2009 International Nuclear Atlantic Conference - INAC 2009
Rio de Janeiro,RJ, Brazil, September27 to October 2, 2009
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: **978-85-99141-03-8**

SAFETY, RELIABILITY, RISK MANAGEMENT AND HUMAN FACTORS: AN INTEGRATED ENGINEERING APPROACH APPLIED TO NUCLEAR FACILITIES

Vanderley de Vasconcelos[1], Eliane Magalhães Pereira da Silva[2], Antônio Carlos Lopes da Costa[3], Sérgio Carneiro dos Reis[4]

Centro de Desenvolvimento da Tecnologia Nuclear - CDTN/CNEN
Caixa Postal 941 Cidade Universitária
30161-970 Belo Horizonte, MG
[1] vasconv@cdtn.br;
[2] silvaem@cdtn.br;
[3] aclc@cdtn.br;
[4] reissc@cdtn.br;

ABSTRACT

Nuclear energy has an important engineering legacy to share with the conventional industry. Much of the development of the tools related to safety, reliability, risk management, and human factors are associated with nuclear plant processes, mainly because the public concern about nuclear power generation. Despite the close association between these subjects, there are some important different approaches. The reliability engineering approach uses several techniques to minimize the component failures that cause the failure of the complex systems. These techniques include, for instance, redundancy, diversity, standby sparing, safety factors, and reliability centered maintenance. On the other hand system safety is primarily concerned with hazard management, that is, the identification, evaluation and control of hazards. Rather than just look at failure rates or engineering strengths, system safety would examine the interactions among system components. The events that cause accidents may be complex combinations of component failures, faulty maintenance, design errors, human actions, or actuation of instrumentation and control. Then, system safety deals with a broader spectrum of risk management, including: ergonomics, legal requirements, quality control, public acceptance, political considerations, and many other non-technical influences. Taking care of these subjects individually can compromise the completeness of the analysis and the measures associated with both risk reduction, and safety and reliability increasing. Analyzing together the engineering systems and controls of a nuclear facility, their management systems and operational procedures, and the human factors engineering, many benefits can be realized. This paper proposes an integration of these issues based on the application of systems theory.

1. INTRODUCTION

Nowadays, the licensing process of nuclear facilities in most countries is largely based upon deterministic criteria where the intent is to ensure safety with multiple layers of defense-in-depth. Design basis accidents (DBAs) are defined and safety systems incorporated into the design to respond to these accidents. In general, risk methods are not explicitly considered in the regulatory process although the selection of DBAs and their inclusion on Safety Analysis Reports implicitly include consideration of their risk potential [1].

As a result of the Three Mile Island and Chernobyl accidents, many countries have incorporated additional steps their licensing processes in order to control the risks from accidents. In Brazil, during the early 1980's, the regulatory body (CNEN), in collaboration with the utility personnel, conducted a Probabilistic Safety Assessment (PSA) for the Angra I Nuclear Power Plant. The purpose of this initiative was to develop a safety assessment of the plant to be used by both CNEN and utility, and also to acquire practical experience with the uses and applications of probabilistic methods. As a result of this effort, several plant weaknesses were identified and managed. Over the years, the utility used successfully the available probabilistic models to support the licensing processes [2].

On the other hand, according to competent environmental bodies [3, 4] a Risk Analysis Study (RAS) of activities that can harm the environment is required for licensing purposes. Thus, not only the pollution issues should be considered in licensing processes, but also accident prevention and mitigation. Milling and mining, chemical and petrochemical industries and nuclear facilities are examples of activities that should provide RAS to Brazilian environmental bodies.

In the United States, many applications of PSA to regulatory issues have been carried out. Both the Nuclear Regulatory Commission (NRC) and the regulated industry have made significant advances in the development and application of risk-based technology [5]. Overall, there is clear evidence in all countries that probabilistic risk assessment methods have become an important part of the safety, reliability, and risk management processes in support of regulation. These questions are normally treated individually and without considering systematically human factors that have significant impact on operational effectiveness and risk assessment and management [6].

The use of common tools in the analysis of each one of these subjects, like FMEA (Failure Mode and Effects Analysis), HAZOP (Hazard an Operability Studies), FTA (Fault Tree Analysis), and ETA (Event Tree Analysis), is a clear indication that an integrated evaluation is feasible [7]. This integrated approach is also particularly important when implementing Quality, Safety, Health, and Environment Integrated Management Systems following ISO 9001, BS 8800, OHSAS 18001, and ISO 14001. Such systems can not assure legal compliance, but if they are effective they should act as a tool so that the organizations know their compliance status and preventive and corrective actions can be efficiently implemented [8].

2. TERMINOLOGY AND CONCEPTS

2.1 Safety and Risk Concepts and Terminology

At the scope of the present paper, the following concepts and terminology are adopted [9, 10].

- *Risk:* combination of the probability of an undesired event and its consequence.
- *Hazard:* inherent property (or properties) of a risk source potentially causing consequences or effects.
- *Hazard analysis*: systematic identification of potential hazards and critical accident scenarios associated with hazardous materials or activities. A comprehensive hazard analysis should be able to eliminate or control process hazards during the life-cycle of the

plant. Engineering and administrative measures that are in place to control process parameters, and how these controls are degraded by technical failures, human failures or external events to lead to undesired events should be considered in this type of analysis [11].

- *Risk assessment:* technical estimation of the nature and magnitude of a risk. It involves basically the answers to three questions: What can go wrong? How frequently does it happen? What are the consequences? [12].
- *Risk management:* systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, planning, managing and mitigating risks in a way that will enable organizations minimizing loss and maximizing opportunities in a cost-effective way.
- *ALARP:* a principle ("As Low as Reasonably Practicable") usually applied to risks in some areas as radiation protection and chemical accident prevention, preparedness and response that fall below a defined level of "intolerable" risk. This principle recognizes that not all risks can be eliminated; there will be always a residual risk of an accident since it may not be practicable to take further actions to reduce the risk or to identify the potential accidents.
- *Safety assessment:* evaluation of the actual and potential hazards to human health and to the environment associated with a nuclear facility during its life-cycle, and with events both deliberate and accidental, which could affect its integrity.

2.2 Hazard and Risk Analysis Techniques

Among the most common hazard and risk evaluation tools that can support the team in analyzing process systems and identifying potential accidents can be highlighted [5, 7, 11]:

- *ETA (Event Tree Analysis):* a technique that uses a graphical logic model that identifies and quantifies possible outcomes following an initiating event.
- *FTA (Fault Tree Analysis):* a technique used for estimating the frequency of a hazardous incident (called the top event) through a logic model of the failure mechanisms of the system.
- *CCA (Cause Consequence Analysis:* a method that uses diagrams for seeking the possible outcomes arising from the logical combination of selected input events or states.
- *PHA (Preliminary Hazard Analysis):* a method designed to recognize early hazards and focuses on hazardous materials and major plant systems during the early stages of life-cycle of the plant, when only few details on the plant design and possibly no information about plant procedures may be available.
- *HAZOP (Hazard and Operability Study):* a systematic procedure for identifying potential hazards and operability problems. The HAZOP procedure makes systematically questions over every part of a system to discover how deviations from the design intent can occur. The consequences of these deviations are then determined and, if significant, remedial actions are recommended.
- *FMEA (Failure Mode and Effects Analysis):* a tool that aids in quantifying severity, occurrences and detection of failures, as well as guiding the recommendation of corrective actions, process improvements and risk mitigation plans.
- *Block Diagrams:* a graphical representation of the components of a system and how they are related or connected.

There are many other techniques, like *CL (Checklist Analysis), WI (What If Analysis), SR (Safety Review),* and *RR (Relative Ranking),* that can also support the estimation process of safety, reliability and risk [11].

2.3 Reliability, Maintainability and Availability

- *Reliability* is the probability that an engineering system will perform its intended function satisfactorily for its intended life under specified environmental and operating conditions [13]. Reliability is basically a design parameter and must be incorporated into the system at the design stage. Then, it is an inherent characteristic of the system, just as is its capacity or performance. To analyze and measure the reliability and maintainability characteristics of a system, there must be a mathematical and a logical model of the system that shows the functional relationships among all the components, the subsystems, and the overall system. The reliability of a system is a function of the reliabilities of its components. A system reliability model consists of some combination of a reliability data through the use of techniques like block diagrams, cause consequence analysis, or fault tree analysis. For reliability assessment, the determination of distributions of failure and repair rates, as well as the statement of spare and repair strategies are necessary.

- *Maintainability* is a measure of the ease with which a system or equipment can be restored to operational status following a failure [13]. It is a characteristic of equipment design and facility, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed. Maintainability is the probability that maintenance of the system will retain the system in, or restore it to, a specified condition within a given time period.

- *Availability* is the probability that the system is operating satisfactorily at any time, and it depends on both reliability and maintainability [13].

2.4 Human Factors and Ergonomics

Human Factors is the discipline concerned with the development and application of human system interface technology to systems analysis, design and evaluation. This technology includes human machine, human task, human environment, and organizational-machine interfaces. The efforts of human factors engineering are directed to improving the operability, maintainability, usability, comfort, safety and health characteristics of systems in order to improve the human and system effectiveness and to reduce the potential of injury and error [14].

Human Factors is often used interchangeably with ergonomics that commonly refers to designing work environments for maximizing safety and efficiency. Biometrics and anthropometrics play a key role in this use of ergonomics concept. The importance of ergonomics nowadays is because the companies have learned that designing a safe work environment can also result in greater efficiency and productivity. In Brazil, there are some laws requiring a safe work environment [15]. The design of the workplace as a whole results in a great impact on both safety and efficiency. The easier it is to do a job, the more likely it is to see gains in productivity due to greater efficiency. Analogously, the safer it is to do, also the more likely it is to see gains in productivity due to reduced time off for injury.

Ergonomics can address both of these issues concurrently by maximizing the workspace, equipments and activities needed to do a job.

2.5 Human Reliability Assessment

Human Reliability Assessment (HRA) is a method that involves systematic prediction of potential human errors when interacting with a system. Once they are identified, actions are suggested to try eliminating or reducing their occurrence probabilities, in order to maximize safety and performance of the system or facility. Results of HRA can be entered into risk management actions to reduce the risk to ALARP both by system re-design and implementation of controls and mitigations.

The HRA steps commonly include the identifying of:

- Error types;
- Likelihood of error occurrence;
- Opportunities to recover from errors;
- Consequence of errors.

The HRA should analyze the current design and recommend how to mitigate the errors identified. At the error identification step many reliability and risk analysis tools like FMEA, FTA, ETA and HAZOP, can be used. There are also many other HRA specific techniques like *SHERPA (Systematic Human Error Reduction and Prediction Approach), HEART (Human Error Assessment and Reduction Technique), THERP (Technique for Human Error Rate Prediction), CREAM (Cognitive Reliability and Error Analysis Method)* and *ATHEANA (A Technique for Human Event Analysis)* [16].

2.6 Integrated Health, Safety and Environmental Management

There are several standards of management systems such as ISO 9001 for Quality Management System, ISO 14001 for Environmental Management System, and OHSAS 18001 for Safety and Health Management System. These management systems are often treated as independent functions within organizations. However, the corresponding elements between these three management systems are compatible and it is feasible integrating them [8].

The success of integration will depend on training of managers and skill of support groups to maintain the systems. *ISO 9001* is a framework for adopting a systematic approach for managing business processes to meet customer requirements. *ISO 14001* is a model for an environmental management system and focuses on potential environmental impacts of organizational activities and processes such as pollution, hazardous waste, consumption of natural resources and health of employees. OHSAS 18001 (as well as BS 8800) on the other hand, is a model for an Occupational Health and Safety Management System that enables an organization to control its occupational health and safety and improves its performance.

In order to develop an integrated approach to the design and assessment of a management system, firstly the separate management system standards need to have a common structure. Such common criteria allow standards to be used either separately or collectively.

The implantation of Integrated Management Systems can lead to several advantages, such as:

- *Increase effectiveness of management system.* It increases the effectiveness of management system by utilizing common policies, planning, training, inspecting, monitoring, etc.
- *Reduce duplication and therefore costs.* In the different management systems, there are several elements that are basically similar. The integrated management can therefore minimize the duplicated works in order to achieve an optimum working productivity and profitability.
- *Balance conflicting objectives*. Each management system has it own goal. Sometimes the conflicts occur when the objectives are faced one another. The integrated management can balance the objectives and clearly list the final aims of the project and the way to reach them. Conflict reduction between Safety, Health, Environmental and Quality concerns could be achieved by encouraging the organization to consider the implications of changes to the whole system.
- *Eliminate conflicting responsibilities.*

However, some disadvantages of integration can also be highlighted, for instance:
- Some major differences between each management standard could difficult the correspondence. For instance, while quality standards would affect an organization and its clients, environmental standards have a greater reach that would affect an organization's relationship to its neighborhood, whereas health and safety standard would protect the workers at site from accidents.
- Another disadvantage is that some elements of good safety programs have to be forced to fit into the other two system schemes. Emergency preparedness, for example, does not directly correspond to any ISO quality standard element, and safety requirements often include behavioral aspects that are not typically addressed in any quality procedure.

3. SYSTEMS THEORY

To understand complex systems, scientists usually try to envisage the phenomena of nature and processes as simplified versions of reality known as a system. A system can be defined as a collection of interrelated parts that work together by way of some driving process. Systems are often visualized as component blocks that have connections drawn between them. Systems can be modeled using tools like block diagrams, facilitating the evaluations of safety, reliability or failure modes, for instance.

Most systems share the same common characteristics. These common characteristics include the following [6]:

- Systems have a structure that is defined by its parts and processes.
- Systems are generalizations of reality.
- Systems tend to function in analogous ways. This involves the inputs and outputs (energy, matter or services) that are then processed causing them to change in some way.
- The various parts of a system have functional as well as structural relationships between each other.
- The fact that functional relationships exist between the parts suggests the flow and transfer of some type of energy and/or matter.
- Systems often exchange energy and/or matter beyond their defined boundary with the outside environment, and other systems, through various input and output processes.

- Functional relationships can only occur because of the presence of a driving force.
- The parts that make up a system show some degree of integration - in other words the parts work well together.

Within the boundary of a system we can find three kinds of properties*:*

- *Elements* - are the kinds of parts (things or substances) that make up a system. These parts may be hardware, software, raw materials, and persons, for instance.
- *Attributes* - are characteristics of the elements that may be perceived and measured. For example: productivity, reliability, safety, and availability.
- *Relationships* - are the associations that occur between elements and attributes. These associations are based on cause and effect. In an organizational system, for example, there is a close relationship between human factors and productivity, safety and availability.

The state of a system is defined through the determining of the value of its properties (the elements, attributes, and relationships).

4. INTEGRATED FRAMEWORK

The methodology proposed by this paper for safety, reliability, risk management and human factors integration is shown in Figure 1.

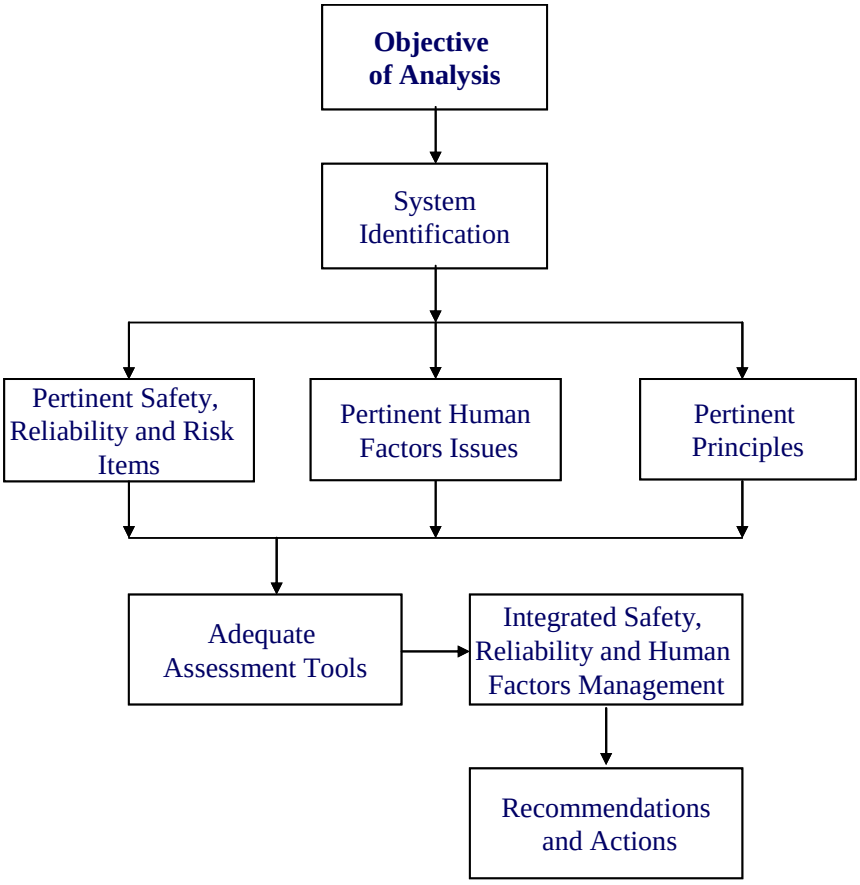


Figure 1. Proposed methodology for safety, reliability, risk management and human factors integration

Once the objective of analysis is defined, Figure 2 can be used as an overview of the possibilities of integration of the human factors (ergonomics), the life-cycle step of the project (design, implantation, operation or decommissioning), the target (quality, occupational health and safety, or environmental management), and the focus of analysis (safety, reliability, or risk). These later attributes will be evaluated taking into account the applicable principles and criteria.

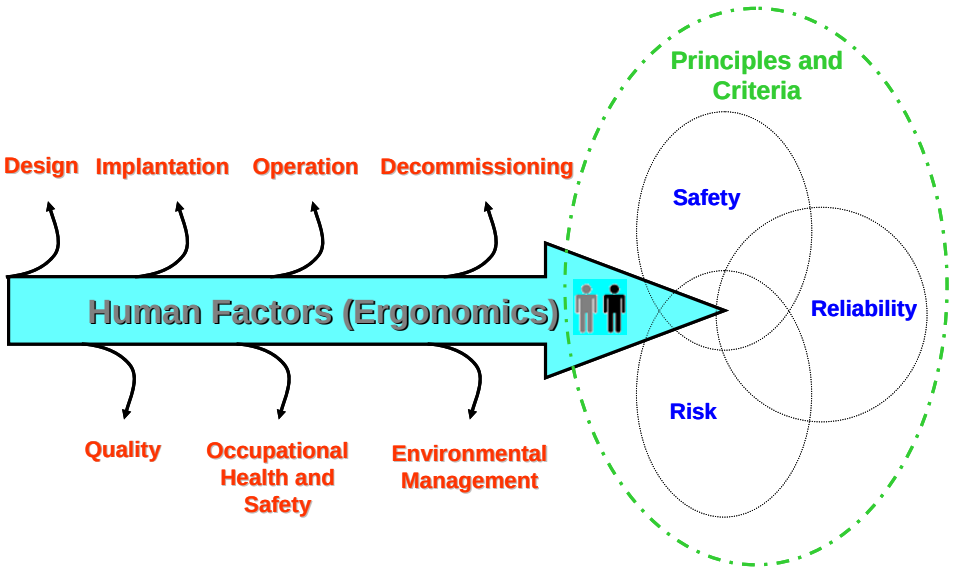


Figure 2. Overview of the framework for human factors integration

The identification of the system to be analyzed is carried out with the aid of systems theory, as illustrated in Figure 3 which shows a systematic model of an organization adapted to an industrial facility [6]. The first box represents the inputs into the system and includes physical, human and financial resources, as well as service and knowledge. The *Transformation Process* integrates the plant (*hardware*) the human resource (*liveware*) and the policies, procedures, rules, and processes (*software*). The right box represents the outputs and, depending on the targets of analysis, elements of quality, occupational health and safety, or environmental management are selected.

The systematic integration of human factors in the analysis is best viewed in Figure 2 through the intersection of the Human Factors (Ergonomics) arrow with the attributes in focus (safety, reliability, or risk) or their intersections. For example, in Figure 4 we can see some identified pertinent safety and reliability items, as well as common pertinent items and human factors issues. By this way, the systems to be analyzed are systematically identified under all focus combination, within the life-cycle step and the required target.

The human factors to be considered in analysis are grouped into six areas in order to warrant that all issues will be considered and can be adequately prioritized. In Table 1 are shown the six human factors areas and some example issues within each one. At each selected focus applicable principles and criteria are selected (examples in Table 2) and the integrated analysis is carried out using the common tools referred in item 2.2 of this paper.

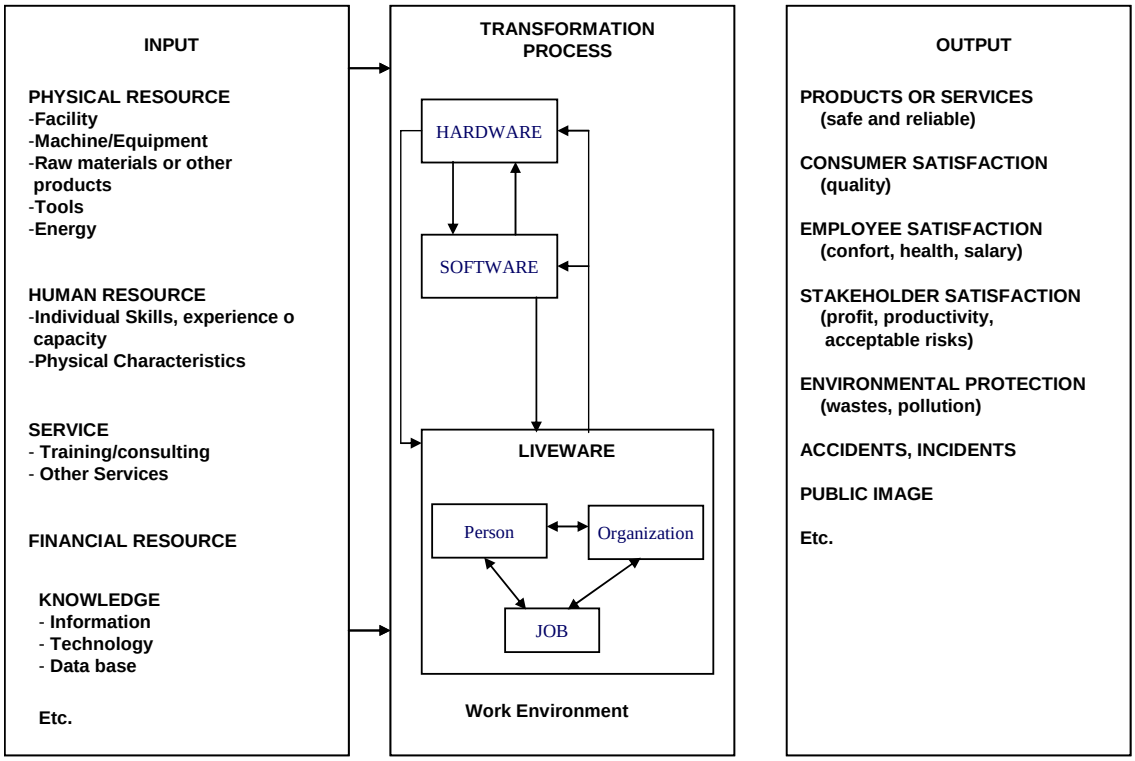
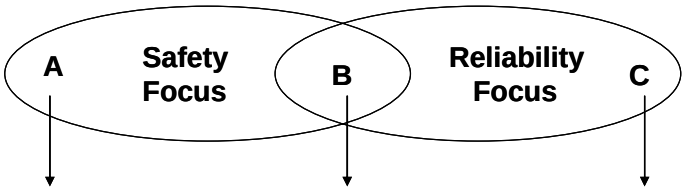


Figure 3. Systemic model of an organization (adapted from [6])



Pertinent Safety Items	Common Pertinent Items and Human Factors issues	Pertinent Reliability Items
Safety control	Safety control	Control
Safety instrumentation	Safety instrumentation	Instrumentation
Engineering safety features	Engineering safety features	Process equipments
Critical equipments	Maintenance of safety systems	Hardware
Hazardous materials	Workload	Software
Radioactive and nuclear materials	Operation of safety systems	Power supply
Etc.	Human reliability	Utilities
	Etc.	Etc.

Figure 4. Examples of pertinent items and Human Factors within an integrated safety and reliability focus

Table 1. Six Human Factors areas and example Human Factors Issues (adapted from [17])

Human Factors Area	Example Issues
1. Human-Machine Interaction (HMI)	Input devices, visual displays, information requirements, alarm handling, console/working area, HMI usability, user requirements, health risks, fatigue, distraction and concentration, noise, lighting, temperature/humidity/air quality, workplace arrangement, workplace accommodation.
2. Organization and Staffing	Staff requirements, manpower availability, human resource profile/selection criteria, job attractiveness, ageing, shift organization.
3. Training and Development	Training needs, performance/competence standards, training content, training methods and media, negative transfer of training, trainer role/responsibilities/competency, transition from classroom to On-the-Job Training (OJT), emergency/unusual situation training, testing of training effectiveness, negative effects on operational task performance.
4. Procedures, Roles and Responsibilities	Allocation of function, involvement, workload, trust/confidence, skill degradation, procedure format and structure, procedure content, procedure realism, documentation.
5. Teams and Communication	Team structures/dynamics/relations, (inter-) team coordination, workload communication, phraseology, national language differences, changes in communication methods, interference effects, information content, types of communication.
6. Recovery from Failures	Human error potential, error prevention/detection/recovery, detection of and recovery from system failures, error taxonomies.

Table 2. Examples of design and analysis principles and criteria applied to safety, reliability, risk and human factors

Safety	Reliability	Risk	Human Factors
Fail-safe design	Standby redundancy	Prevention principle	Ergonomics principles:
Double contingency	Diversity	Precautionary principle	- Work in neutral Postures
Single failure design	k-out-of-n redundancy	Protection principle	- Reduce excessive force
ALARP	Fault tolerant systems	Basic principles of nuclear energy	- Keep everything in easy reach
Defense-in-depth	Safety factors	Principle of limitation of risks to individuals	- Maintain a comfortable environment
Principles of Waste management		Design basis accidents	- Reduce excessive motions

5. CONCLUSIONS

This paper has shown that an integrated analysis of safety, reliability, risk and human factors can be carried out through a proposed methodology that systematically directs the analysis starting from the selection of applicable life-cycle step (design, implantation, operation, or decommissioning) and the required target (quality, occupational health and safety, or environmental management). The analyses of the attributes in focus (safety, reliability, or risk) or their intersections are carried out through the integration of human factors that are selected, prioritized and analyzed considering the applicable principles and criteria, and using common applicable safety, reliability, and risk assessment tools. The merging of these various assessment and management systems could reduce duplication of efforts and costs, and increase the effectiveness of management systems, among others. The authors intend to automate the use of the proposed methodology through the implementation of a computer program integrating their steps and required tools.

ACKNOWLEDGMENTS

The authors would like to thank the Center of Nuclear Technology Development - CDTN/CNEN and FAPEMIG (Minas Gerais State Foundation for Research Development) that sponsored this work, and their colleagues of CDTN/CNEN who were involved with this work.

REFERERENCES

1. CNEN – Comissão Nacional de Energia Nuclear. *Licenciamento de instalações nucleares*. CNEN NE-1.04, Rio de Janeiro, Brasil, 20 p. (2002).
2. Vasconcelos, V.; Silva, E.M.P.; Reis, S.C.; Senne Jr., M.; Jordão, E. "Risk Assessment Methodologies Applied to the Handling of Radioactive and Hazardous Waste". *Proceedings of the International Nuclear Atlantic Conference – INAC 2007,* Santos, Brazil (September 30 to October 5, 2007).
3. CONAMA – Conselho Nacional do Meio Ambiente. *Resolução CONAMA n° 237, de 18/12/1997. Dispõe sobre licenciamento ambiental.* Brasil, (1997).
4. CETESB - Companhia de Tecnologia de Saneamento Ambiental. *Manual de orientação para a elaboração de Estudos de Análise de Riscos*. Norma Técnica CETESB P4.261, Secretaria de Estado de Meio Ambiente, São Paulo, Brasil, 120 p. (2003).
5. Borysiewicz, M.J. et al. *Quantitative Risk Assessment (QRA*), CoE MANHAZ, Institute of Atomic Energy, Poland, 292 p. (2003).
6. Cox, S. and Tait, R. *Safety, Reliability and Risk Management: an Integrated Approach.* 2d. Edition, Butterworth-Heinemann, Oxford, Great Britain, 325 p. (1998).
7. USNRC - U. S. Nuclear Regulatory Commission. *Integrated Safety Analysis - Guidance document. NUREG-1513*, Office of Nuclear Material Safety and Safeguards, Washington D.C., USA, 65 p. (2001).
8. Chaib, E.B.D. *Proposta para implementação de gestão integrada de meio ambiente, saúde e segurança do trabalho em empresas de pequeno e médio porte: um estudo de caso da indústria metal-mecânica.* Dissertação de Mestrado, COPPE, Universidade Federal do Rio de Janeiro, Brasil, Rio de Janeiro, 138p. (2005).

9. Christensen, F.M. et al. “Risk terminology - a platform for common understanding and better communication”, *Journal of Hazardous Materials*, **103**, pp. 181-203 (2003).
10. WHO – World Health Organization, *IPCS risk assessment terminology.* International Program on Chemical Safety (ICPS), Geneva, Switzerland, 122 p. (2004).
11. Lees, F.P. *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, 2d.Edition, Butterworth-Heinemann, Oxford, Great Britain, 3 v. (1996).
12. Stamatelatos, M. et al. *Probabilistic Risk Assessment procedures guide for NASA managers and practitioners - Version 1.1*, Office of Safety and Mission Assurance, NASA Headquarters, Washington D.C., USA, 323 p. (2002).
13. Mobley, R.K., Higgins, L.R. and Wikoff, D.J. *Maintenance Engineering Handbook.* 7th Edition, McGraw Hill Ltd., New York, USA, 1244p. (2008).
14. Iida, I. *Ergonomia, Projeto e Produção*. 2ª. Edição, Editora Edgard Blücher, São Paulo, Brasil, 614 p. (2008).
15. Araújo, B. A. *Normas Regulamentadoras Comentadas. Legislação de Segurança e Saúde no Trabalho*. 6ª. Edição, Gerenciamento Verde Editora e Livraria Virtual, Rio de Janeiro, Brasil, 1196 p. (2007).
16. USNRC - U. S. Nuclear Regulatory Commission. *Good Practices for Implementing Human Reliability Analysis (HRA) – NUREG-1792.* Washington D.C., USA, 103 p. (2005).
17. EUROCONTROL – European Organization for the Safety of Air Navigation. *The Human Factors Case: Guidance for Human Factors Integration - HRS/HIS-003-GUI-01*. Brétigny, France, 114p. (2004).