Scheda informativa su nuove norme

GUIDANCE ON HUMAN ASPECTS OF DEPENDABILITY

La Norma IEC 62508, Ed. 1.0-2010

Risk Management – Risk Assessment Techniques

Per conto di AICQ CN[1] *- Autore Giovanni Mattana - Consigliere di Giunta AICQ CN –Presidente della Commissione IEC per la Fidatezza*

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

L'INDICE DEI CONTENUTI DELLA NORMA

Components of the system and their interactions

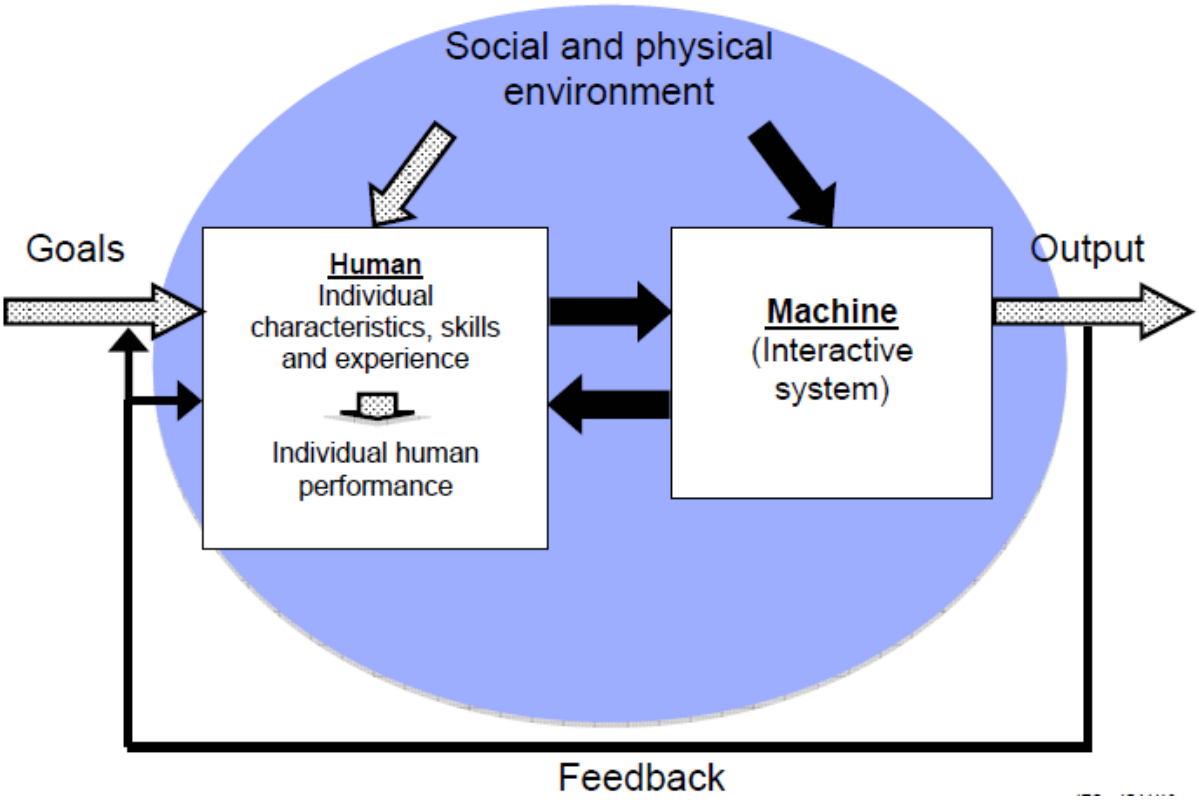
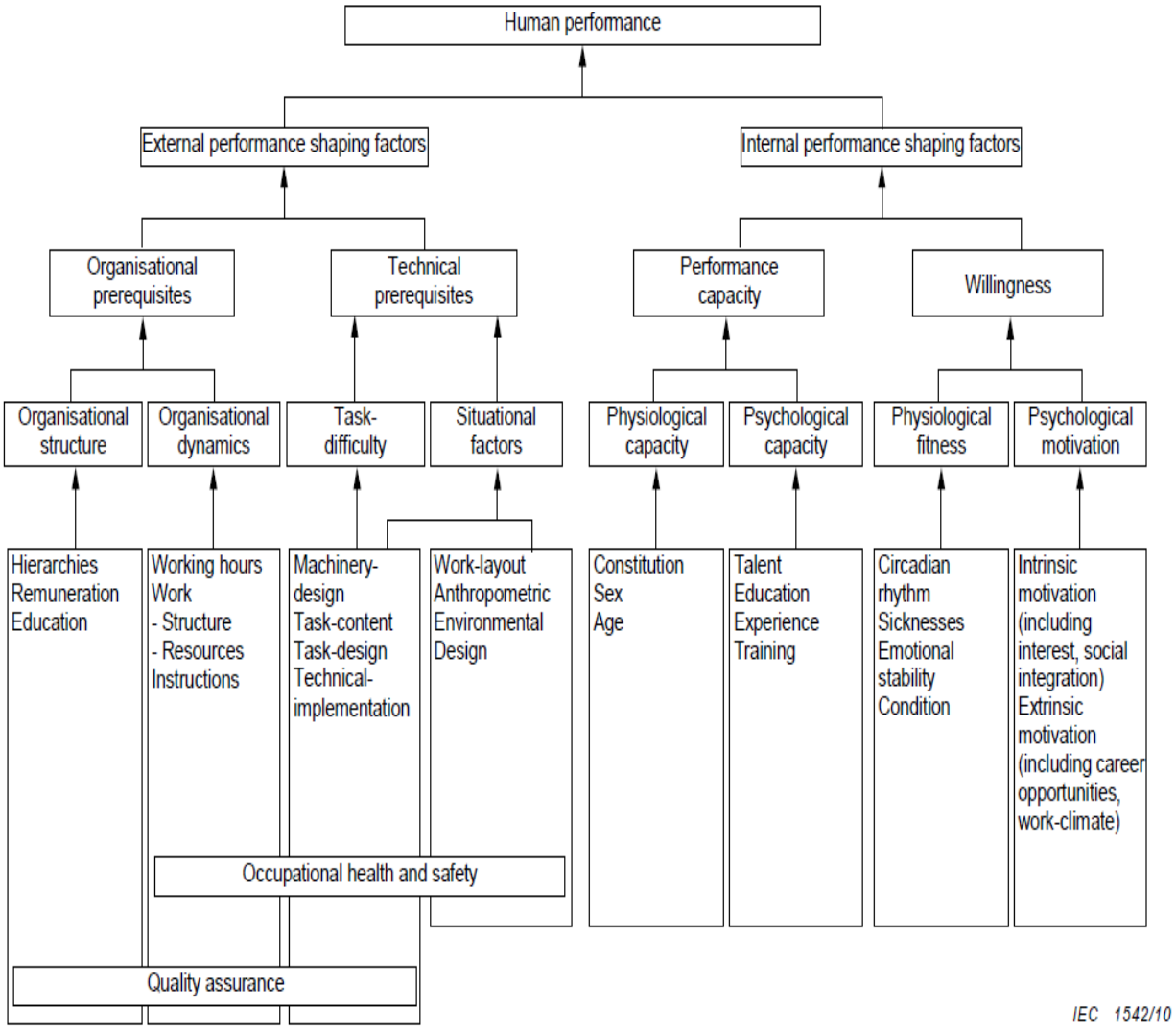


Table 1 – People who influence dependability

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

Figure 2 – Human performance shaping factors



Simple model of human information processing

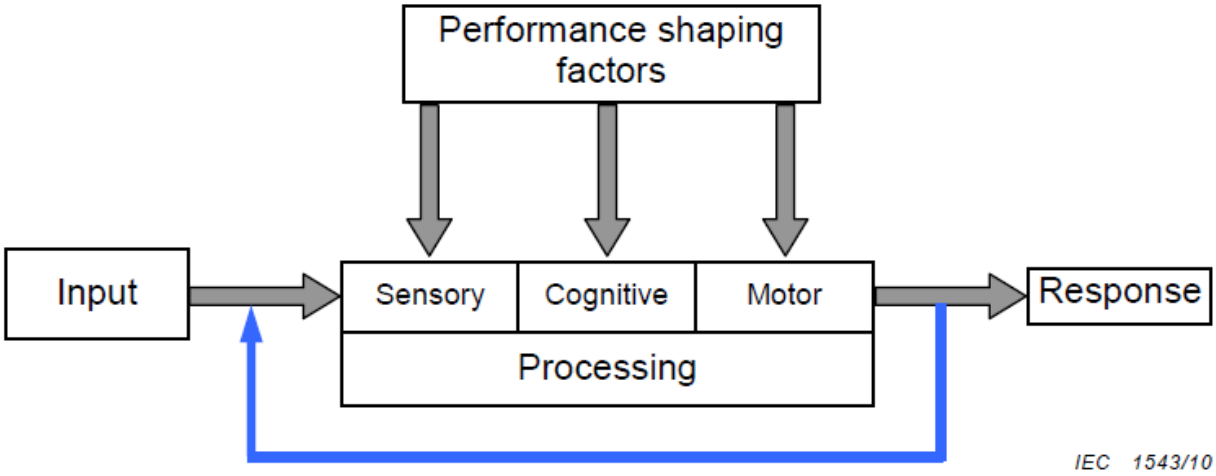


Figure 4 – Human-centred design activities

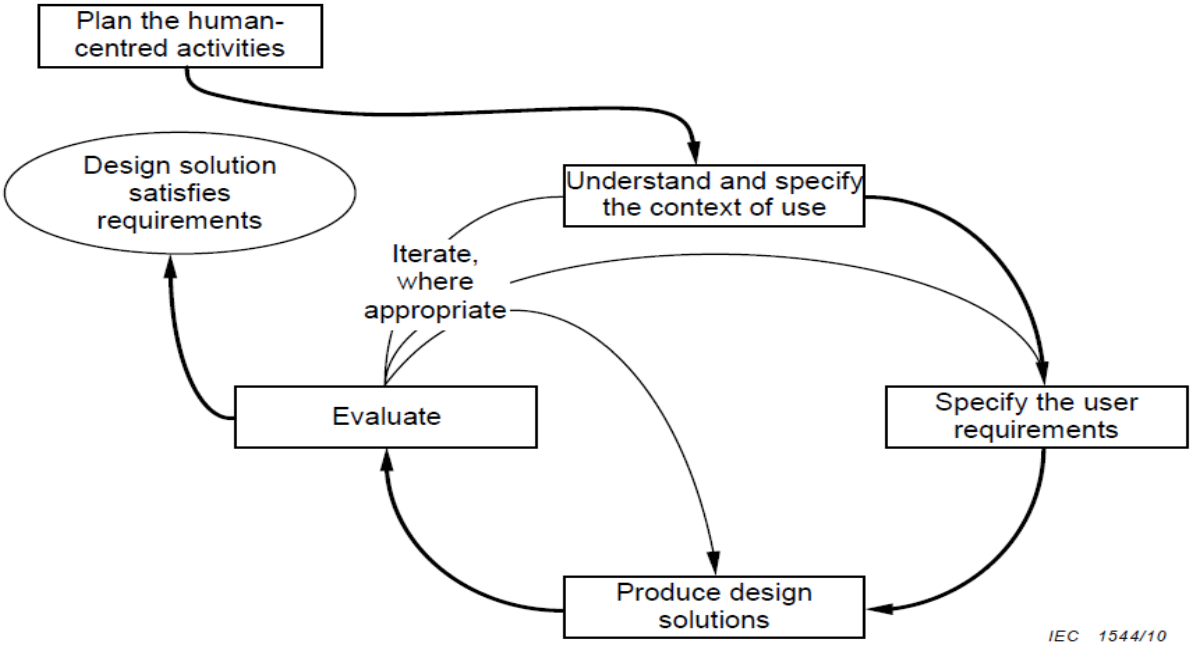
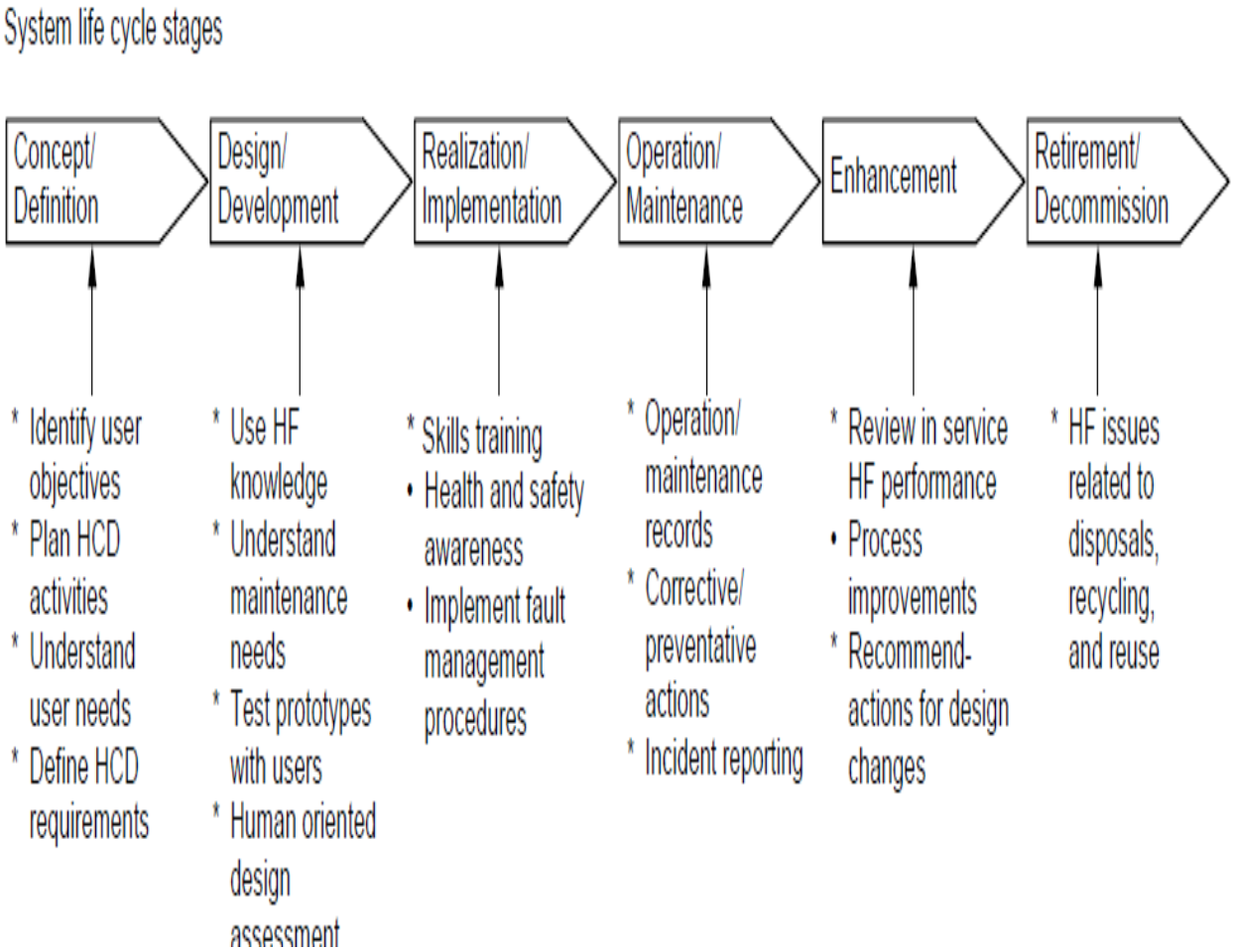


Figure 5 – Human aspects of the system life cycle



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	

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

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.

Annex C- Best practices for human-centered design

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

clic su Strument

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