Integrated Engineering Approach to Safety, Reliability, Risk Management and Human Factors

Vanderley de Vasconcelos, Wellington Antonio Soares, and Raíssa Oliveira Marques

Abstract Nuclear industry has important engineering legacies to share with the conventional industry. As a result of nuclear accidents at Three Mile Island, Chernobyl, and Fukushima, many countries have incorporated new steps into the licensing processes of Nuclear Power Plants (NPP), in order to manage accident risks. Probabilistic Safety Analysis has been used for improving safety, reliability and availability in the design and operation of NPP. Despite the close association between these subjects, there are some important different approaches. The reliability engineering approach uses several principles and criteria to minimize the component failures. These include, for instance, redundancy, diversity, and standby systems. System safety is primarily concerned with risk management, that is, the evaluation and control of hazards, which requires the assessment of interactions among system components. Events that cause accidents can be complex combinations of component or instrumentation failures, faulty maintenance, design errors, or human actions. Then, system safety deals with a broader spectrum of risk management, including human factors (ergonomics), licensing requirements, and quality control. Taking care of these topics individually can compromise the completeness of the analysis and the measures associated to risk reduction, and increasing safety and reliability. This chapter presents an integrated framework for analyzing engineering systems, operational procedures, and the human factors based on the application of systems theory. An application example assessing safety, reliability, risk, and human factors issues related to a complex task of Non-destructive Inspection of piping segments of a primary circuit of a NPP shows the benefits of using the proposed integrated approach.

Keywords Safety • Reliability • Human errors • Risk management • Probabilistic Risk Assessment

V. de Vasconcelos (✉) • W.A. Soares • R.O. Marques
Centro de Desenvolvimento da Tecnologia Nuclear—CDTN, Belo Horizonte, Brasil
e-mail: vasconv@cdtn.br; soaresw@cdtn.br; raissaomarques@gmail.com

F. De Felice, A. Petrillo (eds.), *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures*, Springer Series in Reliability Engineering, https://doi.org/10.1007/978-3-319-62319-1_4

1 Introduction

Current developments for ensuring safe and competitive operation of industrial plants, such as nuclear facilities, in most countries, is largely based upon deterministic criteria using multiple layers of Defense-in-depth (DiD). Design basis accidents (DBAs) are then 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 (IAEA 2009).

As result of the nuclear accidents at Three Mile Island, Chernobyl, and Fukushima, many countries have incorporated additional steps to the licensing processes of Nuclear Power Plants (NPPs) in order to control accident risks. Lessons learned included recommendations to improve plant systems, resources, and operator training to effective responses to severe accidents (IAEA 2012). Probabilistic Risk Assessment (PRA) is used in the nuclear industry in the United States and in many other countries for analyzing accidents beyond-design-basis, such as Fukushima event. Sometimes named Probabilistic Safety Analysis—PSA, this approach is useful for improving safety, reliability and availability in design and operating of NPPs (NAS & USNRC 2014).

Although risk assessment is an integral part of evaluating NPP safety, the main strategy for designing and regulating such facilities remains in DiD philosophy. This involves the use of multiple redundant systems for preventing and mitigating components and human failures. In addition, Human Reliability Analysis (HRA) is typically performed as part of these PRAs (or PSAs) to quantify the likelihood of omission and commission errors, as well as fail in recovery actions.

The United States is an example of country where many application of PRA to regulatory issues have been carried out. Both the U.S. Nuclear Regulatory Commission (USNRC) and the regulated industry have made significant advances in the development and application of risk-based technology (USNRC 2011). Overall, there is clear evidence in all countries that PRA methods have become an important part of the safety, reliability, and risk management processes in support to 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 (Cox and Tait 1998).

On the other hand, the use of common tools in the analysis of each one of these subjects, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), and Event Tree Analysis (ETA), is a clear indication that an integrated evaluation is feasible (USNRC 2001). 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 standards. Such systems cannot assure legal compliance, but if they are effective, they can help the organizations to know better their compliance status, so that

preventive and corrective actions can be efficiently implemented (Vasconcelos et al. 2009).

This chapter proposes an integration of safety, reliability, risk management and human factors issues based on the application of systems theory. Section 2 presents main terminology and concepts related to safety assessment, risk management, reliability engineering, human factors and ergonomics. Section 3 presents an overview of the integrated framework based on systems theory. Section 4 describes briefly the common tools used in the integrated analysis, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Event Tree Analysis (ETA), and Technique for Human Error Rate Prediction (THERP), including mathematical and statistical basis. Section 5 presents a simple representative example to illustrate the benefits of integrated engineering approach to safety, reliability, risk management and human factors for a generic Loss of Coolant Accident (LOCA) in a Nuclear Power Plant. Finally, the conclusions about the integrated framework and summary about application example are presented in Sect. 6.

2 Terminology and Concepts

In the scope of this chapter, there are many concepts and terminology adopted within an integrated engineering approach to safety, reliability, risk management and human factors.

2.1 Safety Assessment

ALARP "As Low as Reasonably Practicable" is a principle 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 risk 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 (HSE 2017). The associated term used in Nuclear Regulatory Commission (NRC) standards is ALARA (As Low As Reasonably Achievable). ALARA means making every reasonable effort to maintain exposure to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, economic factors, and public interest (USNRC 2017).

Safety Assessment Safety can be seen as a practical certainty that adverse effects will not result from exposure to an agent under defined circumstances (Christensen et al. 2003). Safety assessment is therefore a systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the

activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design. Safety assessment includes the formal safety analysis, i.e., it includes the evaluation of the potential hazards associated with the operation of a facility or the conduct of an activity (IAEA 2016a, b).

Defence-in-depth (DID) It is an established safety philosophy, in which multiple lines of defence and safety margins are applied to the design, operation, and regulation of plants to assure that public health and safety are adequately protected. NRC statement for DID is a safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs. This philosophy ensures that the public is adequately protected, and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the safety philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility (ANS 2016).

Design Basis Accidents (DBA) Design-basis accidents are postulated accidents that are used to set design criteria and limits for the design and sizing of safety-related systems and components. When developing a nuclear power plant, DBAs are selected to ensure that plant can withstand and recover from these accidents (USNRC 2013).

Deterministic Safety Analysis It is the engineering analysis of a plant response using validated models, calculations and data that predict transient response of the plant to an event sequence typically uses conservative estimates, safety margins and DBAs, and it is based on expert judgement and knowledge of the phenomena being modelled (ANS 2016).

Probabilistic Safety Assessment (PSA), also referred to as Probabilistic Risk Analysis (PRA) PSA or PRA is a qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public, in the case of NPP (ANS 2016).

2.2 Risk Management

Risk There are many different definitions of risk. In the scope of this chapter, risk is a comprehensive set of event sequences, a quantitative assessment of the event sequence frequencies and their consequences, and an evaluation of the uncertainties in the assessments (Christensen et al. 2003; WHO 2004; ANS 2016). Mathematically this can be expressed as a product of frequency of occurrence and severity, as shown in Eq. 1 (USNRC 1975).

$$Risk\left[\frac{consequence}{time}\right] = frequency\left[\frac{event}{time}\right] \times severity\left[\frac{consequence}{event}\right] \quad (1)$$

Hazard It is an event or a natural phenomenon that poses some risk to a facility. Internal hazards include events such as equipment failures, human failures, and flooding and fires internal to the plant. External hazards include events such as flooding and fires external to the plant, tornadoes, earthquakes, and aircraft crashes (Lees 2012).

Hazard Analysis It is the determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by assessment of hazardous situations associated with a process or activity. Qualitative techniques are normally used to pinpoint weaknesses in design or operation of the facility that could lead to hazardous material releases. The hazard analysis examines the complete spectrum of potential events that could expose members of the public, facility workers, and the environment to hazardous materials (Lees 2012).

Risk Assessment Refers to technical estimation of nature and magnitude of a risk. It involves basically answers to three questions: What can go wrong? How frequently does it happen? What are the consequences? Figure 1 illustrates the risk assessment process. Risk assessment is a process for measuring, qualitatively and quantitatively, the risks a particular agent represents for a specific system or facility (Stamatelatos 2002).

Risk Management It is a systematic application of management policies, procedures and practices of establishing the context, identifying, analyzing, planning, implementing, controlling, communicating and documenting risks in a way that will enable organizations minimizing loss and maximizing opportunity in a cost-effective way (Stamatelatos 2002; IAEA 2001). A risk management process is illustrated in Fig. 2.

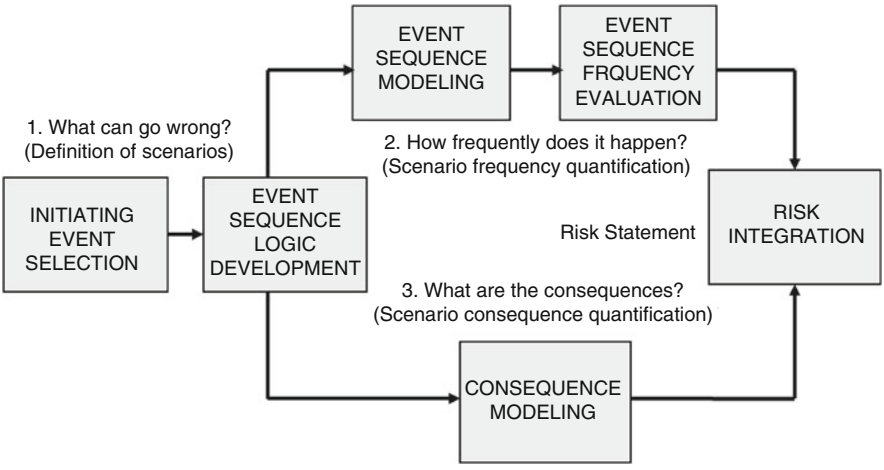

Fig. 1 Illustration of a risk assessment process (adapted from Stamatelatos 2002)

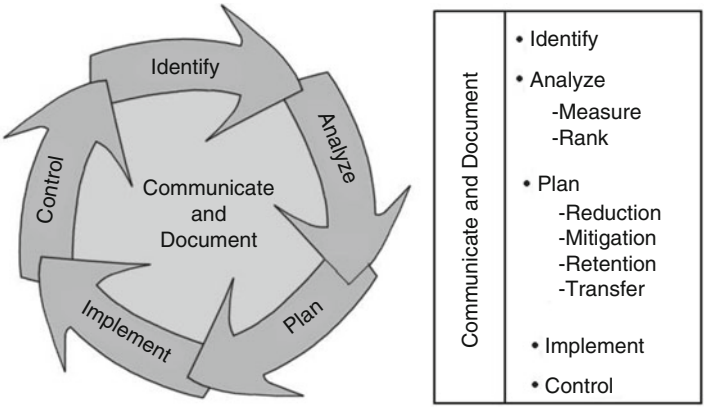

Fig. 2 Illustration of risk management process

Risk management activities encompass the following steps:

- **Identify**. States the risk in terms of conditions and consequences; capture the context of risk; e.g., what, when, where, how, and why.
- **Analyze**. Evaluates probability and severity, prioritizes and classifies groups with similar or related risks.
- **Plan**. Identifies techniques or strategies to manage the risk, including actions to mitigate, transfer or retain risks.
- **Implement**. Carries out the chosen techniques or strategies.
- **Control**. Analyzes results, decides how to proceed (re-plans, closes the risk, invokes contingency plans, continues tracking, etc.) and executes control decisions, providing feedback so that risk analysis is always updated.
- **Communicate and document**. Essential risk status is to be documented and communicated on a regular basis to the entire team.

2.3 Reliability Engineering

System is a collection of interrelated parts (components) that work together by way of some driving process. In this context, reliability is defined as the probability that an engineering system will perform its intended function satisfactorily for its intended life under specified environmental and operating conditions. 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 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 use of techniques like block diagrams or fault trees. A definition of all equipment failure and repair distributions and a statement of spare and repair strategies are necessary (IAEA 2016a).

Since component failure characteristics can be described by distributions, the system reliability is actually time-dependent (ReliaSoft 2015). Assuming an exponential life distribution, the reliability of the component i as function of time, t, $R_i(t)$, is:

$$R_i(t) = e^{-\lambda_i t}, \tag{2}$$

where λ_i is the failure rate of component i.

Mean life (or Mean Time to Failure, MTTF) can be obtained by integrating system reliability function from zero to infinity:

$$MTTF = \int_0^\infty R_i(t)dt = \int_0^\infty e^{-\lambda_i t}dt = \frac{1}{\lambda_i}. \tag{3}$$

As reliability of a system is the probability that a system will operate successfully by a given time, in dealing with repairable systems, these definitions need to be adapted to deal with the case of the renewal of systems/components. Repairable systems receive maintenance actions that restore system components when they fail. These actions change the overall makeup of the system.

Maintainability, $M_i(t)$, is defined as the probability of performing a successful repair action within a given time, t. In other words, maintainability measures ease and speed a system can be restored to its operational status after a failure occurs. In maintainability, the random variable is time-to-repair, in the same way, as time-to-failure is the random variable in reliability (Mobley et al. 2008). As an example, consider the maintainability equation for a system in which repair times are distributed exponentially. Its maintainability is given by:

$$M_i(t) = 1 - e^{-\mu_i t}, \tag{4}$$

where μ_i is repair rate.

Mean Time to Repair, MTTR, can be obtained by integrating maintainability function from zero to infinity:

$$MTTR = \int_0^\infty M_i(t)dt = \int_0^\infty e^{-\mu_i t}dt = \frac{1}{\mu_i}. \tag{5}$$

If one considers both reliability (probability an item will not fail) and maintainability (probability an item is successfully restored after failure), then an additional

metric is needed for probability a component/system is operational at a given time, (i.e., has not failed or it has been restored after failure). This metric is availability. Availability is then a performance criterion for repairable systems that accounts for both reliability and maintainability properties of a component or system. Availability, *A(t),* is defined as probability a system is operating properly when it is requested for use. In other words, availability is the probability a system will not fail or undergoing a repair action when it needs to be used. In case of a single component, *i, $A_i(t)$* is given by:

$$A_i(t) = \frac{System\ up\ time}{System\ up\ time + System\ downtime} = \frac{MTTF}{MTTF + MTTR} = \frac{\mu_i}{\lambda_i + \mu_i}. \quad (6)$$

2.4 Human Factors and Ergonomics

Human Factors It is a 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 organization machine interfaces. Efforts of human factors engineering are directed to improving operability, maintainability, usability, comfort, safety and health characteristics of systems in order to improve human and system effectiveness and to reduce the potential of injury and error (Stanton et al. 2005).

Ergonomics It is a term often used interchangeably with human factors that commonly refers to designing work environments for maximizing safety and efficiency. Ergonomics nowadays has great importance because companies have learned that designing a safe work environment can also result in greater efficiency and productivity. Today, around the world, there are many laws requiring safe work environment. Design of workplace results in a great impact on both safety and efficiency. The easier is to do a job, the more likely is to gain productivity due to greater efficiency. Analogously, the safer is to do it; also, the more likely it is to see gains in productivity due to reduced time off for injury. Ergonomics can address both these issues concurrently by maximizing workspace, equipment and activities needed to do a job (Stanton et al. 2005).

Human Reliability Assessment (HRA) HRA is a method that involves systematic prediction of potential human errors when interacting with a system. Once such errors are identified, this method tries to eliminate or reduce their occurrence, in order to maximize safety and performance of a system or facility. Results of HRA can be entered into risk management actions to reduce risk to ALARP, both by system re-design and implementation of controls and mitigations (USNRC 2005).

HRA, in general, encompasses the identification of error types, likelihood of error occurrence, opportunities to recover from errors and consequence of errors. This method should analyze current design and recommend how to mitigate errors

identified. Many reliability and risk analysis tools as FTA and ETA can help HEP steps. There are also many HRA specific techniques like THERP (Technique for Human Error Rate Prediction), SHERPA (Systematic Human Error Reduction and Prediction Approach), HEART (Human Error Assessment and Reduction Technique), CREAM (Cognitive Reliability and Error Analysis Method) and ATHEANA (A Technique for Human Event Analysis) (Calixto 2013). THERP will be briefly discussed in Sect. 4.4.

3 Integrated Framework for Assessing Safety, Reliability, Risk and Human Factors

Management systems in complex facilities like Nuclear Power Plants encompass several areas such as Quality (ISO 9001 standards), Environment (ISO 14001 standards), and Safety, Health and Risk Assessment (BS 8800 and OHSAS 18001 standards). Such management systems are often treated as independent functions within organizations. However, corresponding elements between these management systems are compatible and it is feasible integrating them. An integrated management and a systemic approach, i.e. an approach relating to the system as a whole in which the interactions among technical, human and organizational factors are fully considered, are essential to the specification and application of adequate safety measures and the fostering of a safety culture (IAEA 2016b).

3.1 Systems Theory

To understand complex systems, scientists usually try to envisage phenomena of nature and processes as simplified versions of reality known as a system. As defined, system can be envisaged as a collection of interrelated parts that work together by way of some driving process. They can be visualized as component blocks that have connections between them. Systems can be modeled using tools like block diagrams, facilitating evaluations of safety and reliability, for instance (ReliaSoft 2015).

Most systems share the same common characteristics. These common characteristics include the following (Cox and Tait 1998):

- Systems have a structure defined by its parts and processes.
- Systems are generalizations of reality.
- Systems tend to function in a same way. This involves inputs and outputs of material (energy or matter) that is then processed, causing it to change in some way.
- Various parts of a system have functional as well as structural relationships between each other.

- The fact of having functional relationships between parts suggests flow and transfer of some type of energy or matter.
- Systems often exchange energy or matter beyond their defined boundary with 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, three kinds of properties can be found:

- *Elements*—kinds of parts (things or substances) that make up a system. These parts may be hardware, software, raw materials, and persons, for instance.
- *Attributes*—characteristics of elements that may be perceived and measured. Examples: production, reliability, safety, and availability.
- *Relationships*—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 production, safety and availability.

The state of a system is defined by the value of its properties (elements, attributes, and/or relationships).

3.2 Overview of Human Factors Integration

Figure 3 can be used to support the definition the objective of integrated analysis. It shows an overview of possibilities of integration of human factors (ergonomics), life-cycle step of the project (design, implantation, operation or decommissioning), target (quality, occupational health and safety, or environmental management), and focus of analysis (safety, reliability, or risk).

3.3 Integrated Framework

Figure 4 shows the steps for the proposed methodology considering safety, reliability, risk management and human factors integrations.

Identification of a system to be analyzed is carried out with the aid of systems theory. Figure 5 illustrates a systematic model of an organization adapted to an industrial facility (Cox and Tait, 1998). The first box represents inputs into the systems and includes physical, human and financial resources, as well as service and knowledge. The transformation process integrates plant (hardware), human resources (liveware) and policies, procedures, rules, and processes (software). The

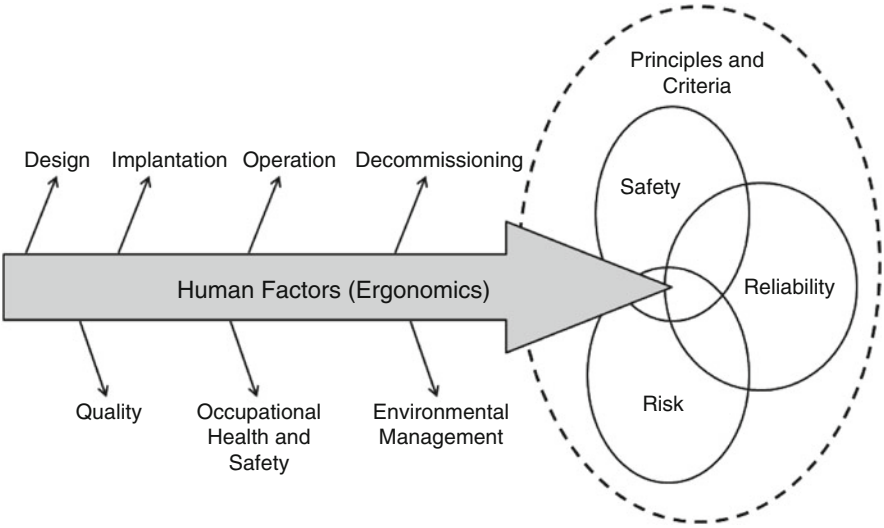

Fig. 3 Overview of framework for human factors integration (Vasconcelos et al. 2009)

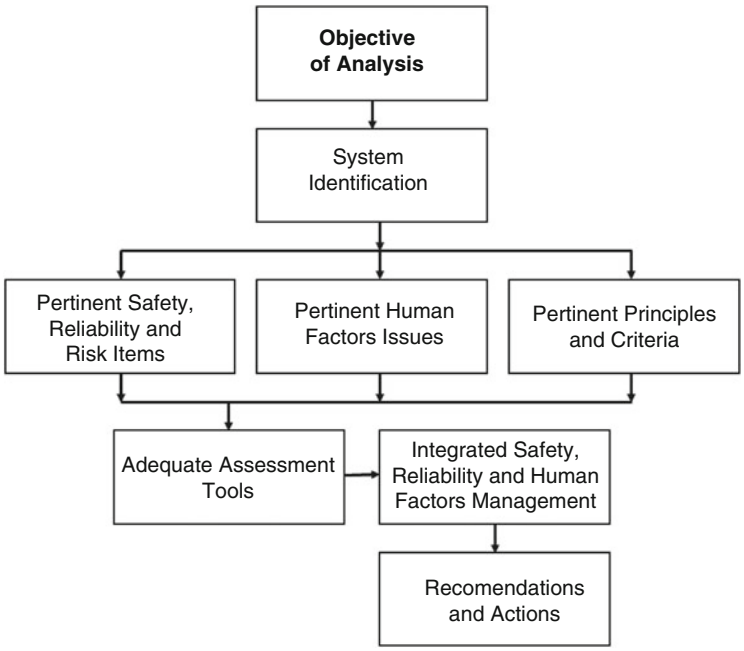

Fig. 4 Proposed methodology for safety, reliability, risk management and human factors integration (Vasconcelos et al. 2009)

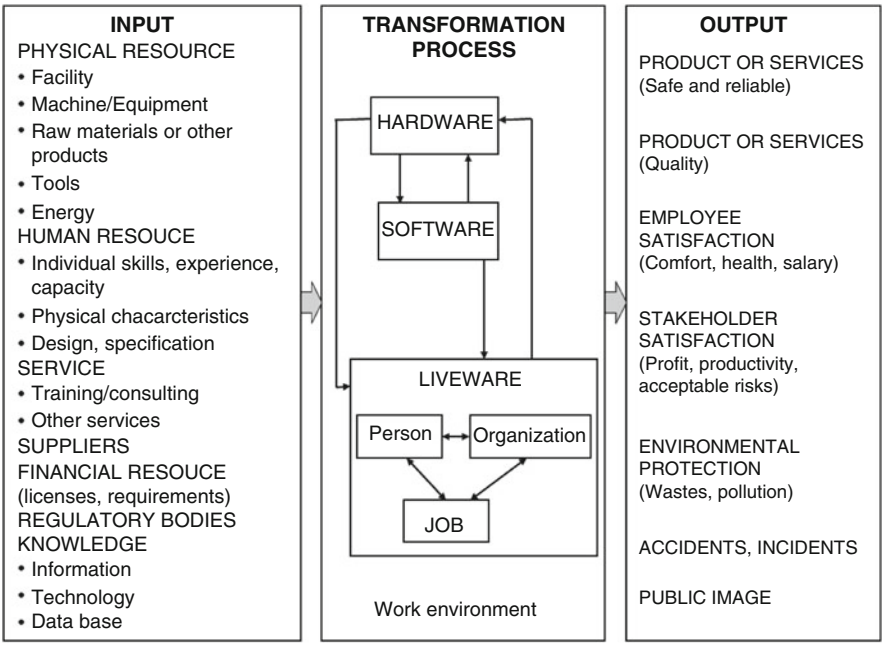

Fig. 5 Systemic model of an organization (adapted from Cox and Tait 1998)

box at right represents outputs and depending on targets of analysis, elements of quality, occupational health and safety, or environmental management can be selected.

The overview of framework for human factors integration, illustrated in Fig. 3 through the intersection of human factors (ergonomics) arrow with characteristics in focus (safety, reliability, or risk) or their intersections is best illustrated in Fig. 6. This figure illustrates some identified pertinent safety and reliability items, as well as common pertinent human factors issues. By this way, systems to be analyzed are identified systematically under all focus combination, within the life-cycle step and the required target (EUROCONTROL 2004). At each selected focus, applicable principles and criteria are chosen (examples in Table 1). Human factors to be considered in analysis are grouped in six areas in order to warrant that all issues will be considered and can be adequately prioritized. Six human factors areas and some example issues within each one are shown in Table 2. The integrated analysis can be carried out using common tools referred in Sect. 4 of this chapter.

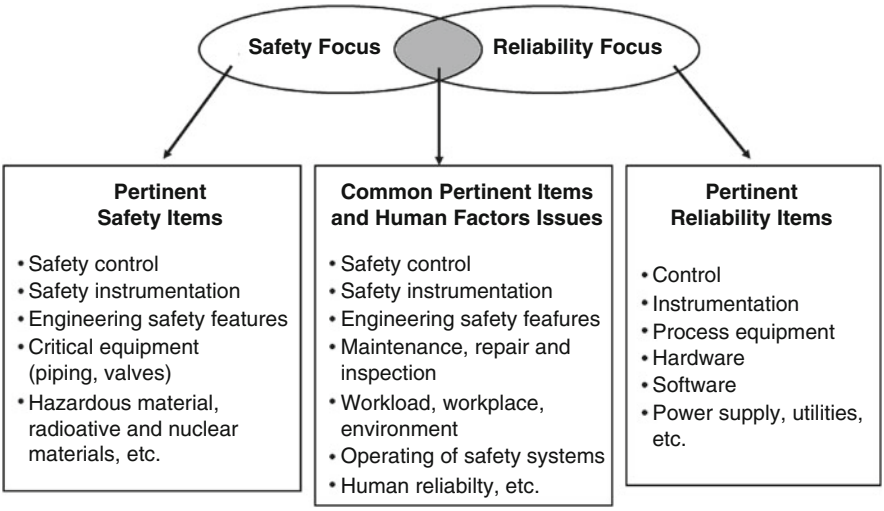

Fig. 6 Examples of pertinent items and Human Factors within an integrated safety and reliability focus (adapted from EUROCONTROL 2004)

4 Applied Models and Methods

Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), and Technique for Human Error Rate Prediction (THERP) are examples of common safety, reliability, and risk evaluation tools that can support the team in proposed integrated framework for analyzing process systems and identifying potential accidents.

4.1 Event Tree Analysis (ETA)

Modeling of accident scenarios within a risk assessment process proceeds with inductive logic and probabilistic tools called Event Trees (ETs). An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (Defence-in-depth levels), until an end-state is reached. (Stamatelatos 2002). Figure 7 illustrates an event tree for a generic initiating event and two levels of Defence-in-depth. Considering λ_{ie} as the frequency of occurrence of an initiating event, and p_1 and p_2, as the probabilities of failure of Defence-in-depth levels 1 and 2, respectively, the frequency of occurrence, *F*, for four possible accident scenarios (no-consequence, and accident scenarios 1, 2 and 3) can be calculated as shown in Fig. 7. Notice that these estimates are only valid if the events involved in each sequence are independent.

Table 1 Examples of design and analysis principles and criteria applied to safety, reliability, risk and human factors (adapted from Vasconcelos et al. 2009)

Selected focus	Principles and criteria
Safety	Fail-safe design
	Double contingency
	Single failure design
	ALARP
	Defence-in-depth
	Principles of waste management
	Licensing requirements
	Radioprotection
Reliability	Standby and redundancy
	Diversity
	k-out-of-n redundancy
	Fault tolerant systems
	Safety factors
	Availability
	Maintainability
	Sensitivity
Risk	Prevention principle
	Precautionary principle
	Protection principle
	Basic principles of nuclear energy
	Principle of limitation of risks to individuals
	Design basis accidents
	Environmental risks
	IAEA safety principles
Human factors (Ergonomics principles)	Work in neutral postures
	Reduce excessive force
	Keep everything in easy reach
	Maintain a comfortable environment
	Reduce excessive motions
	Accessibility
	Usability and affordance

4.2 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is an analytical technique, whereby an undesired state of a system is specified, usually a state that is critical from a safety or reliability standpoint. The system is then analyzed in the context of its environment and operation, to find all realistic ways in which the undesired event (called top event) can occur. Fault tree itself is a graphic model of various parallel and sequential combinations of faults that will result in the occurrence of the top event. Faults can be events that are associated with component hardware failures,

Table 2 Six human factors areas and examples of human factors issues (adapted from EUROCONTROL 2004)

Human factors area	Example issues
Human-Machine Interaction (HMI)	Input devices, visual displays, information requirements, alarm handling, HMI usability, user requirements, health risks, fatigue, distraction and concentration, noise, lighting, temperature/humidity/air quality, workplace arrangement
Organization and staffing	Staff requirements, manpower availability, human resource profile/selection criteria, job attractiveness, ageing, shift organization
Training and development	Training needs, performance/competence standards, training content, training methods and media, trainer role/responsibilities/competency, On-the-Job Training (OJT), emergency/unusual situation training, testing of training effectiveness
Procedures, Roles and responsibilities	Allocation of functions, involvement, workload, trust/confidence, skill degradation, procedure format and structure, procedure content, procedure realism, documentation
Teams and communication	Team structures/dynamics/relations, team coordination, leadership, workload communication, phraseology, national language differences, changes in communication methods, information content, types of communication
Recovery from failure	Human error potential, error prevention/ detection/recovery, detection of and recovery from system failures, error taxonomies

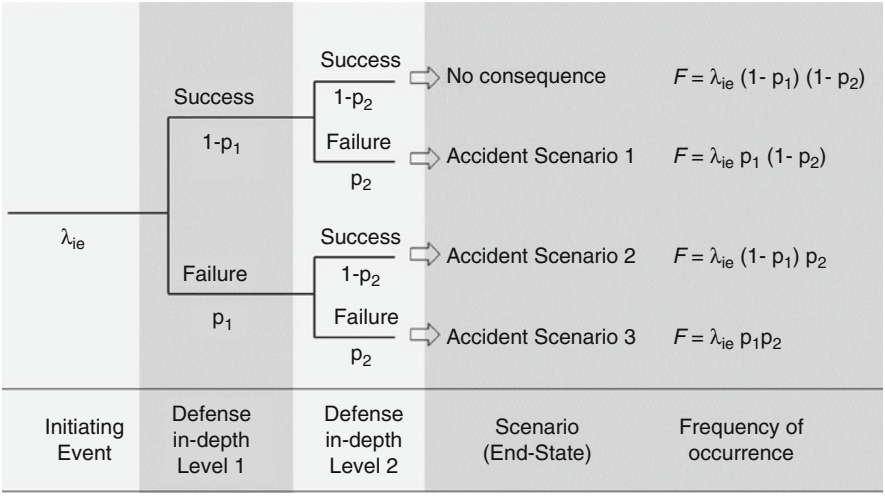

Fig. 7 Event Tree for a generic initiating event and two levels of Defence-in-depth

human errors, software errors, or any other pertinent events, which can lead to the top event. A fault tree thus depicts the logical interrelationships of basic events that lead to the top event of the fault tree (Stamatelatos 2002).

Both qualitative and quantitative evaluations can be performed with the help of fault tree technique. Fault tree itself is a qualitative assessment of events and shows

relationships that lead to the top event. In constructing fault tree, significant insights and understanding are gained concerning causes of the top event. Additional evaluations serve to further refine of the information that fault tree provides.

Qualitative evaluations basically transform a fault tree into logically equivalent forms that provide more focused information. The principal qualitative results obtained are the Minimal Cut Sets (MCSs) of the top event. A cut set is a combination of basic events that can cause the top event. An MCS is the smallest combination of basic events that result in the top event. MCSs relate the top event directly to the basic event causes. A set of MCSs for the top event constitutes all ways that basic events can cause the top event. Because the excessively large number of possible combinations of basic events in MCS, computer programs are necessary to identify MCS. For instance, in a system with 100 basic events there are 100 possible cut sets of one basic event, 161,700 cut sets with two basic events, 3,921,225 cut sets with three basic events, and so on. It is virtually impossible a manual review of these possible combinations and check if they are MCSs. Specialized computer programs are then necessary in order to obtain MCS for more complex fault trees (ReliaSoft 2015).

Quantitative evaluations of a fault tree consist of determining the top event probabilities and relative importance of basic events. Uncertainties in any quantified result can also be determined. Fault trees are quantified, typically, by calculating the probability of each MCS and by summing these probabilities, if the events in MCS are independent. Different types of probabilities can be calculated for different applications. In addition to a constant probability value that is typically calculated, time-related probabilities can be calculated providing the probability distribution of the time of first occurrence of the top event. Occurrence rates and availabilities of top events can also be calculated. These characteristics are particularly applicable if the top event is a system failure. Two examples of fault trees representing series and parallel systems respectively are shown in Fig. 8.

Top event probability is calculated from a fault tree using the probabilities that are input for the basic events. Depending on the specific top event definition, the top event probability can be the probability of the top event occurring during a mission time or in a given period of time, i.e., the probability that the top event exists at a given point in time. In some cases, the top event probability can be also the frequency of the top event occurring or the expected number of occurrences of the top event in some time interval. This only occurs if the inputs are basic event frequencies or expected numbers of occurrences.

Using the set theory concepts (Stamatelatos 2002) the probability equations of the two fault trees in Fig. 8 can be expressed as:

$$\mathrm{P(A\ or\ B)} = \mathrm{P(A \cup B)} = \mathrm{P(A)} + \mathrm{P(B)} - \mathrm{P(A \cap B)}, \tag{7}$$

$$\mathrm{P(A\ and\ B)} = \mathrm{P(A \cap B)} = \mathrm{P(A|B)\ P(B)} = \mathrm{P(B|A)\ P(A)}, \tag{8}$$

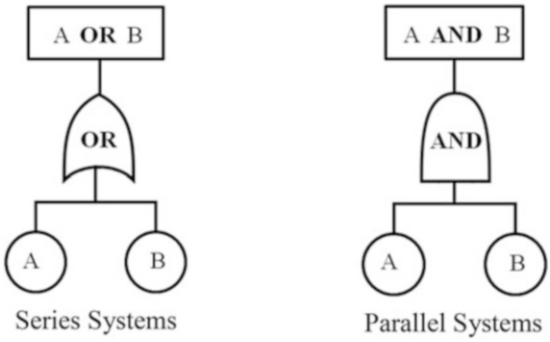

Fig. 8 Fault trees representing series and parallel systems

where P(A) and P(B) are the independent probabilities of basic events, and P(A|B) and P(B|A) are the conditional probabilities. If events A and B are independents, Eqs. 7 and 8 become:

$$\mathrm{P(A\ or\ B)} = \mathrm{P(A \cup B)} = \mathrm{P(A)} + \mathrm{P(B)} - \mathrm{P(A)\ P(B)}, \tag{9}$$

$$\mathrm{P(A\ and\ B)} = \mathrm{P(A \cap B)} = \mathrm{P(A)\ P(B)}. \tag{10}$$

4.3 Reliability Block Diagrams (RBD)

An overall system reliability prediction can be made by looking at the reliabilities of the components that make up the whole system or product. A Reliability Block Diagram (RBD) is a graphical representation of the components of a system and how they are related or connected (ReliaSoft 2015). RBDs for series and parallel systems are shown in Fig. 9.

In a series configuration, failure of any component results in failure of the entire system. In most cases, when considering complete systems at their basic subsystem level, it is found that these are arranged reliability-wise in a series configuration. A failure of any of these subsystems will cause a system failure. In other words, all of components in a series system must succeed for the system to succeed.

The reliability of a series system, R_s, is the probability that all n components in the system succeed. Therefore, the reliability of the system is then given by:

$$\begin{aligned} R_s &= P(X_1 \cap X_2 \cap \ldots \cap X_n) \\ &= P\left(X_1\right)P(X_2|X_1)P\left(X_3|X_1X_2\right)\ldots P\left(X_n|X_1X_2\ldots X_{n-1}\right) \end{aligned} \tag{11}$$

where X_i is the event of component i being operational,
$P(X_i)$ is probability that component i is operational, and
$P(X_i\ |X_1X_2\ X_3\ \ldots\ X_{i-1})$ is conditional probability.

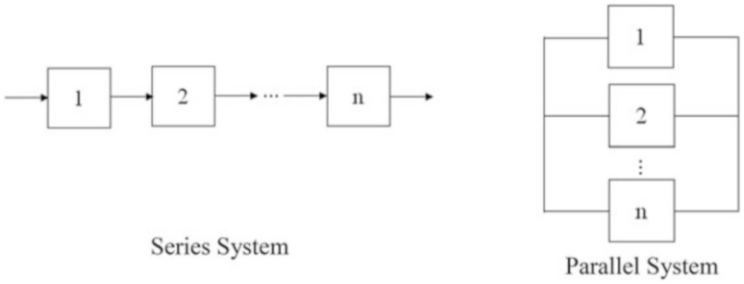

Fig. 9 Reliability block diagrams representing series and parallel systems

In the case where failure of a component affects failure rates of other components, the conditional probabilities in equation above must then be considered.

However, in the case of independent components, the equation above becomes:

$$R_s = P(X_1)P(X_2)P(X_3)\ldots P(X_n) = R_1R_2R_3\ldots R_n, \tag{12}$$

where R_i is the reliability of component i.

In a parallel configuration, at least one of the components must succeed for the system to succeed. For this reason, components in parallel are also referred to as redundant components. Redundancy is a very important method of improving system design and reliability.

Probability of failure, or unreliability, Q_p, for a system with n parallel components is the probability that all components in the system fail. Therefore, the unreliability of a parallel system is then given by:

$$\begin{aligned} Q_p &= P(x_1 \cap x_2 \cap \ldots \cap x_n) \\ &= P(x_1)P(x_2|x_1)P(x_3|x_1x_2)\ldots P(x_n|x_1x_2\ldots x_{n-1}), \end{aligned} \tag{13}$$

where x_i is the event of failure of component i,

$P(x_i)$ is the failure probability of component i, and

$P(x_i|x_1x_2\ldots x_{i-1})$ is conditional probability.

In the case where the failure of a component affects failure rates of other components, the conditional probabilities in equation above must be then considered.

However, in the case of independent components, equation above becomes:

$$Q_p = P(x_1)P(x_2)P(x_3)\ldots P(x_n) = Q_1Q_2Q_3\ldots Q_n\,. \tag{14}$$

So, the reliability of a parallel system, R_p, is then given by:

$$R_p = 1 - Q_p = 1 - (1 - R_1)(1 - R_2)(1 - R_3)\ldots(1 - R_n). \tag{15}$$

4.4 Technique for Human Error Rate Prediction (THERP)

Technique for Human Error Rate Prediction (THERP) is the most structured, detailed, and widely used Human Reliability Analysis (HRA) method in PRAs for NPPs. Swain and Guttmann (1983) define THERP as a method to predict Human Error Probabilities (HEP) and to evaluate the degradation of a man-machine system. This degradation can be caused by human errors alone or in connection with equipment malfunctions, operational procedures and practices, or other system and human characteristics that influence system behavior.

THERP analysis encompasses the following steps (Calixto 2013):

- Understanding the problem to be assessed to see if THERP is the best tool for finding the answer.
- Understanding of human error context and how human tasks influence activity or system being assessed.
- Listing and analyzing the related human tasks.
- Estimating error probabilities for each task using database, expert opinion or literature data.
- Estimating the final HEP for the whole activity using a THERP tree event.
- Proposing recommendations to reduce HEP.
- Estimating the effects of recommendations on HEP after they are implemented.

THERP depends heavily on a detailed and properly performed task analysis. Upon completion of the task analysis, Human Interaction (HI) is logically represented by an HRA event tree, which is used to combine HEPs associated with various HI tasks/subtasks, including cognitive response and action response. Figure 10 shows an example of an HRA event tree for an HI with two tasks A and B (Swain and Guttmann 1983).

As can be seen in Fig. 10, the probability of success P(S) or failure P(F) of a task is the sum of the probabilities for respective sequences. So, for the series system:

$$\mathrm{P(S)} = \mathrm{a(b|a)}, \tag{16}$$

$$\begin{aligned}\mathrm{P(F)} &= 1 - \mathrm{a(b|a)} \\ &= \mathrm{a(B|a)} + A\mathrm{(b|A)} + \mathrm{A(B|A)}.\end{aligned} \tag{17}$$

For the parallel system:

$$\begin{aligned}P\mathrm{(S)} &= 1 - \mathrm{A(B|A)} \\ &= \mathrm{a(b|a)} + \mathrm{a(B|a)} + \mathrm{A(b|A)},\end{aligned} \tag{18}$$

$$P\mathrm{(F)} = \mathrm{A(B|A)} \tag{19}$$

Many dependency models were developed to account for potential dependencies among multiple tasks or human interactions (Zhou et al. 2017; Su et al. 2015). In the model proposed by Swain and Guttmann (1983), the dependency level between two HI/tasks is broken into five levels, as shown in Table 3: Zero Dependence (ZD),

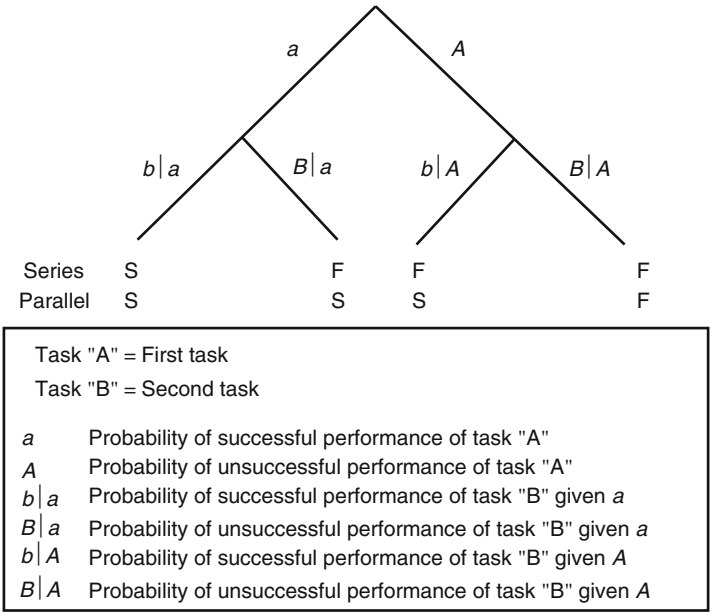

Fig. 10 HRA event tree example for series or parallel system (adapted from Swain and Guttmann 1983)

Table 3 Dependence model for Human Error Probability System (Swain and Guttmann 1983)

Dependency level	Dependent probability
ZD—Zero Dependence	HEP_n
LD—Low Dependence	$\frac{1+19HEP_n}{20}$
MD—Moderate Dependence	$\frac{1+6HEP_n}{7}$
HD—High Dependence	$\frac{1+HEP_n}{2}$
CD—Complete Dependence	1

Low Dependence (LD), Moderate Dependence (MD), High Dependence (HD), and Complete Dependence (CD). In Table 3 HEP_n is the HEP for Task n given Zero Dependence to Task $n-1$.

Many authors consider the assessment of dependence level in THERP highly subjective and dependent of a considerable amount of expert judgment. The criticisms also include the absence of specific guidance that makes the use of THERP dependence method difficult and the results may lack traceability and repeatability (Su et al. 2015). Despite such methodology does not consider human performance-shaping factors that cause human error, which is a characteristic of first generation of HRA methodologies, the longevity of THERP is a testament of its significance. THERP started the field of HRA, and newer methods can be seen as extensions of this pioneering work (Boring 2012).

5 Application Example

In this section, a simple representative example is presented in order to illustrate the benefits of integrated engineering approach to safety, reliability, risk management and human factors for a generic Loss of Coolant Accident (LOCA) in a Nuclear Power Plant (NPP).

5.1 Objective of Analysis

The objective of analysis is to improve Non-destructive Inspection (NDI) process of pipe segments of a core cooling system of a NPP, reducing LOCA probability, increasing system reliability and managing risks through acting on human factors issues. The life-cycle focus of analysis is the operation phase of the NPP.

5.2 System Identification

Figure 11 shows a simplified block diagram of a generic core cooling system (primary system) of a NPP and pertinent safety and reliability items that act as DID levels in case of a LOCA.

In this example, LOCA consequences are prevented or mitigated through actuating of safety systems, flaw detection, leak detection, or maintenance and repair. Piping flaws can be identified using NDI techniques, like ultrasonic inspection. Maintenance and repair actions can prevent leak and avoid accidents. If the NDI method fails, a leak will occur and could be detected by leak detection systems. The leak detection system can have the functions of initiating safety, maintenance and repair actions, mitigating the consequences.

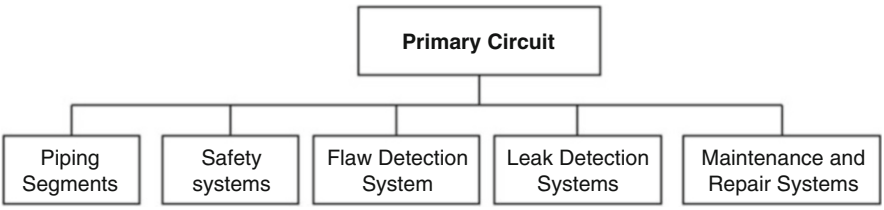

Fig. 11 Simplified block diagram of a primary circuit of a NPP

5.3 Pertinent Safety, Reliability and Risk Items

The identified pertinent safety items are piping segments, safety instrumentation, flaw detection systems, leak monitoring systems, and engineering safety features (safety systems). Reliability items include piping segments, control instrumentation and engineering safety features. Common pertinent safety and reliability items include piping segments, safety instrumentation, and engineering safety features. Risk management of a generic LOCA in the primary circuit is the pertinent risk item.

5.4 Pertinent Human Factors Issues

Table 4 shows examples of human factors issues related to a generic LOCA analysis, taking into account the six human factors areas defined in Table 2.

5.5 Pertinent Principles and Criteria Issues

According the pertinent principles listed in Table 1, the following issues were identified to the selected application example.

The pertinent safety principle and criteria of the operation phase of NPP is Defence-in-depth (DID) against LOCA. DID level 1 includes the use of operational

Table 4 Examples of human factors issues related to generic LOCA

Human factors area	Example issues
Human-Machine Interaction (HMI)	Automatic/manual In-service Inspection (ISI) systems, leakage alarm handling, ISI system usability, user requirements, health risks, workplace accessibility, redundant detection systems
Organization and staffing	Staff requirements for ISI, operator capability and limitation, job attractiveness
Training and development	Training needs, On-the-Job Training (OJT), testing of training effectiveness, ISI training, maintenance and repair training
Procedures, roles and responsibilities	ISI planning, ISI procedure, complementary ISI procedures due to task complexity, maintenance and repair procedure, leak detection procedure
Teams and communication	Team coordination, feedback in sustaining effective inspection performance, communication of existing plant data, communications of ISI and leak detection groups to maintenance and repair, report inspection data, methods and results, manual/automatic recording
Recovery from failures	Human error potential due to task complexity of ISI, supervisory tasks, detection and recovery from inspector errors

experience, planning of safety improvements, maintenance and training. DID level 2 includes ISI and leakage detection. Automatic and manual actuation of safety systems are part of DID level 3. The pertinent reliability principle and criteria are maintainability of piping segments and redundancy of leakage detection and safety systems. LOCA is the Design Basis Accident (DBA) criteria considered in risk management and some human factors should be considered in order to reduce risks. Workspace accessibility, usability of ISI, leakage, maintenance and repair systems, as well as cognitive ergonomics features of related operating plans and procedures are some pertinent criteria for human factors that can be cited.

5.6 Adequate Assessment Tools

In order to analyze safety, reliability, risk management and human factors for a generic LOCA in a NPP, using the proposed integrated engineering approach, a set of tools should be selected.

Sequences of plant end-states after an initiating event involving flaw occurrence in a pipe segment of primary circuit and the actuation of DID levels can be analyzed using Event Tree Analysis (ETA) technique.

Occurrence of piping rupture (that can cause LOCA or core damage) can be analyzed qualitative or quantitatively using Fault Tree Analysis (FTA) technique, which can involve hardware failures and human errors.

Evaluation of human errors occurring through the completion of selected complex tasks as NDI and typical action sequence for inspection can be carried out using THERP. Human performance issues can then be analyzed and improvements of NDI process of pipe segments of NPP can be suggested. In this example, only a qualitative use of these tools is done.

5.7 Integrated Assessment

Considering as pertinent safety items the pipe segments, NDI, leakage detection and safety systems, an event tree considering as initiating event "Flaw occurrence in a pipe segment" is shown in Fig. 12. This example is based in a previous work of Holmberg and Nirmark (2008) related to risk-informed assessment of Defence-in-depth of a generic LOCA.

The following event sequences were considered. The occurrence of the initiating event can be avoided by DID level 1, as use of operational experience, planning of safety improvements, maintenance and training. If the initiating event occurs, the flaw can be identified by In-service-Inspection (ISI), using NDI methods (DID level 2). If the NDI method fails, a leak will occur. This leak, assumed to be a small LOCA, can propagate to a large LOCA if the leakage detection system fails. Both

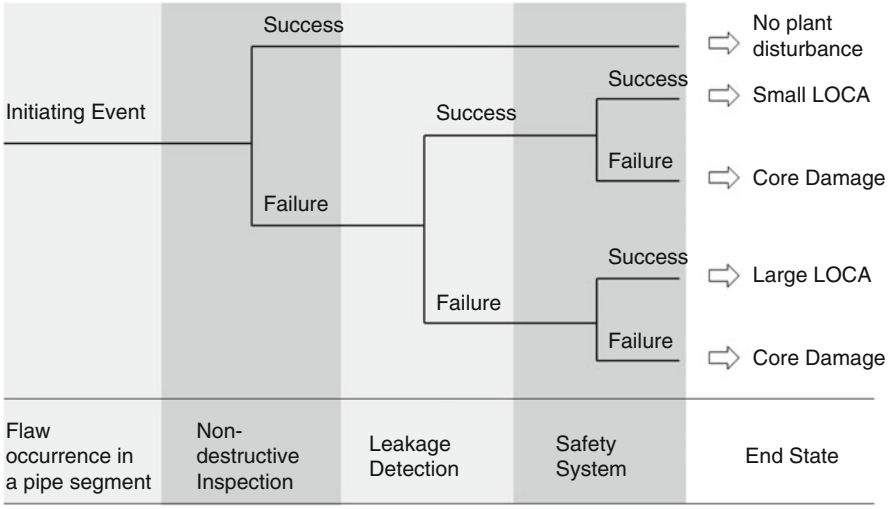

Fig. 12 Example of a simple event tree for LOCA (adapted from Holmberg and Nirmark 2008)

the small and large LOCA can lead to Core Damage, if safety systems fail. The leak detection system and the safety systems are DID level 3 methods in this example.

A fault tree was constructed in order to evaluate qualitatively the likelihood of occurrence of piping rupture taking into account the reliability of ISI and leak detection systems. Considering "Piping failure" as top event and ranking piping states into four types, "successive state", "detectable flaw state", "detectable leakage state" and "failure state", a fault tree model can be constructed as shown in Fig. 13. The descriptions of the primary events of the fault tree are listed in Table 5. The parameters expressing primary events rates in fault tree depends on both historical generic component data and plant specific data. Among the necessary data for estimating primary event parameters, can be highlighted: effectiveness rate to inspect flaw, piping flaw probability, piping rupture probability, effectiveness rate of leakage detection, and leakage occurrence rate. A qualitative evaluation of such fault tree can be performed through identification of Minimal Cut Sets (MCS), i.e., the minimal combination of events that can cause the top event occurrence.

In order to estimate the effectiveness rate to inspect flaw, a THERP event tree evaluating the likelihood of human errors occurring throughout the completion the task of piping inspection is constructed and shown in Fig. 14.

The tasks considered in this THERP are: define inspection strategy, select inspection technique, prepare equipment and procedures, acquire data, analyze data, record data, and report inspections (Parris 1988). The Human Error Probability (HEP) of NDI task depends on HEP for each action of the sequence, and they are described as follows.

Define Inspection Strategy To be effective, an inspection must be based on existing information about location, geometric profile, frequency of inspection,

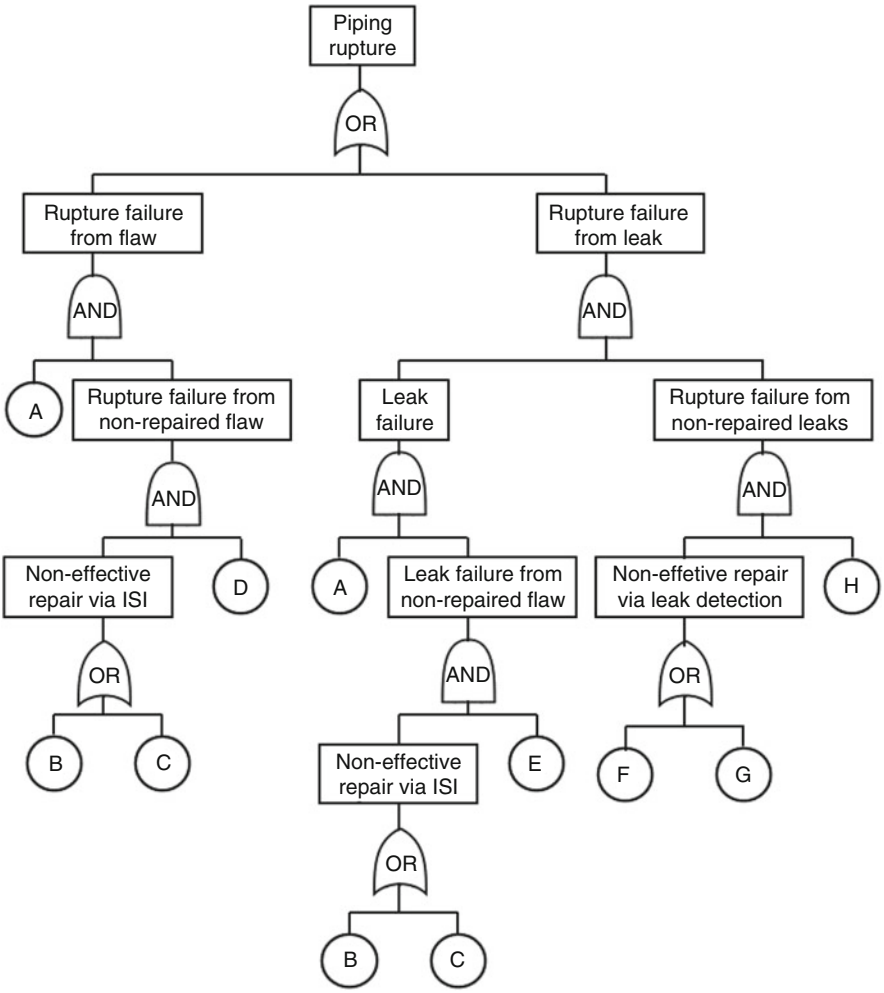

Fig. 13 Fault tree model for piping failure (adapted from Vasconcelos et al. 2016)

Table 5 Description of the primary events of fault tree of Fig. 13

Symbol	Description
A	Flaw occurrence
B	Non-effective repair
C	Non-effective ISI
D	Rupture failure given flaw
E	Leak failure given flaw
F	Non-effective repair
G	Non-effective leak detection
H	Rupture failure given leak

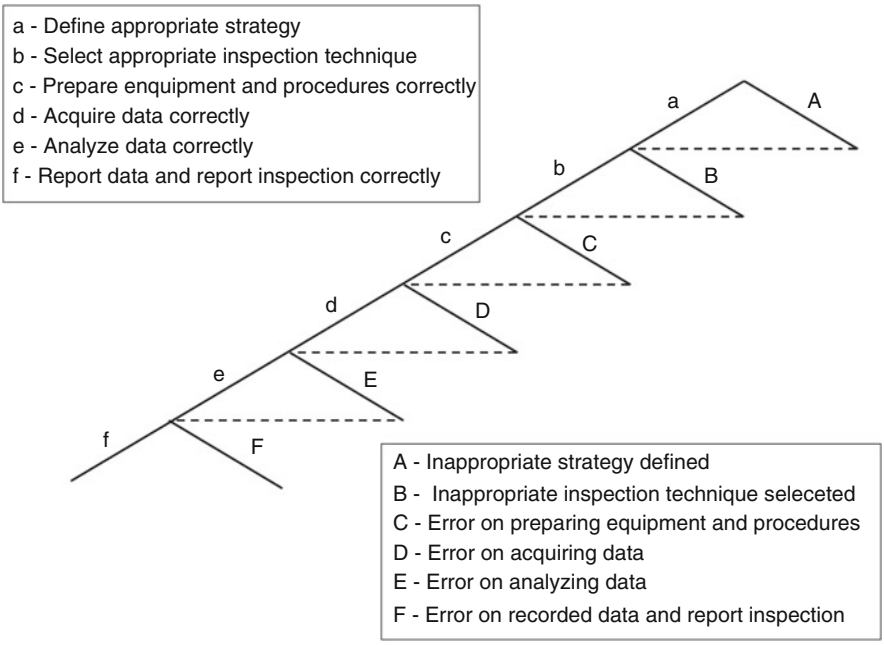

Fig. 14 THERP for evaluating the probability of human errors occurring throughout the completion the task of piping inspection

history, risks, etc., in order to define inspection strategy. Critical human function must be performed more automatically and remotely, reducing radiation exposure and improving results of inspections.

Select Inspection Technique The selection of most effective inspection technique for flaw detection involves considerations of geometry and materials properties, and detailed procedures to be carefully followed.

Prepare Equipment and Procedures The preparing involves calibration, equipment set and tests, establishing team coordination, and following written and trained procedures.

Acquire Data Acquiring data needs explicitly written and trained procedures, i.e., specific steps must be prescribed and followed invariably. Sometimes this is not possible due to task complexity and the number of variables and conditions that must be addressed in ISI.

Analyze Data Interpreting flaw data and discriminating them from another signal depends on many equipment sets, inspector skill and training, and accurate procedures.

Record Data and Report Inspections In manual data recording and inspection reporting, data such as, relevant parameters and defect indications and locations,

are collected and analyzed at the same time, increasing error possibilities. Automatic data recording and analyses do not need proceed simultaneous with data collection, reducing HEP.

5.8 *Improvements on Safety, Reliability and Risk Management*

A quantitative assessment of safety, reliability and risk including human factors for complex tasks as NDI in this application example is not easy to do, because it depends on specific data and HEP for each step of THERP, which are usually unavailable. However, the qualitative integrated assessment illustrated in this application example can be helpful for understanding the human error context and identify many improvements that can be made in human factors issues and, accordingly, in safety, reliability and risk management.

Among the improvements of generic NDI process of pipe segments of a core cooling system of a Nuclear Power Plant (NPP) can be highlighted:

- **Definition of an optimal strategy of inspection**. There are different possible inspection strategies involving locations, techniques, frequencies, etc. A Risk-Based Inspection approach, for instance, prioritizing locations and higher risks systems should be considered (Soares et al. 2015).
- **Development of guidelines for operator-control interface design**. Use of human-factors principles and criteria in design of new inspection systems. This guidelines can be used to design more effective systems, and reduce the time and expense required for inspection tasks (Stanton et al. 2005).
- **Reduction of complexity of manual NDI**. Manual NDI are typically too complex to produce reliable results, because many variable must be addressed in order to preparate and conduct inspections. In NPP, the task is usually performed in radioactive areas, with time pressure and protective clothes that difficult the tasks. Manual NDI should only be peformed where accessibility limitations preclude automatic ones (Parris 1988).
- **Application of human factors principles and criteria to the preparation of written instructions**. NDI procedures usually offer many opportunities for human performance errors. Many inspections are in general, similar, but different in significant details. The principal means of countering error potentials is to provide understandable, action-oriented instructions combined with labels on controls and indicators, for instance, taking into account ergonomic principles as usability and accessibility. As an example, instructions that emphasizes graphics and decision tables rather than narrative presentation of information are less error-prone (Stanton et al. 2005).
- **Collection and analysis of NDI performance data**. Many studies have shown that inspection accuracies are typically lower than expected. It is necessary to know what might be done to redesign the tasks or instrumentation to yield better

results. Collected performance data should be interpreted and transformed into specific recommendations to task, instrumentaion, and training improvements (Parris 1988).

- **Development of method for feedback information of effectiveness of NDI**. Task performance tends to deteriorate if feedback is lacking or not adequate. Complete, accurate, and timely information on task performance is one of the best ways to improve and sustain human performance of complex task as NDI and to better the risk management (IAEA 2001).

6 Conclusions

This chapter proposes and applies a systematic methodology for integrated analysis of safety, reliability, risk and human factors. Interactions among technical, human and organizational factors can be fully considered by using systems theory.

The systematic approach directs the analysis, starting from the selection of applicable life-cycle step 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 applicable principles and criteria, and using common applicable safety, reliability, and risk tools. Merging of these various assessment and management systems could reduce duplication of efforts and costs, and increase the effectiveness of management systems, among others.

Main terminology and concepts related to safety assessment, risk management, reliability engineering, human factors and ergonomics were presented. Concepts of systems theory, supporting the integrated framework for assessing safety, reliability, risk and human factors, were also introduced. Mathematical and statistical basis for assessment of reliability, unreliability, maintainability and availability were described. The systematization of the application of the methodology was driven by the use of figures and tables, helping the definition of objectives of analysis, detailing their steps, as well as defining the pertinent items, principles and criteria applied to safety, reliability and human factors.

Common tools used in integrated analysis, as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Event Tree Analysis (ETA), and Technique for Human Error Rate Prediction (THERP), including mathematical and statistical basis, were briefly described. So, an event tree for a generic initiating event and two levels of Defence-in-depth was presented, showing the frequency of occurrence estimation for possible accident scenarios, as function of frequency of occurrence of initiating event and probabilities of failure of Defence-in-depth levels. Concepts of Fault Trees and Reliability Block Diagrams were presented, including theoretical basis for qualitatively and quantitatively assessment of likelihood of failures and reliability for series and parallel systems. THERP was also presented through a Human Reliability Analysis event tree for series and parallel systems, illustrating

how to estimate the probability of successful and unsuccessful performance of tasks.

Finally, a simple representative example was presented, in order to illustrate the benefits of the integrated engineering approach to safety, reliability, risk management and human factors for a generic LOCA in a Nuclear Power Plant (NPP). The qualitative assessment demonstrated the benefits of using the proposed integrated approach. The application example illustrated an integrated assessment of safety, reliability and risks, including human factors for a complex task of Non-destructive Inspection (NDI) of piping segments of primary circuit of a NPP. A quantitative assessment of complex tasks as NDI involved in the application example is difficult to do, because it depends on specific data and human error probabilities for each step of developed THERP, which are usually unavailable. However, this qualitative integrated assessment was helpful for understanding the human error context and identify many improvements that can be made in human factors issues and, consequently, in safety, reliability and risk management. Some generic improvements for NDI process of piping segments of primary circuit were then presented for the purpose of reducing LOCA probabilities.

Acknowledgments The authors would like to thank the following Brazilian institutions that supported the writing of this chapter: Nuclear Technology Development Center (CDTN), Brazilian Nuclear Energy Commission (CNEN), Financier of Studies and Projects (FINEP), Brazilian Council for Scientific and Technological Development (CNPq), and Minas Gerais State Foundation for Research Development (FAPEMIG).

References

ANS. American Nuclear Society (2016) Glossary of definitions and terminology. American Nuclear Society, La Grange Park, IL, 186 p

Boring RL (2012) Fifty years of THERP and human reliability analysis. Proceedings of the 11th probabilistic safety assessment and management conference. International—PSAM11, Idaho Falls, ID, June

Calixto E (2013) Gas and oil reliability engineering. Modeling and analysis. Elsevier, Amsterdam, 545 p

Christensen FM, Andersen O, Duijm NJ, Harremoës P (2003) Risk terminology—a platform for common understanding and better communication. J Hazard Mater 103:181–203

Cox S, Tait R (1998) Safety, reliability and risk management: an integrated approach, 2nd edn. Butterworth-Heinemann, Oxford, 325 p

EUROCONTROL. European Organization for the Safety of Air Navigation (2004) The human factors case: guidance for human factors integration—HRS/HIS-003-GUI-01. Brétigny, 114 p

Holmberg JE, Nirmark J (2008) Risk-informed assessment of Defence-in-depth, LOCA example phase 1: mapping of conditions and definition of quantitative measures for the Defence-in-depth levels. Rev 0. VTT Technical Research Centre, Espoo, Finland, 42 p (SKI Report 2008:33)

HSE. Health and Safety Executive (2017) Principles and guidelines to assist HSE in its Judgements that duty-holders have reduced risk as low as reasonably practicable. Retrieved 7 Apr 2017, from http://www.hse.gov.uk/risk/theory/alarp1.htm

IAEA. International Atomic Energy Agency (2001) Risk management: a tool for improving nuclear power plant performance. Vienna, 88 p (IAEA-TECDOC-1209)
IAEA. International Atomic Energy Agency (2009) Deterministic safety analysis of nuclear power plants. Specific Safety Guide N° SSG-2. Vienna, 84 p
IAEA. International Atomic Energy Agency (2012). IAEA report on protection against extreme earthquakes and tsunamis in the light of accident of the Fukushima Daiichi Nuclear Power Plant. International Expert Meeting. Vienna
IAEA. International Atomic Energy Agency (2016a) Safety glossary terminology used in nuclear safety and radiation protection. Vienna, 219 p
IAEA. International Atomic Energy Agency (2016b) Leadership and management for safety. General Safety Requirements No. GSR Part 2. Vienna (STI/PUB/175)
Lees FP (2012) Loss prevention in the process industries: hazard identification, assessment and control, 4th edn, 3 vol. Butterworth-Heinemann, Oxford
Mobley RK, Higgins LR, Wikoff DJ (2008) Maintenance engineering handbook, 7th edn. McGraw Hill, New York, NY, 1244 p
NAS & USNRC. National Academy of Sciences and U.S. Nuclear Regulatory Commission (2014) Lessons learned from the Fukushima nuclear accident for improving safety of U.S nuclear plants. National Academies Press, Washington, DC, 394 p
Parris DH (1988) Human performance in non-destructive inspections and functional tests. EPRI NP-6052. Final Report. Palo Alto, CA, October
ReliaSoft (2015) System analysis reference: reliability, availability and optimization. ReliaSoft Publishing, Tucson, AZ
Soares WA, Vasconcelos V, Rabello EG (2015) Risk-based inspection in the context of nuclear power plants. Proceedings of the International Nuclear Atlantic Conference—INAC 2011, São Paulo, October 4–9
Stamatelatos M (2002) Probabilistic risk assessment procedures guide for NASA managers and practitioners—version 1.1. Office of Safety and Mission Assurance, NASA Headquarters, Washington DC, 323 p
Stanton N, Hedge A, Brookhuis K, Salas E, Hendrick H (2005) Handbook of human factors and ergonomics methods. CRC Press, Boca Raton, FL, 685 p
Su X, Mahadevan S, Xu P, Deng Y (2015) Dependence assessment in human reliability analysis using evidence theory and AHP. Risk Anal 35(7). doi:10.1111/risa.12347
Swain AD, Guttmann HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278. U.S. Nuclear Regulatory Commission
USNRC. U.S. Nuclear Regulatory Commission (1975) WASH-1400—Reactor Safety Study, NUREG-75/014, Washington, DC
USNRC. U.S. Nuclear Regulatory Commission (2001) Integrated safety analysis—guidance document. NUREG-1513. Office of Nuclear Material Safety and Safeguards, Washington, DC, 65 p
USNRC. U.S. Nuclear Regulatory Commission (2005) Good Practices for implementing Human Reliability Analysis (HRA). NUREG-1792. Washington, DC, 103 p
USNRC. U.S. Nuclear Regulatory Commission (2011) An approach for using probabilistic risk assessment in risk-informed decisions on plant specific changes to the licensing basis. Regulatory Guide 1.174—Revision 2. Washington, DC, 37 p
USNRC. U.S. Nuclear Regulatory Commission (2013) Glossary of risk-related terms in support of risk-informed decision-making. NUREG 2122. Washington, DC, 187 p
USNRC. U.S. Nuclear Regulatory Commission (2017) Full-text glossary. Retrieved 31 Mar 2017 from https://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html
Vasconcelos V, Silva EMP, Reis SC, Costa ACL (2009). Safety, reliability, risk management and human factors: an integrated engineering approach applied to nuclear facilities. Proceedings of the International Nuclear Atlantic Conference—INAC 2009, Rio de Janeiro, , September 27–October 5

Vasconcelos V, Soares WA, Costa ACL, Rabello EG, Marques RO (2016) Evaluation of piping reliability and failure data for use in risk-based inspections of nuclear power plants. Proceedings of "Congresso Brasileiro de Engenharia e Ciência dos Materiais", 12th CBECIMAT, Natal, November 6–10

WHO. World Health Organization (2004) IPCS risk assessment terminology. International Programme on Chemical Safety (ICPS). World Health Organization, Geneva, 122 p

Zhou X, Deng X, Deng Y, Mahadevan S (2017) Dependence assessment in human reliability analysis based on D numbers and AHP. Nucl Eng Des 313:243–252

Vanderley de Vasconcelos was born in Brazil, in 1956. He received the B.E. degree in Electrical Engineering from the Federal University of Uberlândia, Brazil, in 1978, his M.Sc. degree in Nuclear Science and Technology, in 1985, and his Ph.D. degree in Metallurgical and Mining Engineering from the Federal University of Minas Gerais, Belo Horizonte, Brazil, in 1997. He has experience in system analysis, reliability, probabilistic risk assessment, accident analysis, environmental management, and licensing of radioactive and nuclear facilities. He was head of the Department of Environment, Waste and Radiation Protection, coordinating a variety of environmental and nuclear licensing processes. Since 2006, he has been Professor of Production Engineering Department at Itaúna University Foundation, Itaúna, Brazil, and his research interests cover industrial risk management, ergonomics, and occupational safety engineering. He is currently senior researcher in the Nuclear Technology Development Center, a research institute from the Brazilian Nuclear Energy Commission.

Wellington Antonio Soares was born in Brazil on April 16, 1950. He received the B.E. degree in Civil Engineering from the University of Brasília, Brasília, Brazil, in 1975, his M.Sc. degrees in Nuclear Science and in Engineering of Structures in 1983 and 1991, respectively, from the Federal University of Minas Gerais, Belo Horizonte, Brazil, and the Ph.D. degree in Nuclear Technology from the University of São Paulo, São Paulo, Brazil, in 1999. He has experience in areas such as nuclear power plants licensing, stress analysis and mechanical vibrations, fracture mechanics, design of explosion-resistant structures, photoelasticity and risk-based inspection in nuclear facilities. He has also experience in management and in social communication. He coordinated the 10th Meeting on Nuclear Applications held in Belo Horizonte, Brazil, in 2011. He is currently senior researcher in the Nuclear Technology Development Center, a research institute from the Brazilian Nuclear Energy Commission.

Raíssa Oliveira Marques was born in Brazil, in 1992. She received the B.E. degree in Control and Automation Engineering from the Federal University of Minas Gerais, Belo Horizonte, Brazil, in 2015. She had developed works on prospecting technological innovation demands, in order to identify strategic opportunities in Research & Development for the automotive industry, and implemented methodologies and software to assist management of risks and waste in nuclear and radioactive facilities. Her main areas of research interest are risk management, probabilistic safety analysis, reliability and human factors. She is currently a master student in Science and Technology of Radiations, Minerals and Materials from the Nuclear Technology Development Center, a research institute of Brazilian Nuclear Energy Commission. Her master's dissertation in progress involves Risk-Based Inspection methods applied to nuclear research reactors.