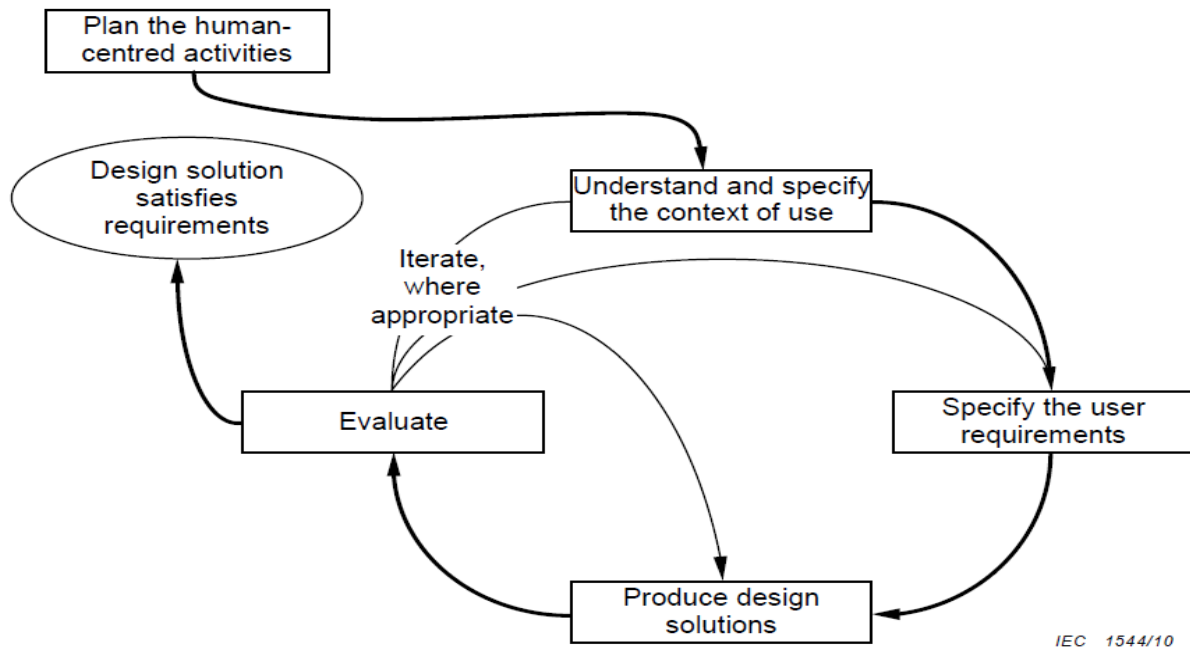


Figure 4 – Human-centred design activities



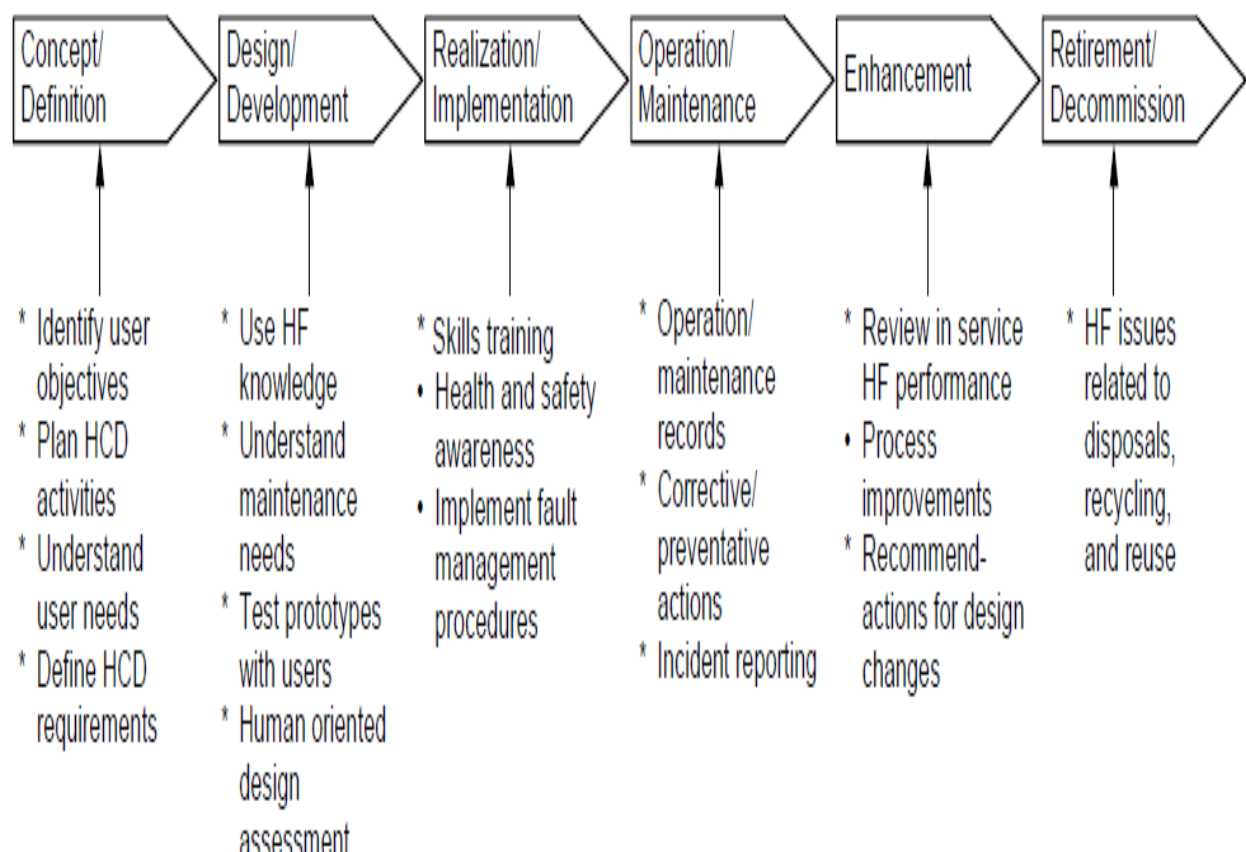
GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

Figure 5 – Human aspects of the system life cycle

System life cycle stages



GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

HRA methods and their application

METHOD AND SHORT DESCRIPTION	Level of use
ASEP – Accident Sequence Evaluation Program	
ATHEANA – A Technique For Human Error Analysis	
CAHR – Connectionism Assessment Of Human Reliability	
CREAM – Cognitive Reliability And Error Analysis Method	
ESAT –expert system for task taxonomy	
FMEA/FMECA – Failure Modes And Effects Analysis	
HCR/ORE (Human Cognitive Reliability / Operator Reliability experiments)	
HEART/CARA – Human Error Assessment And Reduction Technique	
MERMOS –Method for the evaluation of the realization of an operator’s mission regarding safety	
SHERPA – Systematic Human Error Reduction And Prediction Approach	
SLIM – Success Likelihood Index Methodology	
SPAR-H – Standardized Plant Analysis Risk (SPAR) HRA	
THERP – Technique for Human Error Rate Prediction	

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

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

Table B.1 – Automation

Human-centred design activity	Impact on system dependability
<ul style="list-style-type: none"> • 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 safeguards) 	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Improved maintainability. • Improved reliability. • Simplification of maintenance functions. • Enhancing testability, diagnostics, and fault identification. • Reduced maintenance time and logistic support resource requirements.

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

Annex C- Best practices for human-centered design

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)	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – Context of use analysis
1.2 Planning	Develop a plan to achieve and maintain usability throughout the life of the system (2.4-1)	<ul style="list-style-type: none"> – Plan to achieve and maintain usability – Plan use of HSI data to mitigate risks
a) General	Identify the specialist skills required and plan how to provide them (2.4-2)	
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)	<ul style="list-style-type: none"> – 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