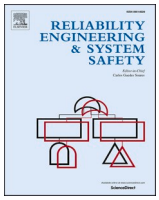
Reliability Engineering and System Safety 216 (2021) 107989

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress



定量人的行为模型在燃料贮存池冷却系统操作程序设计中的应用

Application of a quantitative human performance model to the operational procedure design of a fuel storage pool cooling system

Marcos Coelho Maturana [a], Marcelo Ramos Martins [a,*], Paulo Fernando Ferreira Frutuoso e Melo [b]

[a] Analysis, Evaluation and Risk Management Laboratory – LabRisco, Naval Architecture and Ocean Engineering Department, University of São Paulo, Av. Prof. Mello Moraes, 2231, 05508-030 São Paulo, Brazil
[b] Graduate Program of Nuclear Engineering, COPPE, Federal University of Rio de Janeiro, Av. Horácio Macedo 2030, Suite G-206, 21941-214 Rio de Janeiro, RJ, Brazil.

ARTICLE INFO

Keywords:
Systems design
Human Reliability Analysis
Bayesian Networks
Technique for the Early Consideration of Human Reliability – TECHR
Probabilistic Safety Assessment
Human Performance Analysis

ABSTRACT

Probabilistic safety analyses and Human Reliability Analysis have a potential contribution for designing new systems. For this, it is essential to develop models that are able to feed analyses at the design stage and to bring results that can be used in decision-making. This reinforces the need to develop quantitative techniques for performing human reliability still in the design phase of complex systems – a stage with little information available for Human Reliability Analysis. Currently, one can find publications of this kind for equipment reliability but not for human reliability. This paper presents a technique for human performance analysis that can be used in system design phase. This technique is based on the use of different information sources to obtain probability estimates of the various human error types that may occur during a specific action, and to estimate human error probabilities of generic actions. Thus, considering this model and a methodology for the early quantitative consideration of reliability in the design of complex systems, this paper presents the conception of an operational procedure for a Fuel Storage Pool Cooling System for cooling the spent fuel of a pressurized nuclear reactor, by configuring the human factors without changing the equipment preset for the system.

1. Introduction

Uncertainty about complex systems' behavior [1,2] prior to their exposure to the operational environment contributes to system costs and problems, 80% of which are created during development – i.e., cost and quality are mainly attributed to products at their design phase [3]. The risks associated with these problems can be quantitatively analyzed through PSA (Probabilistic Safety Assessment) – also called Probabilistic Risk Assessment (PRA), or Quantitative Risk Assessment (QRA) [4].

The PSA of industrial installations is a subject, which has evolved along with the complexity of systems [5]. PSA is considered a logical, comprehensive and structured methodology, focusing on identifying and evaluating risks of complex technological systems, with the final purpose of improving their safety and performance characteristics while maintaining an acceptable cost-benefit ratio [6]. To quantify such risks, in addition to the information on the operational environment – e.g., natural phenomena statistics –, PSA is based on combining equipment and operator reliability data.

1.1. Brief HRA development history

The importance of considering human reliability in system design has been consensual since the early years of PSA [7,8], and it is done by employing the techniques of HRA (Human Reliability Analysis) in the analysis process [9]. Over the years, the need to evaluate human performance has resulted in the development of various techniques dedicated to HRA [10]. The understanding of the set of said techniques can be obtained by studying the historical evolution of HRA. It is interesting, for example, to note the strong connection between the accident at TMI (Three-Mile Island) [11] on March 28, 1979, and the increase in the number of techniques for HRA – as pointed out in Ref. [12]. The TMI accident is considered a milestone since the human factor has become one of the main concerns, both with the design of control rooms and other points of nuclear power plants, constituting a relevant aspect of PSA to be considered in plant licensing decisions [13]. In subsequent years, major accident studies – e.g., Bhopal (1983), Chernobyl (1986), Fukushima (2011) – reinforced the need to enhance the development of

* Corresponding author.
E-mail address: mrmartin@usp.br (M.R. Martins).

https://doi.org/10.1016/j.ress.2021.107989
Received 22 May 2020; Received in revised form 24 June 2021; Accepted 18 August 2021
Available online 9 September 2021

HRA techniques and the importance of the human factor as the ultimate safety barrier in nuclear power plants [14,15].

The first works on HRA appeared in the 1950s [16], and in 1962 a preliminary version of THERP (Technique for Human Error Rate Prediction) [17], the first formal HRA technique [18], was presented. The other HRA techniques were issued after the leading PSA published by Rasmussen et al in 1975 [19,20] and mainly after the TMI accident. After that, many techniques emerged in the 1980s, with a major increase around 1984. The techniques that have emerged up to this period are considered first generation techniques (e.g., THERP). This period was accompanied by a less pronounced one around 1996, with the emerging of so-called second generation techniques (e.g., Cognitive Reliability and Error Analysis Method – CREAM [21]), which were trying to suppress criticism of first generation techniques – e.g., dichotomous modeling [22], consideration of commission errors, contextual dependencies and cognitive factors [12].

More recently, HRA techniques based on human performance simulation – e.g., Ref. [9] – have emerged and are not classifiable among first or second generation techniques [23]. These techniques present dynamic foundations, i.e., models that seek to replicate human behavior in simulations [4], depending less on empirical data or expert opinion, and, because of their unique characteristics, can be classified as third generation techniques [24–26]. However, according to the characteristics of the various HRA techniques, classification in generations is questionable, i.e., many techniques can be classified, according to their characteristics, in different generations [24].

In 2009, the HSE (Health and Safety Executive) published a report [27] which recognized 72 techniques dedicated to HRA, of which 35 are quantitative, and since then, new techniques have been developed [18], showing the limitation of the techniques presented so far to satisfactorily or in a consensual way respond to the persistent criticisms and needs faced by HRA specialists. The highlighted shortcomings are related to [28,29]: (a) The context of application of the techniques in relation to those of data gathering; (b) Reliability of the database and quantitative results; and (c) Uncovered or developing points: e.g., development of updatable models [22,30–32]; consideration of dependencies [32]; consideration of latent errors [15]; suitability for employment in the conception phase [30–33], and modeling of commission errors [15].

Part of the questions faced by the HRA techniques arises from the difficulty of including dependencies and considering uncertainties in the commonly used quantitative models (e.g., fault trees). As a way to improve this modeling, the use of BNs (Bayesian Networks) [22] has been discussed [34]. In addition to facilitating the combination of different information sources (simulator and empirical data, expert opinion and cognitive models), a BN allows the immediate updating of the quantitative model by means of new information [25,32,35].While allowing for more realistic quantitative modeling, the use of BNs in HRA is not free from gaps, such as those listed by Mkrtchyan et al. [32] whose completion is being worked on by the HRA community [36]. According Mkrtchyan et al., in general, these gaps are related to the scarcity of data and the lack of formalization for the elaboration of BNs – both for the elaboration of the topology and for the quantification of the CPT –, resulting in limitations such as [32]: (a) difficulty in the validation of the models obtained; (b) lack of data for filling out the CPT – it is often necessary to apply algorithms for filling it out; (c) difficulty in assessing the uncertainty of the data provided by specialists – both in the method of collection and in the responses of the specialists, and; (d) difficulty in defining the required level of refinement of the network. To some extent, these gaps prevent full exploitation of the BNs' modeling capabilities. These difficulties are especially relevant when it comes to the system design phase – considering that they add to the limitations inherent in this phase: e.g., uncertainty about the solutions to be adopted and about the operational environment that will be faced by the system.

1.2. PSA and HRA as design tools

The use of PSA and HRA results for designing alternatives comparison is not a new concept [37–39], being applied or identified as important in a variety of areas [40]. The study of PSAs performed in various industries helps understanding the consensus about such concept, and highlights these analyses potential contribution in developing new systems [40]. However, exploring this potential depends on elaborating simple, quantitative, realistic, and prospective processes and models which should be able to feed cost and performance analysis at the design stage, and bring results that can be interpreted by professionals involved in the decision-making process of design.

Despite the recognized benefits of PSA and HRA application at the early stages of design [41,42], there is some resistance to its quantitative results [43,44], since its substantial demand for data [10] (not always available) may lead to non-trivial assumptions in order to make analyses feasible [4,45]. In addition, regarding HRA at the design stages, there is a preference for developing qualitative techniques, limiting the use of HRA's results to the cost-benefit comparison of design alternatives [46] – i.e., it is possible to find consolidated methodologies to quantitatively deal with equipment reliability during early design stages [38,47], the same cannot be said about the case of human reliability [18].

In spite of the difficulties of handling uncertainties during the designing of complex systems, the risk associated with critical systems operation should be limited [48]. In view of the increasing global demands for safety, in general, the design of these systems must comply with safety criteria such as the threshold for the reactor core damage frequency in nuclear power plants [13]. Thus, the safety demonstration is increasingly necessary, even before the system goes into operation, and often this type of criterion is defined quantitatively. On the other hand, this appeal to safety does not eliminate the need to consider cost-related performance aspects – still in the nuclear example, one can find guides demonstrating how reliability assurance methods, techniques and programs can be used to optimize both economic performance and plant safety [49].

1.3. Motivation and content of this paper

As can be inferred from the discussion in the preceding paragraphs, it is expected that the development and application of techniques for the reliability quantification and comparison dedicated to the design phase – especially when considering human reliability – will help overcome the criticism surrounding the PSA and HRA techniques – since available techniques generally target systems already in operation, at a stage when there is more information available for HRA – i.e., for the identification of hazards related to human factors, task analysis and human error analysis.

Given this motivation, this paper presents the results of applying a system design methodology [40] considering a quantitative reliability goal, supported by a prospective model of human reliability developed for use in the early design phases [50] – for defining HEP (Human Error Probability) in a specific way (considering the types of human errors which can occur in the action under analysis, as an alternative to associating performance data of similar actions), thus improving the model representativeness [51].

Thus, as an example, two complementary issues are addressed in this paper: (1) the obtaining of a human performance model, applicable to the design phase, and; (2) the design of an operational procedure for the FSPCS (Fuel Storage Pool Cooling System), by applying the methodology discussed in the next section (Section 2) – and configuring the human operator activities without changing the equipment preset for this system. In this way, Section 3 presents the achievement of the human performance model by describing the disaggregating and aggregating quantitative human error data, and the resulting probabilistic model of human performance, and Section 4 presents the design of the FSPCS operation – by applying the methodology phases presented in Section 2

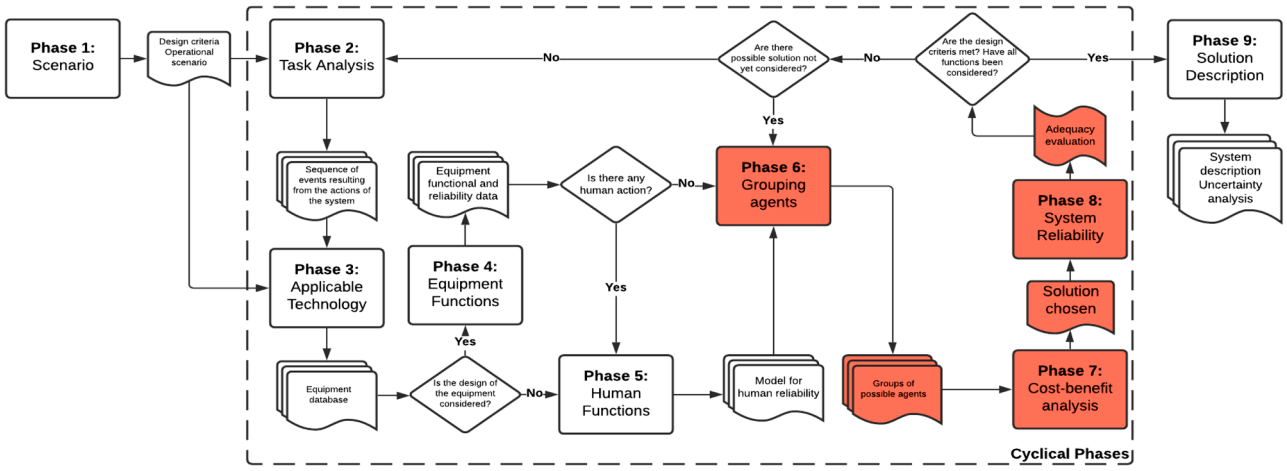


Fig. 1. Methodology flowchart.

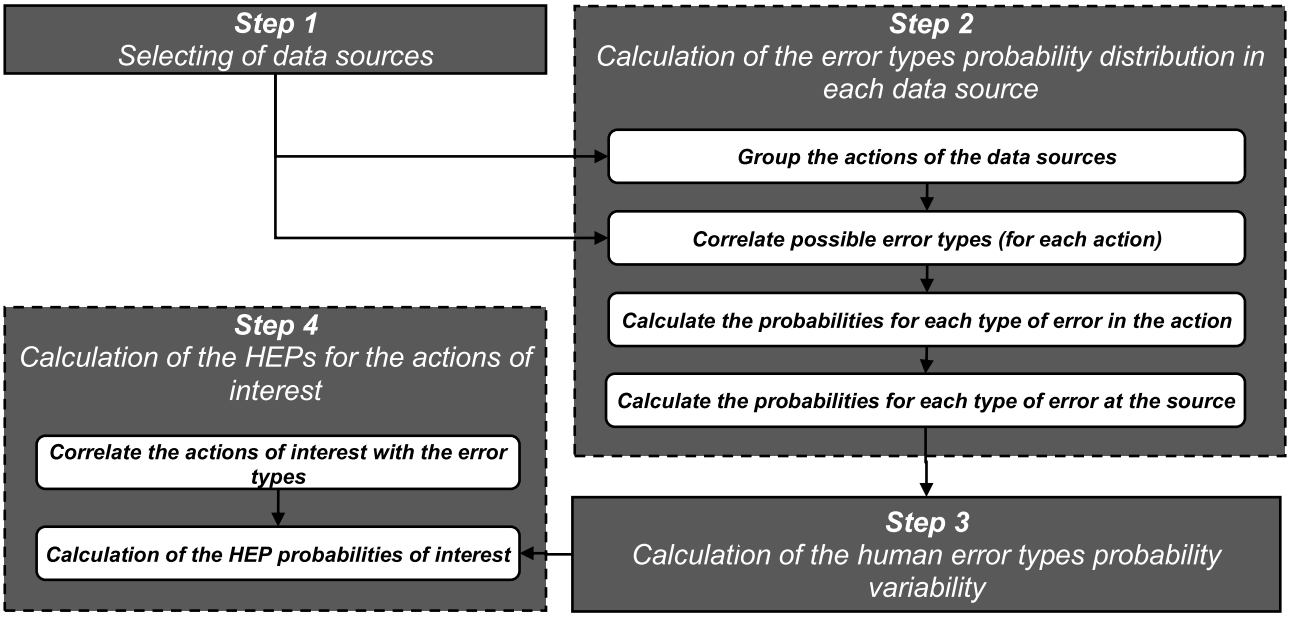


Fig. 2. Steps to obtain a probabilistic human performance model.

and the human performance model presented in Section 3. Finally, Section 5 presents the final discussions and conclusions of this work.

2. Methodology for the early consideration of reliability in the design

In view of the points outlined in the previous section, Martins et al. [40] presented a preliminary methodology for the early quantitative consideration of reliability in the design of complex systems. For operators, this method prospectively compares the agents who can compose the system based on available data, such as HRA techniques, expert opinion, or published PSAs – the human reliability model adopted in this application is described in the next section.

Fig. 1 presents the nine phases of the proposed methodology. In this figure, the rectangles indicate the required activities (phases of the methodology), the diamonds show the decisions to be made, the files represent the main results of each phase, and the arrows indicate the order in which the activities are carried out. The basic objectives of this methodology phases are presented as follows: Phase (1) Scenario: defining the needs to be met by the system and elaborate the operational scenario; Phase (2) Task Analysis: searching for a sequence of events resulting from the actions of the system, which meets the requirements established in the scenario proposed in Phase 1; Phase (3) Applicable Technology: forming an equipment database applicable to the field for which the system is developed; Phase (4) Equipment Functions: discriminating the functional and reliability data for the functions of the equipment listed in Phase 3 – these functions can be obtained by the widespread techniques of Functional Analysis [48,52]; Phase (5) Human Functions: defining a model for human reliability dedicated to the area of the system application (equipment listed in Phase 3); Phase (6) Grouping Agents: for the required actions – described in Phase 2 – among the solutions presented in Phases 4 and 5; Phase (7) Cost–benefit analysis: choosing the solution from Phase 6 which presents the best cost-benefit relation, considering the uncertainty about its estimate – if only reliability data is available, this phase might consider selecting the highest reliability; Phase (8) System Reliability: evaluating the adequacy of the results previously obtained, and Phase (9) Solution Description: describing the system, thus showing the reliability of the found solution, as well as the results of an uncertainty analysis. Phases 6–8 – highlighted (in red) in Fig. 1 – are considered in solution development cycles (when

the information obtained in previous phases is used for constructing a probabilistic model to compare design alternatives).

In Ref. [40], a simplified problem demonstrates the phases of the methodology – that paper presented in a hypothetical example the conception of a system that maintains the water temperature in a tank between predefined limits. Otherwise, this text presents the application of these phases to a real case – i.e., in the conception of the FSPCS operation –, and supported by a specific human performance model.

Moreover, to facilitate the integration of the human performance model (modeled as BN), the case discussed in this paper is structured as a BN – other advantages of applying BN in the design phase instead of FT (Fault Tree), more common in PSA and in reliability engineering, will be discussed along with the case study insights, in Section 5. These application results are described after the presentation of the quantitative human performance model developed to meet the requirements of Phase 5 of the methodology.

3. Obtaining a human performance model

Although the expected little information on a system operation in the design phase – making it difficult to choose and apply available HRA techniques to assess the contribution of human error to the overall reliability performance of the system –, discussing human performance at the early stage of design allows one to take advantage of the greater flexibility at this stage for consideration of improvements and changes, in preparation for later stages – even helping to identify the available HRA technique best suited for the system analysis. However, for application in the early design phases, and in order to compare the available quantitative human performance data and combine it with the equipment reliability data, there is a need to adapt the presentation and to facilitate the manipulation of this data. The following topic describes a technique to manipulate quantitative data presented in different HRA techniques, and the next presents its application, resulting in a probabilistic model of human performance – targeting the requirements of Phase 5 of the methodology presented in Fig. 1.

It is interesting to note that the model discussed in this section was developed as BN to take advantage of the recognized ability of this tool in modeling individuals, their interrelationships and dynamics, in addition to the flexibility to work with discrete or continuous variables and to combine frequentist data with subjective predictions of probabilities [22]. The developed model, however, focuses on available quantitative data, bypassing the difficulties usually encountered with detailed modeling of factors that influence human performance, leading to CPT that can be completed without the need for expert elicitation (as detailed in Section 3.1).

3.1. Disaggregating and aggregating quantitative human error data

In order to generate a probabilistic model of human performance, Fig. 2 suggests four steps to disaggregate and aggregate quantitative human error data. These steps can be briefly described as follows:

- Step (1) Selection of data sources: selection of quantitative data sources that allow the association of human actions with possible types of human error.
- Step (2) Calculation of the error types probability distribution in each data source: this step includes the following activities: (a) Group the actions in the data source in order to facilitate their comparison with the chosen taxonomy for the classification of error types; (b) For each human action in the data source, to correlate the possible types of error listed in the chosen taxonomy; (c) Calculate the probabilities for the error types in each action of the data source, and; (d) Calculate the probability distribution for each error type in the data source, based on the HEP for each action.
- Step (3) Calculation of the human error types probability variability: this step refers to the construction of the probabilistic model for calculating the variability of the error types listed in the selected taxonomy, considering the estimates in each data source.
- Step (4) Calculation of the HEP for generic actions: this step includes the following activities: (a) Correlate the actions of the chosen taxonomy (for the classification of human actions) with the human error types – i.e., this activity consists of judging which types of error can occur in the actions of interest (it is emphasized that this association contributes to the characterization of the generic action in the performance model), and; (b) Calculate the probabilities of the priori HEP of the actions of interest, based on the variability estimates of the human error types obtained in step 3.

The main features that should be available for this steps application are as follows: (a) Human error data: empirical data sources that allow HEP estimates, and which correlate human actions and human error types; (b) A comprehensive *taxonomy for human actions* classification; (c) Technique for classifying human errors: a comprehensive *taxonomy for human errors* classification, and; (d) Tool to facilitate probabilistic modeling (depending on the desired degree of detail of the model): a computational tool that allows the storage and manipulation of the information to be processed by the performance model. The following paragraphs discuss the choices made for the application discussed in Section 3.2.

3.1.1. Human error data

The human reliability data available in the literature, in general, are those used as a basis for the quantitative HRA techniques. Thus, in order to identify techniques with data sources that could be worked on to build the desired prospective model, a comprehensive literature review was carried out, and four data sources were identified (see item 3.2.1).

3.1.2. Taxonomy for human actions

In relation to the classification of human actions, considering the need for future training activities for the operators of the system to be designed, the use of a taxonomy that facilitates the planning of such training was considered. In addition, a search was made for a comprehensive and structured taxonomy that allows for its expansion (since new systems may require actions not listed in taxonomies aimed at specific domains). Thus, the taxonomy of educational objectives [53] – also known as Bloom's taxonomy, in reference to Benjamin S. Bloom, who directed the group that composed this heuristic [54] – was considered. Bloom's taxonomy was developed to categorize the goals of educational experiences by focusing on the expected observable training (activities that the student should be able to perform) after submission of the individual to a training process [53], and divides educational goals into three domains: cognitive, affective, and psychomotor. In these domains, learning at the highest levels depends on the attainment of the knowledge and skills at the lower levels. Originally, two volumes were published, referring to the cognitive domain [53] and the affective domain [55]. Other authors have proposed taxonomies for the psychomotor domain [56–58]. Over the years, changes have been proposed to these original works [54]. The changes considered in the scope of this paper are as follows: (1) Anderson and Krathwohl proposed a revision of Bloom's taxonomy for the cognitive domain [59,60]; and (2) The actions and processes described by Anderson and Krathwohl have been revised in order to consider the situations that emerge from the use of new technologies – such as those identified in Ref. [61].

The cognitive domain of the Bloom's taxonomy is related to the actions centered in the memory of knowledge and in the use of intellectual abilities. Thus, the actions resulting from psychological activities with knowledge function can be classified in the cognitive domain. The categories initially proposed for this domain are knowledge, understanding, application, analysis, synthesis, and evaluation [53]. Anderson and Krathwohl proposed a revision of these categories, reorganizing this domain in the dimensions "knowledge" and "cognitive process". The dimension "knowledge" presents the following categories: effective,

Table 1
Categories of dimension "cognitive process" and associated human actions.

Category	Description	Cognitive processes						
		Process	Description	Examples of human actions				Code
Remember	Recover relevant information previously learned from long-term memory.	Recognize	Find in the long-term memory the knowledge that is consistent with the material presented.	Discriminate Find Tag	Localize Name Sort	Search List Select	Identify Organize Underline	A_C_1a
		Remember	Recover relevant knowledge from long-term memory.	Describe Choose	Recite Remember	Repeat Reproduce	Recover Know	A_C_1b
Understand	Determine the meaning of oral, written, or graphic information. Demonstrate the understanding of facts by exposing ideas and concepts.	Interpret	Change from one form of representation to another.	Take note Convert Report	Recount Revise Reaffirm	Paraphrase Represent Translate	Clarify Research Recognize	A_C_2a
		Exemplify	Find a specific example or illustration of a concept or principle.	Illustrate	Express	Describe		A_C_2b
		Classify	Determine that something belongs to a category.	Categorize	Select	Subordinate		A_C_2c
		Sum up	Summarize a comprehensive theme or larger subject.	Distinguish	Instantiate	Twitter		A_C_2d
		Infer	Sketch a logical conclusion from the information presented.	Sum up	Abstract	Estimate		A_C_2e
		Compare	Detect matches between two ideas, objects, etc.	Ask	Generalize	Defend		A_C_2f
		Explain	Build a cause and effect model of a system.	Conclude	Predict			A_C_2g
Apply	Perform or use a procedure in a given situation. Use information in situations different from that of obtaining knowledge.	Run	Perform a goal or fulfill an order in a known situation.	Schedule File Calculate Compute Demonstrate	Edit Employ Run Do Perform	Show Operate Share Prepare Trim	Draw Drive List Manipulate Sequence	A_C_3a
		Implement	Solve problems in new situations by applying knowledge, facts, techniques and rules.	Adapt Change Fulfill Build Discover Dramatize	Sketch Choose Write Experiment Illustrate Implement	Play (sport) Modify Predict Produce Schedule Use	Rehearse Teach Install Interpret Solve	A_C_3b
Analyze	Separate a material into its constituent parts and determine how the parts relate to each other and to the whole. Find evidence that supports generalizations.	Differentiate	Distinguish relevant and irrelevant parts or important and unimportant parts of displayed material.	Point Centralize Rank Compare Contrast Question	Distinguish Examine Experiment Identify Inspect Decompose	Select Separate Subdivide Test Trim	Discriminate Inventory Order Create a mind map	A_C_4a
		Organize	Determine how the elements work or fit in a structure.	Evaluate Work around Debate Discover Link	Sketch Structure Group Infer Integrate	Diagram Search List Solve Sequence	Find consistency Interrogate Investigate	A_C_4b
		Assign	Determine the point of view, deviations, value or the basic purpose(s) of a presented material.	Deconstruct Criticize	Calculate Interpret	Reverse engineering	Debate Model	A_C_4c
Evaluate	Make judgment based on criteria and standards (determined by the individual or offered to him). Justify a decision or action plan.	Check	Employ a standard of assessment.	Compare Coordinate Describe	Detect Discriminate	Monitor Test	Measure Check	A_C_5a
		Criticize	Evaluate quantitative or qualitative options (e.g., opinions, materials, methods) by judging information, validity of ideas or quality of work based on a set of criteria.	Support Appreciate Argue Evaluate Collaborate Comment Conclude Contrast Criticize	Defend Debate Choose Estimate Explain Interpret Judge Justify Moderate	Prioritize Recommend Reflect List Sum up Review Rhythm Select	Decide Score (note) Post (opinion) Predict Validate Check evaluation	A_C_5b
Create	Bring together elements to form a coherent and functional whole.	Generate	Present alternative hypotheses based on a set of criteria.	Explain Formulate Generate	Propose Infer Improve	List Suppose	Imagine Predict	A_C_6a
	Rearrange the elements into a new pattern or structure.	Plan	Elaboration of a procedure for the execution of some task.	Categorize Set up Rearrange	Get together Organize	Schedule Design	Manage Prepare	A_C_6b
	Generate new ideas or ways of seeing things. Propose alternative solutions.	Produce	Invent a product.	Blog Combine Compose Build Mix	Create Drive Write Expose Do	Publish Rearrange Rebuild Get together	Develop Shoot Invent Synthesize	A_C_6c

Table 2
Categories of psychomotor domain and associated human actions – Harrow's taxonomy.

Category	Description	Human actions			Code
Reflexive Motion	Reacting automatically (involuntarily) to a stimulus.	React	Answer		A_P_1
Basic Movement	Moving reflexively (segmental, intersegmental and suprasegmental reflexes [34]).	Raise	Walk	Reach	A_P_2
Perceptive Ability	Activities focused on the interpretation of various sensory stimuli	Take Write	Explore	Distinguish using the senses	A_P_3
Physical Skill	Change position, move, and perform simple action. It includes the basic movements that can compose more complex groups of fundamental movements: locomotive movement, non-locomotive movement and manipulation.	Support Keep Repeat	Increase Improve Exceed	Develop Force Control	A_P_4
Qualified Movement	Respond to different sensory perceptions. Respond to a kinesthetic, visual, auditory, tactile stimulus or a grouping of environmental stimuli that allow the individual to adjust his/her movements.	Drive Build Juggling	Play a musical instrument	Perform crafts	A_P_5
Non-verbal communication	Activities that require strength, strength, vigor and agility; Which require further development of physical abilities (endurance, strength, flexibility and agility).	Express feelings	Convey feelings	Express meaning	A_P_6

conceptual, procedural, and metacognitive [59].

The "cognitive process" dimension presents the categories remember, understand, apply, analyze, evaluate, and create, grouping nineteen cognitive processes, organized from the most basic to the most complex [60]. In this dimension, the description of categories by verbs harmonizes with the interest of using Bloom's taxonomy for the classification of observable human actions. Table 1 describes the characteristics of each category and cognitive processes and presents a list of actions that can be associated with each process. It is emphasized that Table 1 does not present the actions that make up the cognitive process, but the observable actions resulting from this process. In addition, the last column refers to the code for the type of action used in the prospective human performance model.

The affective domain of the Booḿs taxonomy is related to emotions and postures, i.e., to individual feelings, values, interests, motivations and attitudes. The proposed categories for this domain are receptivity, response, valorization, conceptualization of values, and interiorization of values [55]. In this domain, the actions that make up the process of character formation, i.e., related to attitudes, values and dispositions can be classified. As the case study presented in Section 4 did not find actions classified in the affective domain, it will not be detailed in this paper.

The psychomotor domain of the Booḿs taxonomy relates to the individual's physical abilities. Bloom's group did not define a taxonomy for this domain [54]. Following the approach of this group, however, other authors have proposed taxonomies for the psychomotor domain [56–58]. Considering that in this paper Bloom's taxonomy will be explored as a starting point for the classification of human actions, Harrow's proposal is the most adequate for the purpose of this work.

For the psychomotor domain, Harrow's proposal classifies educational objectives into six categories: reflexive movement, basic movement, perceptive ability, physical ability, skilled movement, and non-verbal communication [56]. Table 2 describes the characteristics of these categories and presents a list of associated actions. In this table, the categories are ordered according to the degree of coordination required, from involuntary responses to skills learned(56). In this taxonomy, the categories represent specific actions. The last column of Table 2 refers to the code for the type of action used in the quantitative models – in item 3.2 and Section 4.

3.1.3. Technique for classifying human errors

The way to classify human error can be as diverse (e.g., classification by task type, according to cognitive model or by the context of occurrence [20]) as the objectives of a heuristic model (e.g., accident analysis, quantification of human error in a specific industry), and several taxonomies have already been published [62]. The GEMS (Generic Error Modeling System) [63], proposed by Reason to explain human errors [64], is the most widespread taxonomy among performance experts [65,66], and derives from the processing model of human knowledge information proposed by Rasmussen [63,67] – known as SRK (skill-rule-knowledge model) [68]. Table 3 summarizes the human error taxonomy derived from GEMS, referred to in this work as Reason's taxonomy – the last column refers to the codes associated with the error types, which are used in the models presented later.

Aligned with the SRK model, GEMS classifies erroneous actions at correlated levels of performance with the following characteristics: (1) Skill level: lapses and slips can occur and, in general, erroneous actions refer to automatic behavior with low level of individual consciousness; (2) Rule level: Rule-based mistake can occur – the context is considered to determine the rule to be adopted (more appropriate actions), and the individual orders the rules by their value, based on the frequency of success in applying the rule, and; (3) Knowledge level: knowledge-based mistake may occur – actions refer to complex reasoning and problem solving in new circumstances and the errors associated are justified by the limitations of resources, incomplete knowledge or incorrect knowledge.

The adoption of GEMS in this application is based on: (1) Expert opinion on GEMS: (a) combined with the SRK model, it is accepted as the most comprehensive human error taxonomy [20,65]; (b) it describes human error within a theoretically plausible structure [66]; (c) SRK is applicable in the development of a predictive tool [20], and; (d) it presents extensive documentation for its understanding [63,64,69]; and (2) Purpose of this work: GEMS was developed to classify human errors in different contexts [21], and the purpose of its taxonomy (by definition, GEMS is a generic system) meets this paper objectives – quantify the human error for a prospective performance model to be used in the design phase of a complex system, when restricted knowledge about its performance in the context of use may be uncertain. On the other hand, this applicability to a multiplicity of contexts shows that GEMS does not have instructions for the identification of specific types of error, being this task delegated to the expert using it.

Thus, in this paper, Reason's taxonomy was directly explored by associating the types of errors listed in the taxonomy with the actions obtained from the data sources (as explained in Section 3.2.2) – considering the characteristics of the actions presented in the data sources, these associations were performed by the authors of this work (whenever the information in the data source was not clear, it was desconsidered: see discussion in item 3.2.2). Once the types of error were associated with the actions, the HEP data were used to estimate the variability of the probability of the types of error [50] – as exemplified in Section 3.2.2.

3.1.4. Tool to facilitate probabilistic modeling

It is intended that the human performance model is updatable throughout the design and allows the use of Bayesian inference to compare design alternatives. Thus, the human performance model was developed as a BN – the computational tool NETICA® [70] was chosen. This option facilitates to integrate the human performance model to the BN resulting from the application of the design methodology (see Section 2).

Table 3
Reason's taxonomy [64].

PerformanceLevel	Error type		Characteristics and Description	Code
Skill Level Performance	Double-capture slips		Routine action; Familiar atmosphere; At the moment of decision making, an event (internal or external) diverts the attention of the individual, The individual makes the decision automatically (by habit).	EG_1a
	Omission after interruption		Routine action, At the time of the execution of a task, the individual is interrupted by an event (internal or external), forgets where he / she was in the task and fails to perform one of its steps.	EG_1b
	Intention reduction		While performing a task, the individual forgets his / her purpose (loses awareness of the entire sequence of actions).	EG_1c
	Perceptive confusion		Routine action, Due to the lack of attention to the senses, the individual makes an erroneous selection.	EG_1d
	Interference errors		This error consists of exchanging actions in the same task (sequence of actions) and replacing them with similar actions.	EG_1e
	Omission		Omission of an action of the task or of the entire final sequence of actions, This error is attributed to the lack of control of the task state in relation to its purposes.	EG_1f
	Repetition		In task execution, the individual repeats an action or sequence of actions, The individual assumes that the task has a number of actions other than the actual number (required for its completion).	EG_1g
	Inversion		In task execution, the individual reverses the order of execution of the actions.	EG_1h
Rule Level Performance	First exceptions		The individual has not learned the correct rule for the solution of a problem and believes in the adequacy of a general rule or a partially valid rule.	EG_2a
	Counter signs and absence of signs		The proper rule is not followed because signals confuse the individual, not allowing their identification.	EG_2b
	Information overload		The large amount of information prevents the consideration of everything before deciding what to do (the individual fails to choose the rule and / or its application).	EG_2c
	Rule strength		Because of the repetition in the use of a certain rule (which thereby becomes strong), the individual tends to use it to the detriment of the others, favoring error.	EG_2d
	General rules		Because they are more comprehensive, general rules tend to be more used than specific rules (and thus become strong), especially in the absence of information, favoring error.	EG_2e
	Redundancy		Information always present, even unrelated to a specific situation, can influence the choice of a rule.	EG_2f
	Stringency		In solving problems, the individual tends to replicate past success formulas (rules), even if simpler and more adequate solutions are available.	EG_2g
	Decoding deficiencies		In performing a task the individual cannot recognize all the conditions necessary for the determination of how to act.	EG_2h
	Poor action: the context for the rule has been learned but the action provided by the rule is inadequate.	Wrong rules	The rule applied is adequate (as learned), The action foreseen in the rule is completely wrong.	EG_2iI
		Non-elegant rules	The action is in accordance with the rule, but the action is outdated because better rules are available.	EG_2iII
		Non-advisable rules	The chosen rule leads to the goal, but with undesired consequences.	EG_2iIII
Knowledge Level Performance	Selectivity		During the task the individual ceases to focus his / her attention on aspects relevant to the solution of his / her problem, focusing on irrelevant aspects.	EG_3a
	Working memory limitation		The problem exceeds the capacity of the individual's working memory;	EG_3b
	Out of sight, out of mind		The individual tends to pay more attention to facts that are available to him / her more easily, disregarding the most inaccessible facts that are important to his / her problem.	EG_3c
	Confirmation bias		The individual tends to value his / her initial hypotheses to the detriment of the evidences that he / she finds throughout the solution of the problem, favoring error.	EG_3d
	Overconfidence		The individual clings to the course initially established to the detriment of the evidence that he / she finds throughout the solution of the problem, favoring error.	EG_3e
	Biased revision		The individual mistakenly considers that he / she has taken into account all the factors that are important for solving the problem.	EG_3f
	Illusory correlation		The individual correlates two or more erroneously dependent variables (e.g., the individual considers that if one variable increases, the other will increase as well, when in fact there is no such a relationship).	EG_3g
	Halo effect			EG_3h

(*continued on next page*)

Table 3 (*continued*)

PerformanceLevel	Error type		Characteristics and Description	Code
			The evaluation of an item or individual interferes in the judgment of other important factors, favoring error (the individual does not make his / her evaluation independently).	
	Problems with causality		The individual greatly simplifies cause-and-effect relationships, underestimating eventualities that may occur in the future.	EG_3i
	Problems with complexity (errors associated with individual's difficulty in dealing with complex tasks).	Problems with delayed return	The individual has difficulty in constructing a predictive model when the return of his / her actions is not immediate; The error is favored by the loss of synchrony between the actions and their results.	EG_3jI
		Insufficient consideration of the process over time	The individual focuses on the current state and ignores its development process.	EG_3jII
		Difficulties with exponential evolution	The individual has difficulty in dealing with processes that develop exponentially, favoring error.	EG_3jIII
		Causal series thinking and not causal networks	The individual tends to think in series, realizing the direct result of his action and ignoring other effects on the system.	EG_3jIV
		Theme digression	The individual abandons a subject or topic, treating it superficially, and initiates a new subject or theme.	EG_3jV
		Encapsulate	The individual develops a topic of the subject much further than necessary, disfavoring the development of other relevant topics.	EG_3jVI

3.2. Probabilistic model of human performance

A scheme of the resulting human performance BN is presented in Fig. 3 [50]. In this figure, the top frames represent the data sources, the respective actions and associated error types, organized according to the level of performance, and illustrate the data processing technique – where the types of errors associated with the actions of each data source are obtained by probability curves.

In the central frames of Fig. 3 the error types are represented, and they are quantified based on the estimates obtained for each data source, and organized according to the level of performance (of the SRK model). Still in the central tables, the points of insertion of the evidences for each type of error are presented – which can be obtained in the system operational phase, or that allow the insertion of expert opinions or data collected in simulators. In the lower tables the generic actions are represented, organized according to the domains (of Bloom's taxonomy) and the levels of performance of each action (of the SRK model). The associations between the errors and the generic actions are represented between the intermediate and lower frames.

The next paragraphs describe how the model illustrated in Fig. 3 was obtained by applying the steps proposed in Fig. 2.

3.2.1. Step 1 – selection of data sources

The three criteria for selecting data sources used to estimate the probabilities of various types of human error are as follows:

- 1st Criterion – Origin of the database: according to this criterion, data sources that have original quantitative bases – e.g., expert opinion, field observations or simulation – were selected. The techniques that did not present a database were not selected, and the techniques that present data based on other techniques were discarded.
- 2nd Criterion – Reliability of Bases and Quantitative Results: the sources of quantitative data had their databases verified in relation to their reliability. In order to do so, publications have been explored which directly or indirectly present comparisons, evaluations or validations of human performance quantitative data, both in relation to its database and in relation to the data that it produces. In addition, its current use was considered for the quantification of human error.
- 3rd Criterion – Data availability: data sources were selected that are not closed or that, in the case of proprietary domain, allow the publication of their database – considering the limitation of resources in the elaboration of this work.

Considering only the criteria above, the CREAM, HEART (Human Error Assessment and Reduction Technique), INTENT, TESEO (Empirical Technique for Estimating Operator Errors) and THERP techniques were selected as data sources for this first application. Essas são técnicas são amplamente empregas na indústria – mesmo a THERP, a mais antiga delas [71]. It is interesting to note that none of these techniques presents the raw data of human performance, i.e., the original empirical data used to generate the HEPs [33], and that, except for CREAM, all are considered first generation techniques [27]. This reflects the difficulty in generating and organizing sufficiently comprehensive empirical quantitative data for the evaluation of the myriad of factors that determine human performance – and which are being considered in the new approaches for HRA, especially in the nuclear industry [29,72–74] this type of data would allow a better quantitative weighting of the context for second and third generations techniques with the reliability observed by the first generation techniques [75] without great dependence on the judgment of experts.

Regarding the techniques selected as a database for this work, its application – generation of HEP for specific contexts – may result in rarely empirically validated estimates [28]. Their basic HEPs, however, have strong links with empirical human performance data and can be combined with subjective predictions of human error probabilities in Bayesian models – e.g., BNs –, in order to generate probabilistic models more adherent to specific contexts. This approach is especially relevant in the design phase of complex systems, when the use of frequentist models is limited by insufficient data.

Therefore, from the sources selected, the basic HEPs and their uncertainties were isolated, since these data can be the base for a generic human performance model. These data present sparse characteristics (reflecting epistemic uncertainties and variability of human performance) and were processed as discussed in the next step.

3.2.2. Step 2 – calculation of the probability distribution of the error types in each data source

The Reason's error types were quantified, and their population variability was obtained – considering that the HEPs presented in the selected data sources resulted from different strata of the population (i.e., each HEP estimation resulted of a subpopulation). Thus, for each data source, different estimates were obtained for the probability functions of the error types – each action represents different contexts for the manifestation of the associated error types – which were combined in an estimate for the respective subpopulation. To do so, it was necessary to cross-reference the types of Reason's errors and the selected actions and errors. In this crossing, the information in the databases and the error types presented in GEMS were considered [64].

For each selected action – or type of error, depending on the data source (to avoid repetition, only the actions are quoted in the rest of the

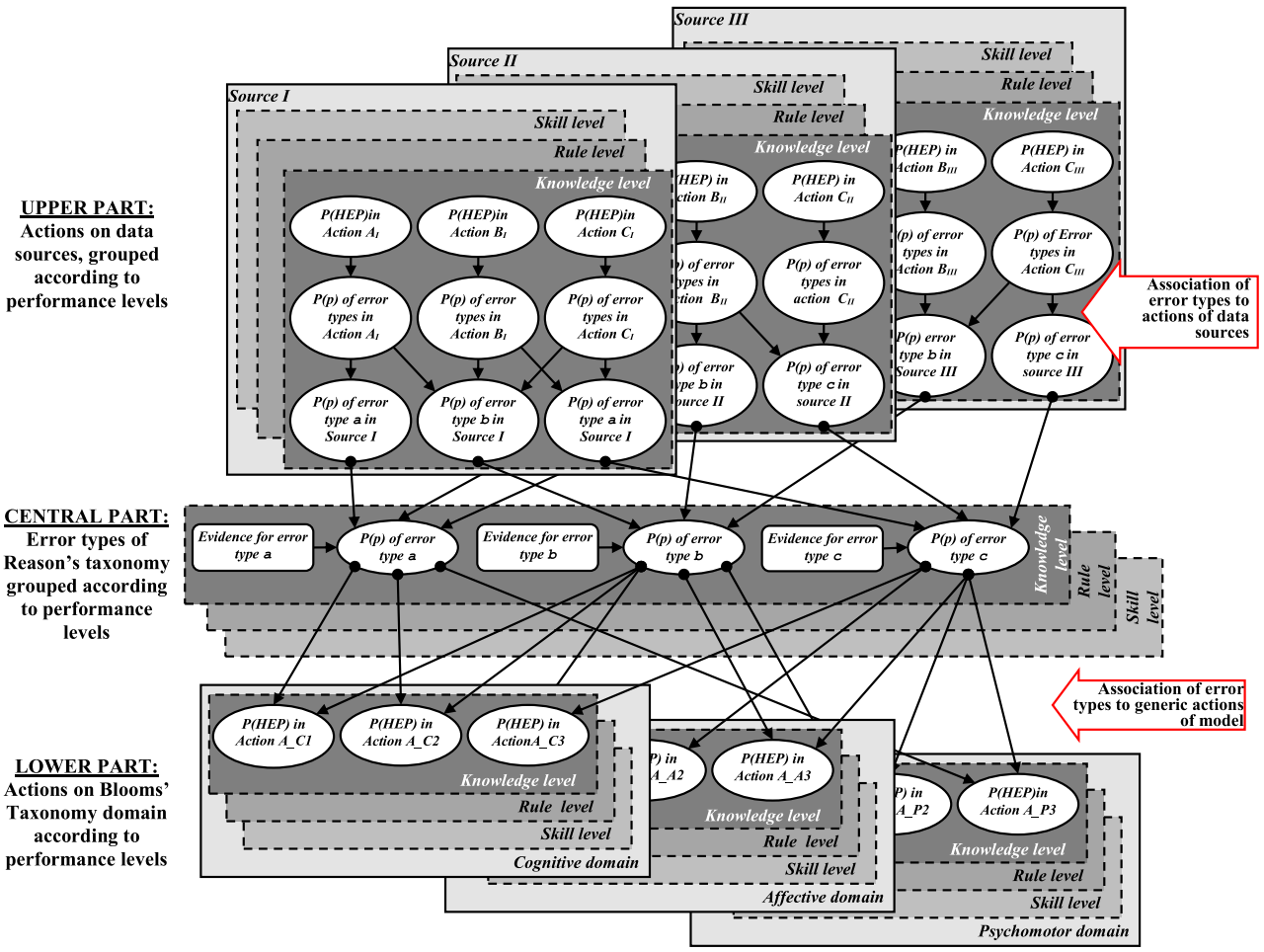


Fig. 3. Scheme for an updatable prospective model of human performance [50].

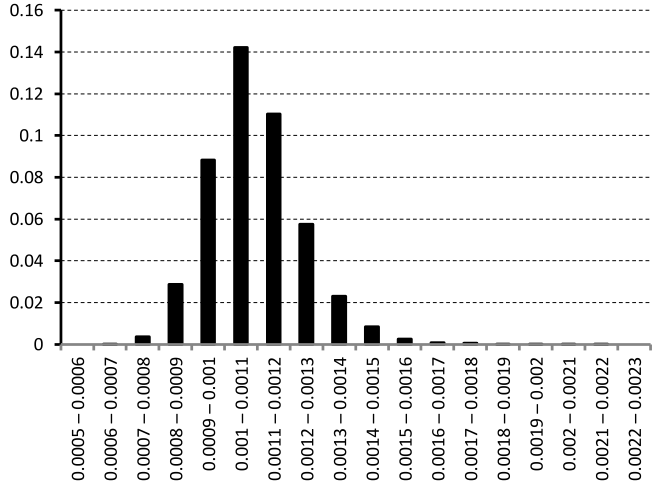


Fig. 4. Identification aid of the performance level and of possible error types.

text) –, the information available in each data source and the types of error described in Table 3 were compared. In general, this consisted in the following activities: (1) gather all information regarding the action presented in the data source for the definition of its execution contexts; (2) employ the diagram shown in Fig. 4, based on the definitions of error types (Table 3), which results in the association of the action with a level of performance of the SRK model and a preliminary list of errors associated with the action, and (3) refine the preliminary list by comparing the action data and all types of errors to their performance level, which results in a list of the types of errors considered most likely.

Fig. 4 represents an attempt to group Reason's error types according to their characteristics. Thus, according to the answers to the questions (yes or no), possible types of errors and / or new questions are presented – in case of doubt, both answers are considered possible. In this diagram, hatched boxes represent types of error (gray for skill level, red for rule level, and blue for knowledge level – the codes from Table 3 are also shown in Fig. 4).

Some correlations between the errors in Fig. 4 and the actions in the data sources are evident (e.g., associating a selection error with button-triggering activities in panels with many options), whereas others are not as much (e.g., associating the memory problem with priority given to problems considered less important). In addition, it was observed that not all the data selected in item 3.2.1 could be used, generally due to the difficulties found in the association of error types. The following is a brief discussion of these issues for each data source.

- CREAM: Reason's error types were associated with the types of error (consequent of the actions) correlated to the human functions defined by Hollnagel [21], i.e., failures in cognitive functions were directly associated with types of Reason's error. Taking into account the characteristics of the respective error types (as a result of actions [21]), these functions were associated with SRK performance levels as follows: (1) observation and execution: skill level, and (2) interpretation and planning: knowledge level. To find the most probable correlations, the descriptions of the error types and

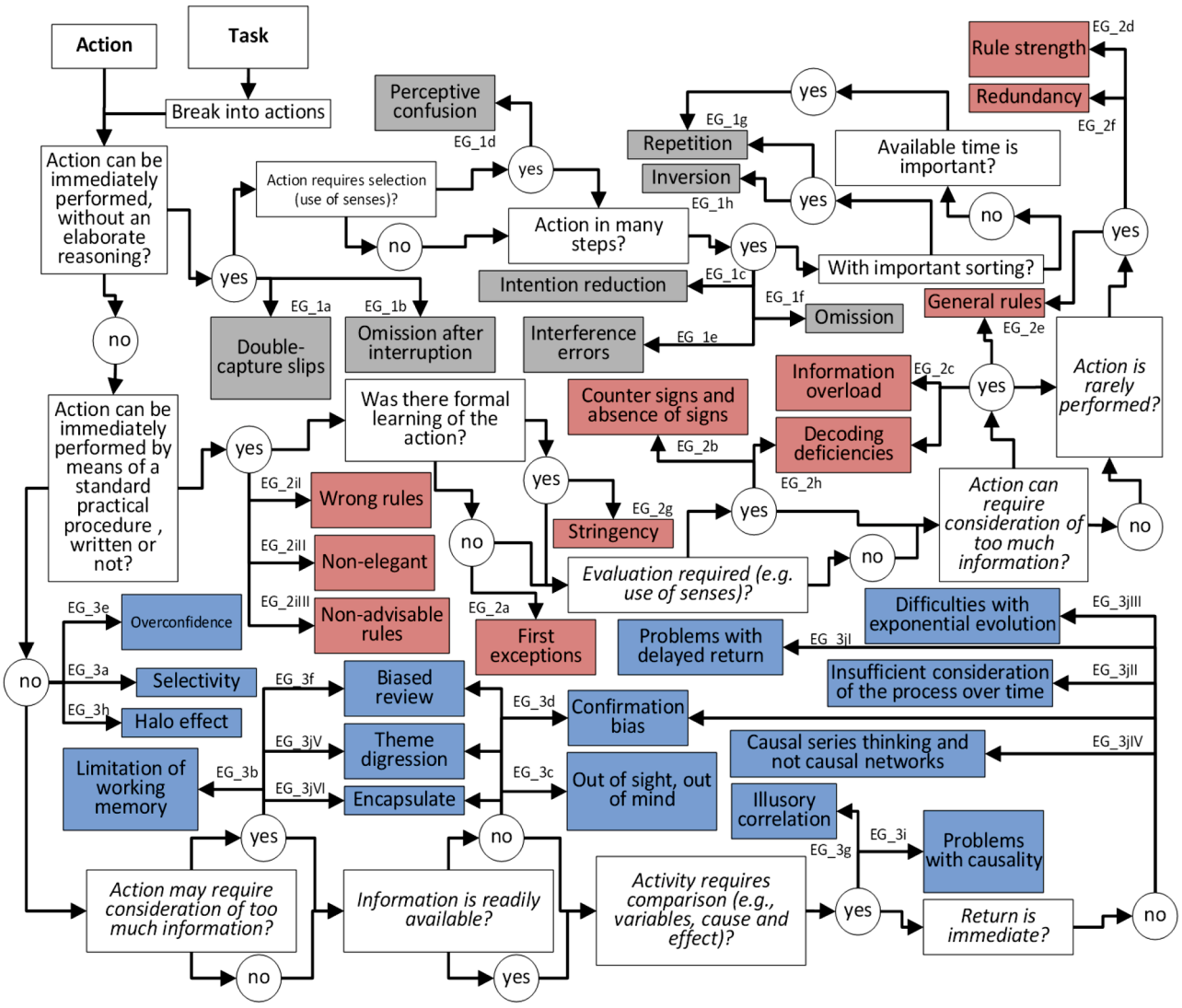


Fig. 5. BN for the probability function for the error types associated with action C_E1.

descriptions of the human functions presented in CREAM [21] were compared – it is emphasized that the correlations considered most probable were maintained, weighting the characteristics of the different types of errors considered in CREAM, while the others were disregarded.

- HEART: the actions presented in HEART [76] were associated with SRK performance levels as follows: (1) Skill level: D (quite simple task performed quickly or giving little attention) and E (routine, highly trained / practiced or fast task involving relatively low skill level); (2) Rule level: B (change or restore the system to a new or original state in a single unsupervised attempt or procedures), F (restore or change a system to its original or new state by following procedures with some verification), G (completely familiar, well-designed, well-practiced routine practice occurring several times per hour, performed to the highest possible standards by a highly motivated, highly trained and experienced professional, fully aware of the implications of failure, with time to correct potential error, but without the benefit of significant aid to his / her work) and H (correct response to system commands even when there is no extended or automated supervision system providing accurate interpretation of system state), and (3) Knowledge level: A (totally unfamiliar, quickly performed with no real notion of possible consequences) and C (complex task requiring high level of understanding and skill). In principle, in order to find the most probable error types, the diagram presented in Fig. 4 was applied and, later, the descriptions of the actions were compared with the characteristics of the error types (summarized in Table 3), with correlations considered to be more likely. The action M (Miscellaneous task for which no description can be found) was disregarded in these tables because it could not be associated with a prevailing performance level.
- INTENT: the error types were directly associated with Reason's error types. In general, the INTENT data associate a situation with an unwanted action and, therefore, are expressions of cognitive dysfunctions [77]. The Reason's error types were correlated to the INTENT data by weighing both the situations and the unwanted results with the categories associated with the performance levels of the SRK model as follows: (1) consequence of the action, actions that lead to violation, and dependence on resources: rule level, and; (2) response defined by the technical team: knowledge level. Error types 8 (common-cause failure due to poor safety culture) and 19 (excessive overtime results in improper judgment), of the categories actions that lead to violation and resource dependence, respectively, were disregarded in these tables because no references were found that allowed its association with performance levels – i.e., it was not possible to associate a predominant level of performance with these errors.

Table 4
CPT for node "P(Error type associated with CE_1)" of the BN of Fig. 5.

Parent Nodes		p									
HEP	L	0.00E+00	1.00E-10	2.00E-10	3.00E-10	4.00E-10	5.00E-10	6.00E-10	...	9.00E-01	1.00E+00
0.00E+00	3	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
1.00E-10		1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
2.00E-10		5.00E-01	5.00E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
3.00E-10		3.33E-01	4.44E-01	2.22E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
4.00E-10		2.50E-01	3.75E-01	2.50E-01	1.25E-01	0.00E+00	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
5.00E-10		2.00E-01	3.20E-01	2.40E-01	1.60E-01	8.00E-02	0.00E+00	0.00E+00	...	0.00E+00	0.00E+00
6.00E-10		1.67E-01	2.78E-01	2.22E-01	1.67E-01	1.11E-01	5.56E-02	0.00E+00	...	0.00E+00	0.00E+00
.		.	.	.	.	.	.	.	.	.	.
.		.	.	.	.	.	.	.	...	.	.
.		.	.	.	.	.	.	.	.	.	.
9.00E-01		1.11E-10	2.22E-10	2.22E-10	2.22E-10	2.22E-10	2.22E-10	2.22E-10	...	0.00E+00	0.00E+00
1.00E+00		1.00E-10	2.00E-10	2.00E-10	2.00E-10	2.00E-10	2.00E-10	2.00E-10	...	2.00E-02	0.00E+00

Table 5
Probability density function for error EG_1a in each source.

p	$P(p)_{CREAM}$	$P(p)_{HEART}$	$P(p)_{THERP}$	p	$P(p)_{CREAM}$	$P(p)_{HEART}$	$P(p)_{THERP}$	p	$P(p)_{CREAM}$	$P(p)_{HEART}$	$P(p)_{THERP}$
0.00E+00	2.34E-07	2.29E-09	6.24E-08	4.00E-07	4.63E-04	4.57E-06	1.25E-04	8.00E-04	2.79E-02	4.56E-03	3.83E-02
1.00E-10	4.67E-07	4.57E-09	1.25E-07	5.00E-07	4.62E-04	4.57E-06	1.25E-04	9.00E-04	2.25E-02	4.56E-03	3.54E-02
2.00E-10	4.67E-07	4.57E-09	1.25E-07	6.00E-07	4.60E-04	4.57E-06	1.25E-04	1.00E-03	9.79E-02	2.51E-02	1.35E-01
3.00E-10	4.67E-07	4.57E-09	1.25E-07	7.00E-07	4.59E-04	4.57E-06	1.25E-04	2.00E-03	6.09E-02	4.54E-02	1.25E-01
4.00E-10	4.67E-07	4.57E-09	1.25E-07	8.00E-07	4.58E-04	4.57E-06	1.25E-04	3.00E-03	2.63E-02	4.52E-02	7.08E-02
5.00E-10	4.67E-07	4.57E-09	1.25E-07	9.00E-07	4.56E-04	4.57E-06	1.25E-04	4.00E-03	1.31E-02	4.48E-02	4.30E-02
6.00E-10	4.67E-07	4.57E-09	1.25E-07	1.00E-06	2.50E-03	2.52E-05	6.85E-04	5.00E-03	7.19E-03	4.41E-02	2.75E-02
7.00E-10	4.67E-07	4.57E-09	1.25E-07	2.00E-06	4.43E-03	4.57E-05	1.24E-03	6.00E-03	4.22E-03	4.31E-02	1.84E-02
8.00E-10	4.67E-07	4.57E-09	1.25E-07	3.00E-06	4.31E-03	4.57E-05	1.24E-03	7.00E-03	2.54E-03	4.18E-02	1.30E-02
9.00E-10	4.67E-07	4.57E-09	1.25E-07	4.00E-06	4.20E-03	4.57E-05	1.23E-03	8.00E-03	1.49E-03	4.02E-02	9.60E-03
1.00E-09	2.58E-06	2.52E-08	6.86E-07	5.00E-06	4.11E-03	4.57E-05	1.23E-03	9.00E-03	7.58E-04	3.84E-02	7.48E-03
2.00E-09	4.67E-06	4.57E-08	1.25E-06	6.00E-06	4.01E-03	4.57E-05	1.22E-03	1.00E-02	1.11E-03	1.58E-01	9.43E-03
3.00E-09	4.67E-06	4.57E-08	1.25E-06	7.00E-06	3.93E-03	4.57E-05	1.21E-03	2.00E-02	2.33E-04	1.44E-01	1.58E-03
4.00E-09	4.67E-06	4.57E-08	1.25E-06	8.00E-06	3.85E-03	4.57E-05	1.21E-03	3.00E-02	6.11E-05	9.16E-02	2.72E-04
5.00E-09	4.67E-06	4.57E-08	1.25E-06	9.00E-06	3.77E-03	4.57E-05	1.20E-03	4.00E-02	2.39E-05	6.66E-02	6.95E-05
6.00E-09	4.67E-06	4.57E-08	1.25E-06	1.00E-05	2.03E-02	2.51E-04	6.43E-03	5.00E-02	1.17E-05	4.96E-02	2.36E-05
7.00E-09	4.67E-06	4.57E-08	1.25E-06	2.00E-05	3.17E-02	4.57E-04	1.10E-02	6.00E-02	6.44E-06	3.56E-02	9.76E-06
8.00E-09	4.67E-06	4.57E-08	1.25E-06	3.00E-05	2.81E-02	4.57E-04	1.05E-02	7.00E-02	3.78E-06	2.35E-02	4.66E-06
9.00E-09	4.67E-06	4.57E-08	1.25E-06	4.00E-05	2.54E-02	4.57E-04	1.01E-02	8.00E-02	2.19E-06	1.38E-02	2.60E-06
1.00E-08	2.57E-05	2.52E-07	6.86E-06	5.00E-05	2.32E-02	4.57E-04	9.80E-03	9.00E-02	1.11E-06	6.14E-03	1.74E-06
2.00E-08	4.68E-05	4.57E-07	1.25E-05	6.00E-05	2.14E-02	4.57E-04	9.53E-03	1.00E-01	1.64E-06	1.98E-04	8.26E-07
3.00E-08	4.68E-05	4.57E-07	1.25E-05	7.00E-05	1.99E-02	4.57E-04	9.29E-03	2.00E-01	3.04E-07	1.65E-07	1.43E-07
4.00E-08	4.68E-05	4.57E-07	1.25E-05	8.00E-05	1.86E-02	4.57E-04	9.08E-03	3.00E-01	6.07E-08	3.49E-09	3.25E-08
5.00E-08	4.68E-05	4.57E-07	1.25E-05	9.00E-05	1.75E-02	4.57E-04	8.89E-03	4.00E-01	1.70E-08	1.90E-10	1.03E-08
6.00E-08	4.68E-05	4.57E-07	1.25E-05	1.00E-04	9.04E-02	2.51E-03	4.42E-02	5.00E-01	5.73E-09	1.56E-11	3.90E-09
7.00E-08	4.68E-05	4.57E-07	1.25E-05	2.00E-04	1.14E-01	4.57E-03	6.96E-02	6.00E-01	2.10E-09	1.73E-12	1.64E-09
8.00E-08	4.67E-05	4.57E-07	1.25E-05	3.00E-04	8.60E-02	4.56E-03	6.20E-02	7.00E-01	7.47E-10	2.39E-13	7.04E-10
9.00E-08	4.67E-05	4.57E-07	1.25E-05	4.00E-04	6.69E-02	4.56E-03	5.57E-02	8.00E-01	2.24E-10	3.61E-14	2.74E-10
1.00E-07	2.57E-04	2.52E-06	6.86E-05	5.00E-04	5.32E-02	4.56E-03	5.03E-02	9.00E-01	3.67E-11	3.13E-15	5.79E-11
2.00E-07	4.66E-04	4.57E-06	1.25E-04	6.00E-04	4.27E-02	4.56E-03	4.57E-02	1.00E+00	0.00E+00	0.00E+00	0.00E+00
3.00E-07	4.64E-04	4.57E-06	1.25E-04	7.00E-04	3.46E-02	4.56E-03	4.17E-02				

- TESEO: it was not possible to identify any correlation between the data presented in TESEO [78] and the data available for this work with Reason's error types. Thus, these data are not being considered in this work.
- THERP: the data were correlated to the three performance levels of the SRK model. In order to find the most probable types of errors in each level, the diagram presented in Fig. 4 was applied, and later the descriptions of the actions were compared with the characteristics of the error types (summarized in Table 3), and the correlations considered more likely were kept. Some THERP tables [17] had associated actions at different levels (e.g., Tables 20–7, item 1: rule level, and Tables 20–7, item 5: skill level). Tables 20–1 and 20–2 were not considered as being based on data from other tables (they are employed in the screening process). For the following reasons, some items from other tables were also not considered: (1) database is the same as another item: (a) Tables 20–12, items 2–4 in relation to Tables 20–9; (b) Tables 20–11, item 1 in relation to Tables 20–10, item 2, and (c) Tables 20–5, items 3 and 4 in relation to Tables 20–5, items 1 and 2; (2) does not present quantitative data: (a) Tables 20–9, item 1; (b) Tables 20–10, item 8; (c) Tables 20–11, items 7 and 8, and (d) Tables 20–12, items 1, 8a, 8b and 8c, and (3) model approximations: Tables 20–3, items 1,7 and 14 – the time considered for the execution of the action is insufficient (error may not have occurred).

The quantification of the probabilities of the error types associated to the data sources was done through BNs. This process is illustrated in a simplified way in Fig. 3 (upper part). Thus, the BNs were constructed for each action, in order to estimate the probability functions of the error types in said actions. Then, these estimates were combined to obtain a unique estimate for each source. As this quantification process is similar for each data source and for each type of error, this topic presents an example for which we obtain the probability function for the error types associated with action C_E1 ("Execution: wrong action type") presented in CREAM – the error types EG_1a, EG_1e and EG_1h were associated

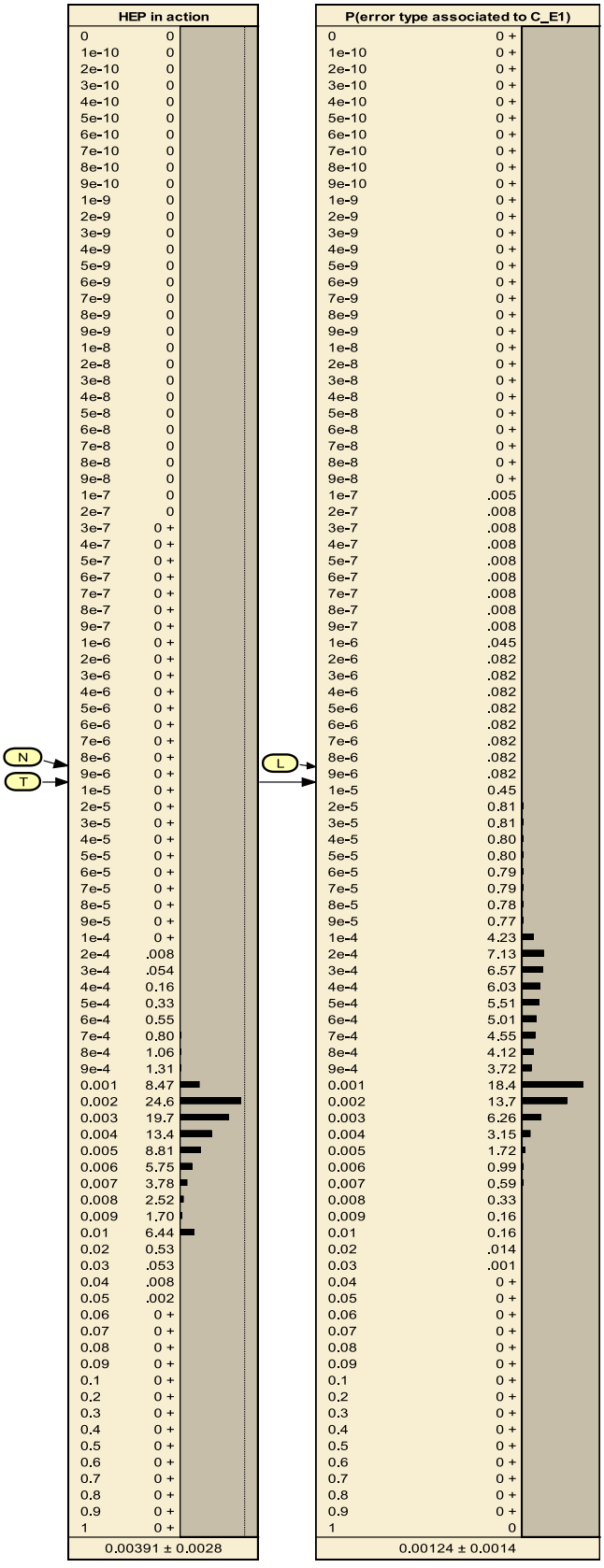


Fig. 6. BN for probability variability of error EG_1a.

with this action –, and obtaining the variability of the probability of error type EG_1a (double-capture slip).

The BN for estimating the probability density functions of the error types associated with action C_E1 is shown in Fig. 5. In the completion of the CPT (Conditional Probability Table) of the node "HEP in Action" shown in Fig. 5, a lognormal distribution was considered for the HEP – Swain and Guttman [17] justified the adoption of lognormal distribution for generic HEPs based on empirical results of their work on human performance –, with median 3.00E-03 and EF (Error Fraction) equal to 3, according to the values presented by bounds in CREAM [33]. The values for the parameters were sent to the deterministic nodes "N" ($\nu = -5.81$) and "T" ($\tau = 0.67$), relative to the mean and standard deviation of the normal distribution associated, respectively. The CPT filling of the node "P (Error type associated with C_E1)" was performed by means of Eq. (1) [50].

$$\boldsymbol{fdp}(\boldsymbol{phep},\boldsymbol{l}) = \begin{cases} \dfrac{(\boldsymbol{l}-1)}{(\boldsymbol{hep}-\boldsymbol{p})}\left(\dfrac{\boldsymbol{hep}-\boldsymbol{p}}{\boldsymbol{hep}}\right)^{l-1}, & 0 \le p < hep \\ 0, & hep \le p \le 1 \end{cases} \tag{1}$$

The probability density function of the type of error presented in Eq. (1) is conditioned to l and hep, which are the variables represented in the BN of Fig. 5 as the parent nodes of the "P (Error type associated with C_E1)" – node "L" and "HEP in Action", respectively. Node "L" is deterministic and, in the case of C_E1, is equal to 3 (since there are three types of error associated with this action). In order to fill the CPT of node "P (Error type associated with C_E1)", partially reproduced in Table 4, the function presented in Eq. (1) was discretized according to Eq. (2) – considering the states p_i for this node, according to a logarithmic scale ranging from 0 to 1, as shown in Fig. 5.

$$\boldsymbol{P}(\boldsymbol{p_i}\boldsymbol{hep},\boldsymbol{l}) = \begin{cases} \dfrac{\boldsymbol{p}_{i+1}-\boldsymbol{p}_{i-1}}{2} * fdp(\boldsymbol{p_i}\boldsymbol{hep},\boldsymbol{l}), & \boldsymbol{p}_i \neq 0,\ 1 \\ 5.10^{-11} * \boldsymbol{fdp}(0\boldsymbol{hep},\boldsymbol{l}), & \boldsymbol{p}_i = 0 \\ 5.10^{-2} * fdp(1\boldsymbol{hep},\boldsymbol{l}), & \boldsymbol{p}_i = 1 \end{cases} \tag{2}$$

The estimation of the probability density functions of the error types associated with action C_E1 were obtained directly from the solution of the BN in Fig. 5 for the node "P (Error type associated with C_E1)". The actions collected from the data sources allowed 15 estimates of the probability density function for the error EG_1a, with data from three sources (CREAM, HEART and THERP). Thus, for each data source, the estimates were combined (regardless of any prevalence among samples), according to Eq. (3), where n refers to the number of estimates at source (3 for CREAM, 2 for HEART and 10 for THERP). The results are reproduced in Table 5.

$$\boldsymbol{P}(\boldsymbol{p})_{Source} = \frac{\sum_{Action} \boldsymbol{P}(\boldsymbol{p})_{Action}}{\boldsymbol{n}} \tag{3}$$

3.2.3. Step 3 – calculation of the error type probability variability

Continuing the example in the previous topic, starting from the functions presented in Table 5, the BN shown in Fig. 6 was constructed, which allows to determine the variability $\boldsymbol{\varphi}(\boldsymbol{p})_{EG\_1a}$ of the error EG_1a probability, and to update it by means of evidence.

The CPTs for the nodes "CREAM", "HEART" and "THERP" were filled with the data presented in Table 5, considering the p values between 1.00E-06 and 9.00E-02 – where the probability of p to be in this interval is greater than 99.5%, i.e., F(9.00E-02) – F(9.00E-05) > 99.5%. Thus, the values of p determined the states for these nodes, as shown in Fig. 6; the states are presented in percentage. The other CPTs were filled in the following way: node "Observations": this node is deterministic and displays the number of observations of an action in which the intention is to

Table 6
Variability for the error types presented in Table 3.

Performance level	Error type	5th percentile	Median	95th percentile	Mean
Skill	EG_1a	3.00E-05	1.00E-03	4.00E-02	7.32E-03
	EG_1b	1.00E-04	7.00E-03	7.00E-02	1.72E-02
	EG_1c	8.00E-05	2.00E-03	7.00E-02	1.35E-02
	EG_1d	3.00E-05	1.00E-03	6.00E-02	1.08E-02
	EG_1e	3.00E-05	1.00E-03	6.00E-02	1.15E-02
	EG_1f	9.00E-05	3.00E-03	7.00E-02	1.44E-02
	EG_1g	5.00E-05	1.00E-03	8.00E-02	1.33E-02
	EG_1h	5.00E-05	1.00E-03	8.00E-02	1.32E-02
Rule	EG_2a	3.00E-05	2.00E-03	5.00E-02	9.79E-03
	EG_2b	2.00E-06	1.00E-03	9.00E-02	1.56E-02
	EG_2c	3.00E-05	2.00E-03	7.00E-02	1.28E-02
	EG_2d	4.00E-05	2.00E-03	1.00E-01	1.80E-02
	EG_2e	2.00E-05	1.00E-03	8.00E-02	1.53E-02
	EG_2f	3.00E-05	2.00E-03	9.00E-02	1.68E-02
	EG_2g	3.00E-06	1.00E-03	9.00E-02	1.52E-02
	EG_2h	2.00E-06	2.00E-03	9.00E-02	1.63E-02
	EG_2iI	9.00E-05	8.00E-03	9.00E-02	2.04E-02
	EG_2iII	8.00E-05	4.00E-03	7.00E-02	1.54E-02
	EG_2iIII	9.00E-05	6.00E-03	8.00E-02	1.72E-02
Knowledge	EG_3a	3.00E-06	4.00E-03	8.00E-02	1.64E-02
	EG_3b	3.00E-06	3.00E-03	8.00E-02	1.44E-02
	EG_3c	3.00E-06	3.00E-03	4.00E-02	9.97E-03
	EG_3d	3.00E-06	5.00E-03	6.00E-02	1.42E-02
	EG_3e	3.00E-06	4.00E-03	9.00E-02	1.67E-02
	EG_3f	3.00E-06	5.00E-03	1.00E-01	2.23E-02
	EG_3g	3.00E-06	5.00E-03	9.00E-02	1.73E-02
	EG_3h	3.00E-06	5.00E-03	9.00E-02	1.69E-02
	EG_3i	2.00E-06	2.00E-03	8.00E-02	1.34E-02
	EG_3jI	4.00E-07	7.00E-03	1.00E-01	2.29E-02
	EG_3jII	3.00E-06	7.00E-03	1.00E-01	2.01E-02
	EG_3jIII	3.00E-06	5.00E-03	6.00E-02	1.42E-02
	EG_3jIV	1.00E-06	4.00E-03	9.00E-02	1.68E-02
	EG_3jV	1.00E-06	1.00E-03	3.00E-02	7.09E-03
	EG_3jVI	1.00E-06	1.00E-03	3.00E-02	7.09E-03

investigate the occurrence of the error type – i.e., it brings the number of opportunities observed for the occurrence of the error type; node "Observed Errors": the CPT has been completed considering a binomial distribution for the evidence of the error type EG_1a; node "Subpopulation weight": completion of the CPT was done considering the same representativeness to each subpopulation – it is expected that these weights will be changed in more advanced design stages, or as it will be possible to say which subpopulation best represents the specific case (e.g., which data source best fits the evidence obtained from system operation). This possibility was not explored in this first paper. It will be presented in a subsequent work, with an improvement of the model through the expert elicitation. In addition, this node can be explored to verify the model consistency, in the model validation or/and in the model refinement process (also in more advanced stages of the project); node "EG_1a": this node is deterministic, and the completion of its CPT considered that the conditional probability of a state, given a subpopulation, is 100% when the state of that subpopulation is equal to the node state, and 0% otherwise.

The estimated variability $\boldsymbol{\varphi}(\boldsymbol{p})_{EG\_1a}$ for the probability of error type EG_1a is obtained directly from the solution of the BN in Fig. 6 for node "EG_1a". The procedure presented for obtaining $\boldsymbol{\varphi}(\boldsymbol{p})_{EG\_1a}$ was repeated for all types of error presented in Table 3. The results were reproduced in Table 6, presenting 5th and 95th percentiles, medians, and means of the variabilities. As in Table 3, the error types in Table 6 were organized according to the performance levels proposed in the SRK model.

3.2.4. Step 4 – calculation of the HEP for generic actions

The diagram shown in Fig. 4 were applied to the generic actions presented in Bloom's taxonomy. Table 6 presents the types of errors associated with actions classified in the cognitive domain. In this domain, the categories of the dimension "knowledge" did not allow the direct classification of human actions. Only an inconclusive correlation between these categories and the performance levels of the SRK model was proposed: (a) effective knowledge: skill level; (b) procedural knowledge: rule level, and; (c) conceptual or metacognitive knowledge: knowledge level. Thus, to classify human actions, only the cognitive process dimension was used, and the errors of each level of performance were correlated. In Table 7, the last column summarizes what was assumed to allow the association of error types with their actions.

Table 8 presents the types of errors associated with actions classified in the psychomotor domain. In filling this table, the cognitive and affective processes involved were neglected. Focusing on psychomotor movement, all action categories in this domain were associated with performance at the skill level. The last column of Table 8 provides a summary of what was assumed to allow these associations. The number of errors associated with the different categories of actions is a reflection of the incipient detail of these categories. The HEPs for the action listed in Tables 7 and Table 8 were estimated considering the variability for the error types listed in Table 6. Assuming that the error types are independent, the relation presented in Eq. (4) is established, which is derived from the inclusion-exclusion principle, where $\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_n$ are possible probabilities for the n error types associated to the action.

$$\mathrm{HEP}(\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots \boldsymbol{p}_n) = \sum_{i=1}^{n} \boldsymbol{p}_i - \sum_{1 \le i < j \le n} \left(\boldsymbol{p}_i * \boldsymbol{p}_j\right) + \sum_{1 \le i < j < k \le n} \left(\boldsymbol{p}_i * \boldsymbol{p}_j * \boldsymbol{p}_k\right) - \ldots . \tag{4}$$

Note that each modeled action admits different values for the HEP, considered independent estimates and determined by the combinations of possible probabilities for the error types associated with the action – e.g. according to Eq. (4). Thus, given the probability density functions of the error types, the probability of each combination can be calculated by means of Eq. (5).

Table 7
Association of error types to actions in the cognitive domain.

Category	Cognitive process		Performance level– SRK model: Skill								Rule										Knowledge												Remarks
			EG_1a	EG_1b	EG_1c	EG_1d	EG_1e	EG_1f	EG_1g	EG_1h	EG_2a	EG_2b	EG_2c	EG_2d	EG_2e	EG_2f	EG_2g	EG_2h	EG_2i	EG_2ii	EG_2iii	EG_3a	EG_3b	EG_3c	EG_3d	EG_3e	EG_3f	EG_3g	EG_3h	EG_3i	EG_3ii	EG_3iii	EG_3iv	EG_3v	EG_3vi	
Remember	*Recognize*	A_C_1a									X	X	X	X	X	X		X				X		X											This action assumes the comparison between what is presented and prior knowledge. Thus, it is considered that the error occurs in the comparison (attention to available data or choice of knowledge) or if the individual does not have the knowledge because he did not learn correctly. Note that the EG_2g error assumes a conscious choice between rules (i.e., this is only possible when the rule has already been located).
	Recollect	A_C_1b		X	X		X	X	X	X							X		X	X	X														This action assumes the comparison between what is presented and prior knowledge. Thus, it is considered that the error occurs in the comparison or the individual does not have the knowledge because he did not learn correctly. Note that the EG_2g error assumes a conscious choice between rules (i.e., this is only possible when the rule has already been located).
Understand	*Interpret*	A_C_2a										X	X					X					X										X	X	Regarding performance at the rule level, errors are related to the flow of information (some rule is considered to be conversion). In the performance at the level of knowledge, the possibility of low memory capacity or the concentration of the individual in other tasks is being considered.
	Exemplify	A_C_2b																				X		X			X	X						X	X	It is assumed that the example may be wrong (centered on irrelevant or mismatched aspects) or incomplete.
	Classify	A_C_2c									X			X	X	X	X																		It is being considered that the individual may not understand the classification rule or has difficulty to understand the item to be classified.
	Sum up	A_C_2d																				X		X			X							X	X	In constructing a summary, the individual can focus on irrelevant aspects or develop a very specific aspect, disfavoring the consideration of relevant aspects. It may occur that the individual wrongly judges to have considered everything.
	Infer	A_C_2e																				X			X	X		X		X	X	X	X		In the process of inference the individual may have difficulty dealing with complex problems (e.g., evolution in time, causal model construction, and exponential evolution), favoring correlations that invalidate the conclusions.
	Compare	A_C_2f																						X	X	X		X	X						It is being considered that a rule for comparison has not been previously defined, which favors error in the judgment of the individual. In addition, illusory correlations may occur, the evaluation may not be independent.
	Explain	A_C_2g																				X					X			X	X	X	X	X	X	Errors related to individual difficulties in building causal relationships and dealing with complex tasks may occur.
Apply	*Execute*	A_C_3a	X	X	X	X	X	X	X	X																										A generic implementation is being considered.
	Implement	A_C_3b									X	X	X	X	X	X	X	X																		It is being considered that the rules learned are correct.
Analyze	*Differentiate*	A_C_4a																				X		X	X									X	X	Errors related to attention and selection of relevant parts in the analysis process were associated.
	Organize	A_C_4b																					X					X		X	X	X	X			Errors related to the determination, in the analysis process, of how the elements work or fit in the process were associated.
	Assign	A_C_4c																								X	X		X							Errors related to the determination, in the analysis process, of the purposes, deviations and value of the presented material were associated.
Evaluate	*Check*	A_C_5a									X	X	X	X	X	X	X	X	X	X	X															Verification is considered to be based on pre-defined standards.
	Criticize	A_C_5b																				X	X	X	X	X	X	X	X	X	X	X	X	X	X	The complexity of the action does not allow the exclusion of any kind of error.
Create	*Generate*	A_C_6a																				X	X	X	X	X	X	X	X	X	X	X	X	X	X	The complexity of the action does not allow the exclusion of any kind of error.
	Plan	A_C_6b																				X	X	X	X	X	X	X	X	X	X	X	X	X	X	The complexity of the action does not allow the exclusion of any kind of error.
	Produce	A_C_6c																				X	X	X	X	X	X	X	X	X	X	X	X	X	X	The complexity of the action does not allow the exclusion of any kind of error.

Table 8
Association of error types to actions in the psychomotor domain.

Category		Performance level – SRK model: Skill								Rule										Knowledge														Remarks
		EG_1a	EG_1b	EG_1c	EG_1d	EG_1e	EG_1f	EG_1g	EG_1h	EG_2a	EG_2b	EG_2c	EG_2d	EG_2e	EG_2f	EG_2g	EG_2h	EG_2i	EG_2iI	EG_2iII	EG_3a	EG_3b	EG_3c	EG_3d	EG_3e	EG_3f	EG_3g	EG_3h	EG_3i	EG_3jI	EG_3jII	EG_3jIII	EG_3jIV	EG_3jV	EG_3jVI	
Reflexive Motion	A_P_1			X			X																												It was considered that the error occurs in this action when the individual loses the consciousness of what he/she is doing, failing to present a reflexive response to a stimulus. Errors related exclusively to perception were ignored.
Basic Movement	A_P_2	X	X	X		X	X	X																											Errors related exclusively to perception were ignored. It is being considered that the order is not relevant.
Perceptive Ability	A_P_3			X	X		X																												Errors related to perception were considered.
Physical Skill	A_P_4	X	X	X		X	X	X	X																										Errors related exclusively to perception were ignored.
Qualified Movement	A_P_5	X	X	X		X	X	X	X																										Errors related exclusively to perception were ignored.
Non-verbal communication	A_P_6	X	X	X		X	X	X	X																										Errors related exclusively to perception were ignored.

$$P[HEP(p_1,p_2,\ldots p_i,\ldots p_n)]=P(p_1)P(p_2)\ldots P(p_i)\ldots P(p_n)$$
$$=fdp(p_1)fdp(p_2)\ldots fdp(p_i)\ldots fdp(p_n)d_{p_1}d_{p_2}\ldots d_{p_i}\ldots d_{p_n} \quad (5)$$

Thus, considering the results of Eqs. (4) and (5), the probability of each HEP' of an action is obtained by means of Eq. (6),

$$P(HEP') = \sum_{\forall\ p_1,\ p_2,\ldots p_i,\ldots p_n:\ HEP'=HEP(p_1,\ p_2\ldots p_i,\ldots p_n)} P[HEP(p_1,p_2,\ldots p_i,\ldots p_n)] \quad (6)$$

It is interesting to note that some of the actions listed in Table 7 and in Table 8 were associated with a large number of error types – e.g., action A_C_6 of Table 7, to which fifteen different types of error were associated. In these cases, the computation of the HEP probability function as proposed in Eq. (6) was unfeasible due to the required computational time – e.g., in action A_C_6, it would be necessary to evaluate 2.86E+29 combinations of probabilities of error types (considering 92 possible probabilities for each type) and their HEPs. This situation is incompatible with the need to apply the prospective performance model in a design context (e.g., there may be a need for several model updates during the design process). Thus, an approximate numerical method was adopted for this calculation (Monte Carlo Method – MCM [79]). The results obtained are summarized in Table 9, which presents the 5th and 95th percentiles, the medians, and the HEP averages for each generic action – the actions can be identified by the codes, which refer to Table 7 and in Table 8.

In order to verify the results presented in Table 9, the robustness of the approximate numerical method was studied – regarding its convergence and the number of iterations needed. As an example of the results of this study, Fig. 7 compares the probability function for HEP in action A_P_1 obtained in three ways: (a) by MCM with 10^3 iterations – i.e., n equal to 10^3; (b) by MCM with n equal to $2*10^7$ (the same number used for obtaining the results presented in Table 12), and; (c) Accurately– i.e., applying Eq. (6). The data presented in Fig. 7 indicate the convergence of the results as the number of repetitions increases, and demonstrate the adequacy of the approach using MCM.

As mentioned earlier, the validation of the BN model for obtaining HEPs is expected during the design (as more data is available for comparison). Alternatively, the results for applying the model can be compared with the results obtained by other HRA techniques. An example of this alternative was presented by the authors in Ref. [50] – when the results of TECHR (Technique for the Early Consideration of Human Reliability) were compared with those of THERP. As expected, that application showed that the results of the generic model are more conservative than those of the specific application (that reference considers the operation of merchant ships).

Still on the validation process, it is worth noting that the results of the BNs were validated by comparing the results of the HRA techniques used as data sources, and by comparing the results of the direct application of the equation presented in this paper – ie, the results obtained through NETICA were compared with those obtained through the equations. The deviations observed in relation to the data from the HRA techniques were attributed to the discretization of the continuous functions (the BN model used discrete nodes).

4. Design of the FSPCS operation

The FSPCS equipment was designed to cool the compartments of a FSP (Fuel Storage Pool) storing the FE (Fuel Element) removed from a PWR (Pressurized Water Reactor), which still produce residual heat and maintain the ability to contaminate the cooling water – in the absence of cooling, this heat can damage the FE cladding and expose its radioactive contents, thus severely contaminating the environment.

This section presents the conception of the FSPCS operation, focusing on the configuration of human factors – without changing the equipment of the system. This was done by applying the methodology proposed in Section 2, as described in the following subsections – organized according to the phases proposed in Fig. 1.

To facilitate the understanding of this case study, the scheme in Fig. 8 presents the order of realization of the methodology phases (according to the flowchart presented in Fig. 1). This scheme presents the phases that were actually performed (necessary) in each iteration and the subsections of this section that report their results. In this figure, the hatched activities are those that were effectively developed – the others used resources already developed in previous iterations (when there was no change in relation to the previous iteration or cycle).

4.1. Phase 1 – scenario

The scheme presented in Fig. 9 was developed to facilitate the FSPCS description – the equipment involved in the operation can be identified by the following codes: (FE) fuel element; (T) heat exchanger; (B) pump; (P) control panel; (S) sound and / or light signal, and (V) valve. In this scheme, the continuous lines represent the pipes considered in this work, whereas the dotted lines represent the control, instrumentation and power cables that connect the FSPCS components; the dashed lines represent the pipes of the systems not modeled in this work (interface systems).

Additionally, the sensors which activate the monitoring and control signals are represented by circles positioned on the monitored equipment. Fig. 9 identifies one of the FSPCS operational modes, in which the FEs are positioned in compartments I and III of the FSP, cooled by the heat exchangers T1 and T3 (shaded in Fig. 9) and with circulation by pumps B1 and B3 (shaded in Fig. 9), respectively – the closed valves are in black (e.g., V57, close to compartment II). Table 10 presents the

Table 9
HEP for the action presented in Table 7 and in 8.

Performance Level	Action	5th percentile	Median	95th percentile	Mean
Skill	A_C_1b	8.00E-03	5.00E-02	3.00E-01	7.73E-02
	A_C_3a	1.00E-02	7.00E-02	3.00E-01	9.38E-02
	A_P_1	7.00E-04	1.00E-02	1.00E-01	2.69E-02
	A_P_2	8.00E-03	5.00E-02	2.00E-01	7.20E-02
	A_P_3	1.00E-03	2.00E-02	1.00E-01	3.69E-02
	A_P_4	1.00E-02	6.00E-02	3.00E-01	8.40E-02
	A_P_5	1.00E-02	6.00E-02	3.00E-01	8.40E-02
	A_P_6	1.00E-02	6.00E-02	3.00E-01	8.40E-02
Rule	A_C_1a	1.00E-02	7.00E-02	3.00E-01	9.69E-02
	A_C_1b	5.00E-03	5.00E-02	2.00E-01	6.41E-02
	A_C_2a	9.00E-04	2.00E-02	2.00E-01	4.28E-02
	A_C_2c	4.00E-03	5.00E-02	2.00E-01	7.03E-02
	A_C_3b	1.00E-02	9.00E-02	3.00E-01	1.11E-01
	A_C_5a	4.00E-02	1.00E-01	4.00E-01	1.57E-01
Knowledge	A_C_1a	4.00E-04	1.00E-02	1.00E-01	2.55E-02
	A_C_2a	9.00E-04	1.00E-02	1.00E-01	2.74E-02
	A_C_2b	1.00E-02	6.00E-02	2.00E-01	7.47E-02
	A_C_2d	6.00E-03	4.00E-02	2.00E-01	5.90E-02
	A_C_2e	4.00E-02	1.00E-01	3.00E-01	1.39E-01
	A_C_2f	1.00E-02	6.00E-02	2.00E-01	7.02E-02
	A_C_2g	3.00E-02	1.00E-01	3.00E-01	1.29E-01
	A_C_4a	6.00E-03	4.00E-02	1.00E-01	5.17E-02
	A_C_4b	2.00E-02	1.00E-01	3.00E-01	1.10E-01
	A_C_4c	2.00E-03	3.00E-02	2.00E-01	5.29E-02
	A_C_5b	7.00E-02	2.00E-01	4.00E-01	2.06E-01
	A_C_6a	7.00E-02	2.00E-01	4.00E-01	2.06E-01
	A_C_6b	7.00E-02	2.00E-01	4.00E-01	2.06E-01
	A_C_6c	7.00E-02	2.00E-01	4.00E-01	2.06E-01

characteristics of the FSPCS considered important for its operational procedure design.

4.1.1. Design constraint

In addition to the aforementioned characteristics, the following restrictions for the system operation design are presented:

- Reliability: the probability of not cooling the FE with significant residual heat must be less than 1.00E-07 per year – this condition is presumed when the FSP water temperature exceeds 60°C. The FSPCS failure rate must be less than 1.00E-03 per year.
- Fluid mixing: in order to minimize the generation of tailings, the fluids in the different compartments must be independently cooled, e.g., the same heat exchanger or circuit section must not participate in the cooling of two compartments simultaneously.

According to this reliability criterion, the frequency of cooling lack should be less than 1.00E-03 per year, specifically for the FSPCS. Note that the lack of water cooling by the FSPCS does not necessarily result in a lack of FE cooling, i.e., the lack of cooling by the FSPCS is an initiating event for other actions, including the FSPCS recovery through corrective maintenance or its operating without meeting the non-mixing criteria. These conditions are not discussed in this text paper.

4.1.2. Reliability data

The equipment comprising the FSPCS were studied and its functions, failure modes (considered most influential to the function of each type of component) and probability of failure (in an 80 h operation, which is the expected actuation time for FSPCS) were obtained. Exponential distributions were adopted for the equipment failure times. The failure rates and the probabilities of failure on demand were obtained from Center for Chemical Process Safety – CCPS [80] and SINTEF [,81]. Only the components represented in the arrangement of in Fig. 9 (e.g., valve V53 of the DS – Drainage System) were considered for the interface systems.

4.1.3. Equipment failure frequency

The event tree reproduced in Fig. 10, valid for any FSPCS operational mode, was elaborated to calculate the frequency of fulfillment of the cooling function by the FSPCS. From the information available for this work, it is not possible to determine the operational modes that will be more (or less) demanded in the system life. Thus, the events presented in Fig. 10 are analyzed considering the worst case scenario. The event EI refers to the need to use FSPCS, and is associated with the need for FE load in the FSP. Thus, the frequency λ(EI) of the cooling requirement was estimated considering that the FSP receives an annual load of FE. In such situation, the frequency λ(EI) was equal to 1/year. As ordered in this event tree, the need to use the FSP is related to the events listed in Table 11.

Thus, in case of failure, the possibility of only one realignment is considered – without this assumption, the frequency of lack of cooling obtained from the event tree may be smaller, and the tree should be changed to fit said hypothesis –, and the degraded operational mode to be obtained by this realignment depends on the components which have failed (detected in event #D2). Additionally, the FE must be introduced into the FSP after the initial alignment (event #A1). The FSPCS failure frequency λ(¬FSPCS), considering the event tree in Fig. 10, can be calculated according to Eq. (7):

$$\lambda(\neg FSPCS) = \lambda(EI)\{1 - P(\#A1)P(\#M1)[P(\#E1) + P(\neg\#E1)P(\#D1)] [P(\#E2) + P(\neg\#E2\_REC)P(\#D2)P(\#E3)P(\#A2)P(\#M2) P(\#E4)]\} \quad (7)$$

The events #A1, #A2, #M1, #M2, #D1 and #D2 have their probabilities estimated in Phase 8 – System Reliability, in which the reliability of the possible solutions is compared to the reliability criterion presented in Eq. [8]:

$$\lambda(\neg FSPCS) \leq 1,00E-3/year \quad (8)$$

The probabilities for events #E1, #E2, #E3 and #E4 can be estimated based on the information available on the FSPCS, since it is not intended to change the already conceived part of the system. As there is no a priori information on the frequency of use of each FSPCS operating mode, such probabilities have been conservatively estimated (as reported below).

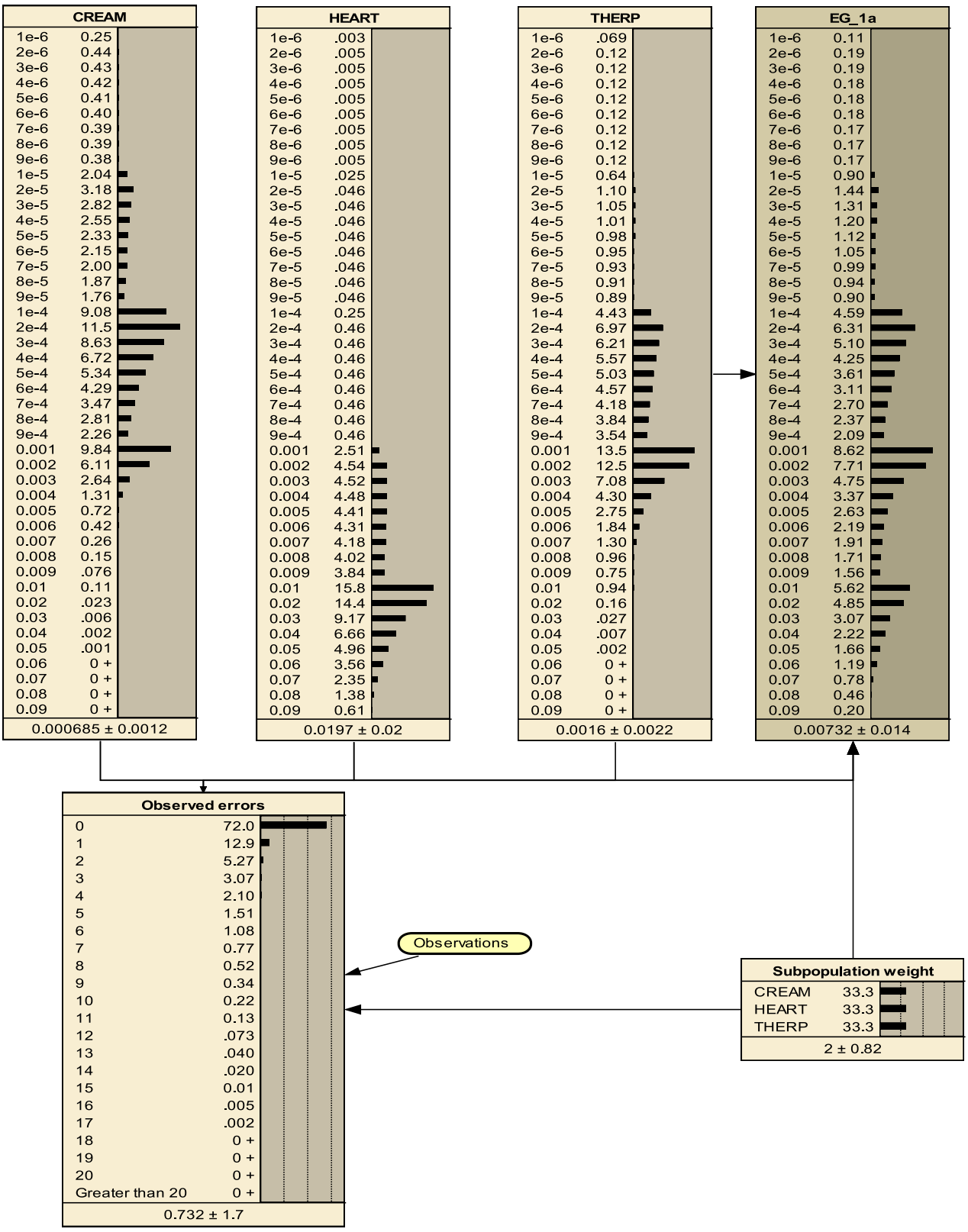


Fig. 7. Probability functions for HEP in action A_P_1.

In order to calculate the probabilities P(¬#E1) of failure in event #E1, reconfiguring the system starting from mode "O" to one of the normal operational modes was deemed necessary. The alignment of the equipment in each normal operational mode was studied, thus allowing for the identification of the equipment which must be actuated for such mode change. The failure on demand for one or more actuated panels and valves is considered for the occurrence of event ¬#E1 – failures on pump demand (including the redundant ones) are considered in event #E2. Thus, for each state change, the probability of failure of one or more equipment was calculated. The change to mode "B" presents the

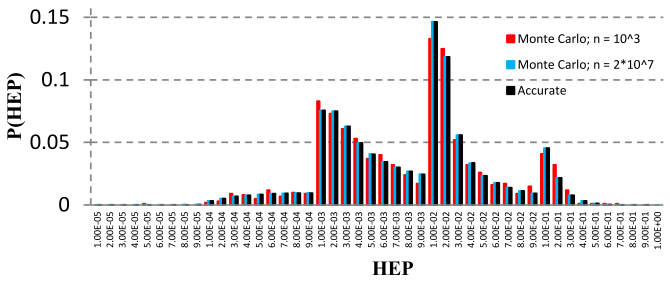


Fig. 8. Activities carried out in the development of the FSPCS operational procedure.

highest probability of failure (equal to 6.74E-04), thus representing the worst case scenario for the probability of the event ¬#E1. Therefore, this is the probability adopted for the solution of Eq. (7), since it is not possible to know the relative frequency (throughout the system's life cycle) between the operational modes.

Similarly to the event #E1 analysis, the need to reconfigure the system is considered to calculate the probabilities of failure for event #E3 – from one of the modes "A", "B", "C", "D" or "E" to an equivalent degraded mode, i.e., cooling the same set of compartments. This calculation is performed for each possible change. The highest probabilities of failure refer to the changes to a degraded mode from "A", with $P(\neg\#E3)$ equal to 2.82E-04, being the highest probabilities among the changes considered.

A BN was elaborated for estimating the probability of failure for event #E2. That BN was adapted to take into account the different normal operational modes of FSPCS. The highest probabilities among the operational modes considered in the BN were adopted for the solution of Eq. (7), i.e., with $P(\neg\#E2\_REC)$ equal 4.00E-04 and $P(\neg\#E2\_IRR)$ equal 2.62E-04. The estimation of the probability P (¬#E4) of failure in event #E4 was carried out by the BN referred to for event #E2, changed to consider the worst degraded condition – in relation to the probability of failure – in which the FSPCS still operates. To do so, the need to cool two heat exchangers was maintained, even with the removal of backup pumps; for maintained pumps, the hypothesis of failure on demand was not considered (previously considered in event #E2). For this, the probability of the state of the nodes related to the demand failure was nullified. In addition, the possibility of shutting down the pumps due to the spurious signals of the monitoring and control components was maintained. The network obtained this way allowed for equating the probability P(¬#E4) to 1.13E-03. Table 12 presents the probabilities of events related to the FSPCS equipment failures used throughout this work.

The failure frequency for the FSPCS is 2.63E-04/year, considering the event tree in Fig. 10, the data in Table 12, and the hypothesis that there is no human error during the operation – null probability of human error. This is considered the least possible failure frequency for the FSPCS, if the assumptions outlined in this topic, as well as in previous topics, are maintained, and in case of a solution for the FSPCS operational procedure design which adds little to the system failure frequency.

4.2. Cyclic phases – first iteration

The cyclic phases of the methodology [40] are performed iteratively (see Fig. 1). Two iterations were performed in this application. This section presents the results of the first iteration, and item 4.3 presents the results of the second iteration in this group of phases.

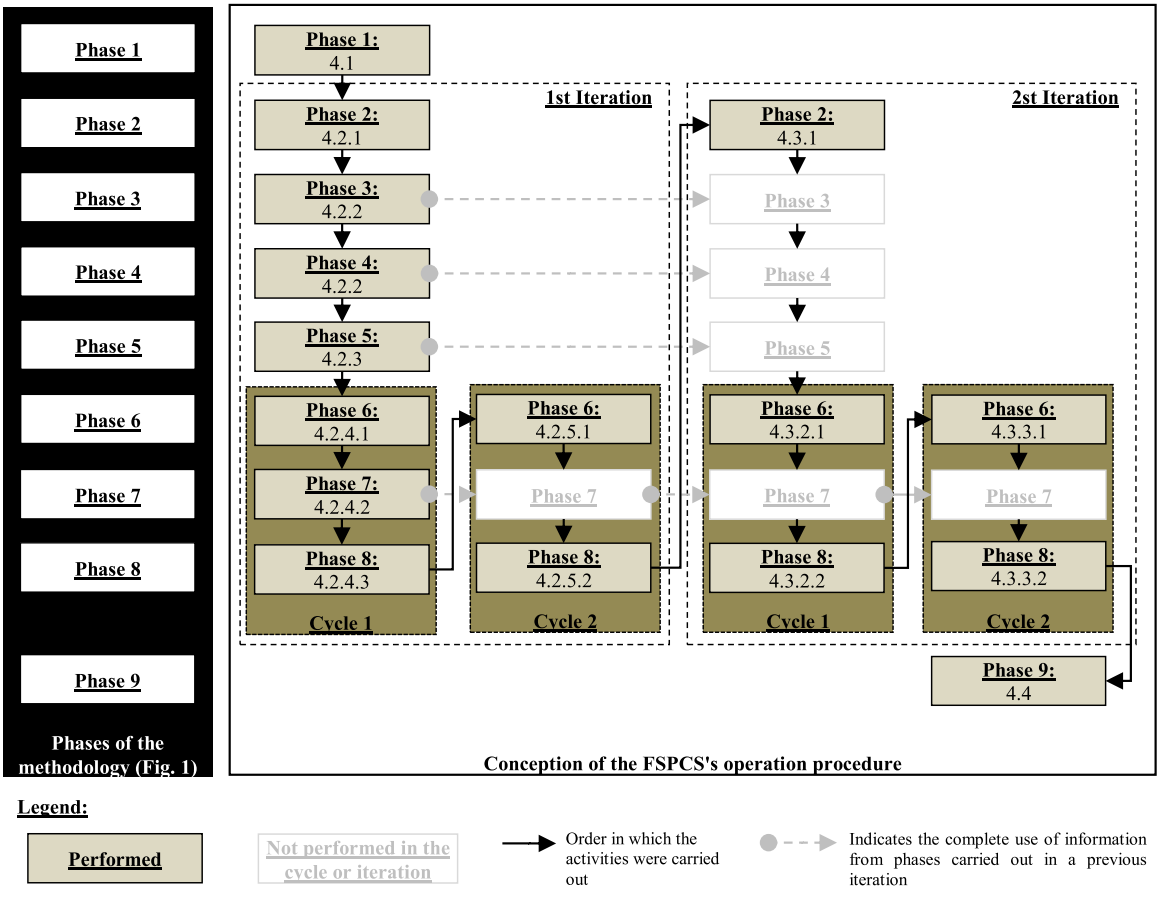


Fig. 9. FSPCS schematic arrangement.

Table 10
Characteristics of the FSPCS.

Characteristics	Description
System functions	It cools the compartments in which the FEs with residual heat are located in normal and degraded operation, thus maintaining the water temperature below 41°C; during a transition – which may occur between normal and degraded operation –, it keeps the water temperature in the FSP below 60°C. The FSP is expected to receive an annual load of FE.
Compartments to be cooled	The FE can be in four compartments of the FSP, called FSP-I (Compartment I), FSP-II (Compartment II), FSP-III (Compartment III) and TC (Transfer Channel) – these compartments are identified in Fig. 9. Only the TC will not be directly cooled – the FE will remain shortly in this compartment. It is important to note that the TC is the physical connection between the FSP compartments, and that, during the cooling operation, these compartments are isolated. Thus, in Fig. 9, the compartments were presented isolated.
Monitoring	In order to assist the operation, the system provides for monitoring the following variables – directly on the displays of the sensors installed in the vicinity of the monitored equipment (although some of these sensors are present, Fig. 9 does not show any of the displays): a) Temperature: in the FSP compartments (FSP-I, FSP-II and FSP-III), in the pumps (B1, B2, B3 and B4), and in the inlets and outlets of heat exchangers (T1, T2, and T3); b) Radiation: in the outlet piping of the hull side of heat exchangers (T1, T2, and T3); c) Flow: downstream of the pumps (B1 or B2, and B3 or B4) and heat exchangers (T1, T2, and T3), and d) Pressure: in pumps (B1, B2, B3, and B4) and in heat exchangers (T1, T2, and T3). Furthermore, the system provides for sending these signals to displays (also not shown in Fig. 9) installed in the panels P1 and P2.
Alarms	In addition to the local monitoring, the following variables are alarmed by sound and light in the CR (Control Room): a) Temperature: in the FSP compartments (FSP-I, FSP-II and FSP-III), via signal S1; b) Flow: downstream of the pumps (B1 or B2, and B3 or B4), via the signal S2, and; c) Radiation: in the outlet pipe on the hull side of heat exchangers (T1, T2, and T3), via signal S3. In spite of this simplified representation, these sensors are presented in pairs in the FSPCS documents, and can be considered independent.
System operation	All actions of pumps and valves depend on manual actuation, with the exception of automatic pump shutdown (B1 and / or B3) in case of low flow downstream, and actuation of the pump on standby – B2, in case of failure of B1 (B1 and B2 are 100% redundant), and / or B4, in case of failure of B3 (B3 and B4 are 100% redundant). The valves are locally actuated and the pumps can be actuated either locally in panel P1, or remotely in panel P2. After the first actuation, pump B1 (and / or B3) remains at low speed provided that there is no need to cool the FSP by the FSPCS, whereas the pump B2 (and / or B4) remains off, and will be actuated only in case of failure of pump B1 (and / or B3) – a controller deactivates pump B1 (or B3) and activates pump B2 (or B4) by a low flow signal received from the sensors.
Heating and cooling time	FSPCS is considered to have the ability to cool the largest FSP compartment from 41°C to 37°C in 4 hours. The FSP temperature, without FSPCS performance, rises from 37°C to 41°C in 8 hours, and from 41°C to 60°C in 38 hours (in the most adverse design condition, i.e., considering the higher ambient temperature of the historical series and the highest possible power for the FE). Additionally, the FE may exhibit negligible residual heat within 10 days, which does not exceed the natural capacity for heat dissipation in the FSP. Thus, considering that the system does not operate continuously, the expected actuation time for the FSPCS is 80 hours.
Operational modes	The operational modes for this system were defined according to the cooled compartments: O) Off; A) FSP-I; B) FSP-II; C) FSP-III; D) FSP-I & FSP-III, and; E) FSP-I & FSP-II. Thus, 39 operational modes were defined (achieved by the proper alignment of the valves shown in Fig. 9), between normal and degraded states – e.g., cooling the FSP-I, with circulation by pump B1 and cooling by the heat exchanger T1 (normal operation), or circulation by pump B1 and cooling by the heat exchanger T2 (degraded operation).
Maintenance procedure	It is expected that the conditions of the FSPCS equipment are checked immediately before its operation. However, in this work, the maintenance procedure is not developed, and it is considered that the equipment will be as good as new immediately after the maintenance procedure – though the possibility of a failure on demand is considered for the equipment with moving parts (valves, panels and pumps), whereas a failure on demand for heat exchangers, for example, is not being considered.

4.2.1. *Phase 2 – task analysis*

In order to determine the initial sequence of the tasks which compose the FSPCS operational procedure, the HTA (Hierarchical Task Analysis) [82,83] technique was applied, as described in Ref. [84]; Ref. [40] presents the correlations between the HTA steps and the design methodology phases. Considering the context described in Phase 1, the primary objectives of the operational procedure directly related to the events ordered in the Fig. 10 event tree were defined as follows: (a) Objectives of the detection task related to event #D1: detect possible stuck valves, panel problems and pump unavailability – considering that the pump failures will be detected in event #D2, given they were available at the beginning of the operation; (b) Objectives of the task for detecting recoverable failure related to event #D2: detect possible failures in FSPCS and evaluate the possibilities of recovery; (c) Objective of the alignment task related to event #A1: align FSPCS valves and other components consistently with the operational mode appropriate to the cooling needs (e.g., compartment to be cooled); (d) Objectives of the realignment task related to event #A2: select the degraded operational mode appropriate to the cooling needs, and align the FSPCS valves and components consistently with said operational mode; (e) Objectives of the monitoring and actuation task related to the event #M1: activate the FSPCS, monitor the temperature in the FSP, and, if necessary, operate in the FSPCS (e.g., changing the pumps from "on" to "off"); (f) Objectives of the monitoring and actuation task related to the event #M2: activate the FSPCS, monitor the temperature in the FSP, and operate in the FSPCS.

The HTA application [84] allowed for the discretization of the primary objectives of the tasks of FSPCS operators and the possibility of associating human activities in order to achieve such objectives. The goal discretization and the associated human activities are presented in Tables 13–18. The codes associated with the possible human activities are explained later, by the time Fig. 11 is commentated.

Observe that, for the detection task related to event #D2, presented in Table 14, the hypothesis of detecting recoverable failures is being considered. Thus, the objectives were divided between the detecting any failure (see item 1 in Table 14) and evaluating the possibilities of recovery (see item 2 in Table 14).

In Table 15, for the FSPCS alignment task (related to event #A1), the goal 1.4.Align the control systems refers to the power and operation of the controller and sensors, so that they only monitor and act on the pumps and lines of interest for the FSPCS operational mode. Also in Table 15, the objective 1.3.Aligning the heat exchangers refers to the activation of the SWCS (Safety Water Cooling System), allowing for the operation of a certain heat exchanger – it does not refer to the alignment of the valves adjacent to the heat exchangers (shown in Fig. 9). In the making of Table 14, it was considered that the error in the alignment of the control components does not lead to a system unrecoverable failure, i.e., in event #D2, a correction can occur (see item 2.1.3.3 of Table 14). However, such errors are considered in the quantification of the probabilities of error and success in event #A1, and in this phase, no recovery actions were assigned to the system alignment activities. As presented in Table 16, the task related to event #A2 presents the same objective of the task related to event #A1, as well as the need to consider the degraded condition of the FSPCS. Moreover, the aligning of the control and monitoring system is not necessary in the realignment.

In Table 17, related to the event #M1, objective 2.4. Put the system in standby refers to the interruption of cooling after ten days, when the FE presents insignificant residual heat – the system is kept ready to act in case of need (such period is not modeled in this work; however, the activity was maintained in the model for its consideration in a future work). At this point, note that, in principle, a specific recovery activity in case of human failure in monitoring was not considered. For the task of activating and monitoring the FSPCS related to event #M2, goal

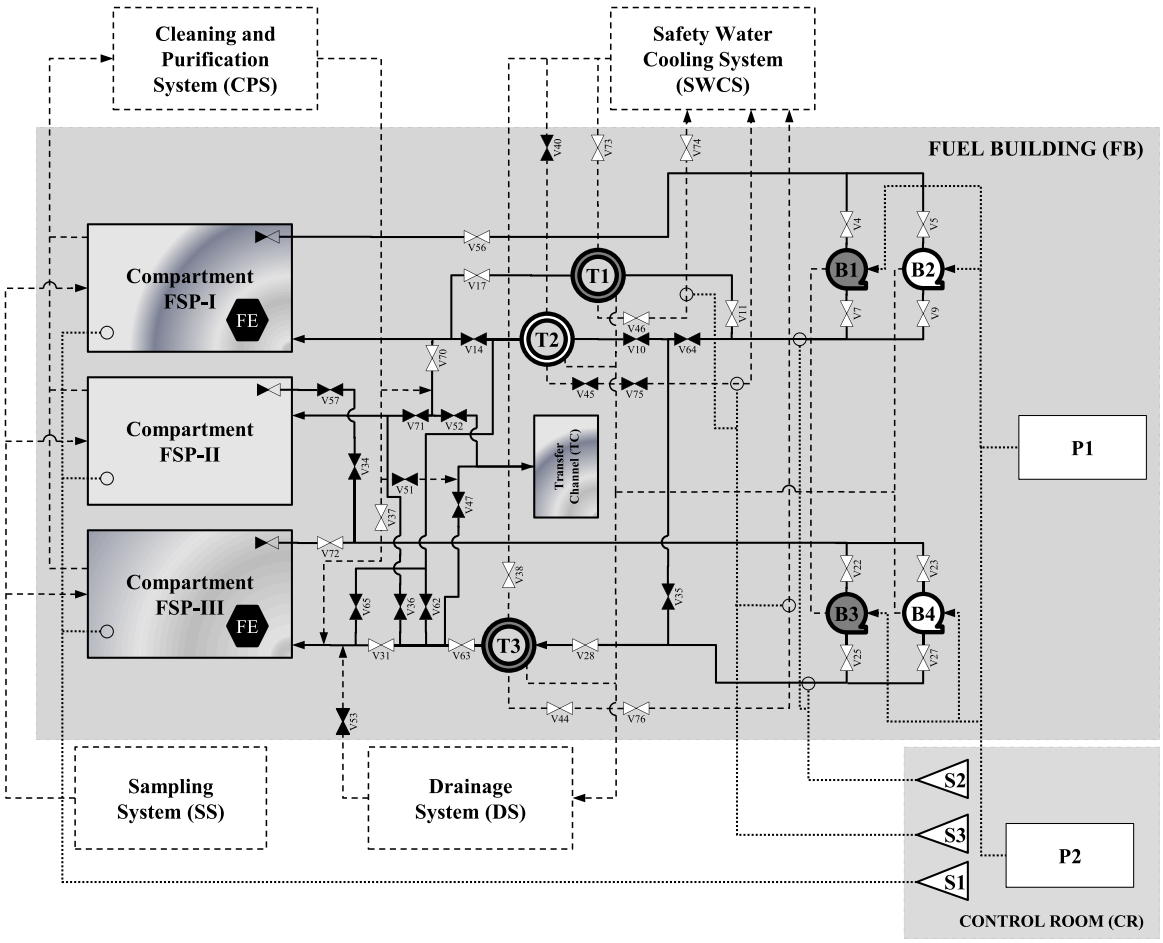


Fig. 10. Event tree for FSPCS.

discretization and related human activities are presented in Table 18. Despite the similarities between these objectives and those presented in Table 17 referring to event #M1, in event #M2 the operator administers the activation and monitoring of the degraded system.

The organization of a logical sequence of activities executed by the operators was possible based on the objectives presented in this topic's tables, thus meeting the scenario proposed in Phase 1 (see item 4.1), i.e., results in the system behavior, which meet the requirements. Fig. 11 presents a sequence with the characteristics for human activities in the FSPCS operation. This is the sequence which will be used in the next phases in the operating procedure design of this system.

The beginning and end of the operation were represented by the shaded circles in Fig. 11. The continuous arrows indicate the next action to be performed, while the dashed arrows indicate the next activity in case of anomaly detection. Additionally, the activities are numbered according to the order of execution. The activities to be performed when the system is in a degraded state have the number accompanied by the letter "d". The activities in this sequence were associated with task objectives by means of this numbering in the last columns of the tables in this topic (from Table 13 to Table 18).

Table 11
Events in the event tree for FSPCS.

Events	Description
#E1 and #E3	Consider the occurrence of an undiscovered failure in FSPCS components (valves and control panels) which will be actuated (in alignment or realignment, respectively; see events #A1 and #A2), thus preventing proper system alignment. For event #E1, the unrecoverable failure hypothesis was not considered, i.e., the hypothesis of realigning the system in a degraded operational mode was not considered, since at the moment of said event, the FE did not depend on the FSPCS to be cooled; the FE will not be deposited in the FSP if the system is in a degraded condition.
#D1	Refers to the human action of detecting the failures considered in event #E1. On the other hand, a failure detection event considered in event #E3 was not included in the tree. In this case, the FE with significant residual heat would depend on the FSPCS for cooling, thus increasing the importance of maintenance time of the failed equipment; the time for maintenance is not being considered in this work.
#A1 and #A2	Consider the human actions performed in the alignment and realignment (for a degraded operational mode) of the system; the failures of the actuated equipment are considered in events #E1 and #E3.
#E2 and #E4:	Consider the possibility of equipment failure during operation. For event #E2, two types of failure are being modeled: a) Recoverable (REC in Fig. 3), which can be overcome by system realignment, and b) Unrecoverable (IRR in Fig. 10), which cannot be overcome without maintenance actions, for example – these alternative actions are not modeled in this work. Moreover, since event #E4 occurs after the system realignment event (event #A2), i.e., the failure occurs when the system operates in a degraded operational mode, the recovery hypothesis was not considered in this event.
#M1 and #M2	Refer to the human actions of temperature monitoring and system activation (the FE is deposited in the FSP after the activation, which is part of #M1), in which #M2 refers to monitoring and operating the system in a degraded mode.
#D2	Refers to the human action of detecting failures considered in event #E2.

Table 12
Events related to equipment failure.

Event	Description	P(Recoverable failure)	P(Not recoverable failure)
#E1	Equipment success in FSPCS alignment	6.74E-04	-
#E2	Equipment success during cooling (in normal condition)	4.00E-04	2.62E-04
#E3	Equipment success in FSPCS realignment	-	2.82E-04
#E4	Equipment success during cooling (in FSPCS degraded condition)	-	1.13E-03

Table 13
Objectives of the detection task related to event #D1 and human activities.

Primary		Secondary		Tertiary		Possible Human Activities
1	Detecting stuck valve	1.1	During the identification of the valve, detect the failures revealed by its general aspects	N / D		2. Check the presence of stuck valve (on identification)
		1.2	During actuation of the valve, detect failures revealed by its abnormal behavior	1.2.1	Raise awareness of the early / excessive end of the valve stroke	4. Check the presence of stuck valve (in the actuation)
				1.2.2	Raise awareness of the clearances, signs of leakage, corrosion, abnormal sounds, and the need for excessive / reduced effort	
		1.3	After actuation of the valve, detect the response different from expected	N / D		11. Monitor the behavior of the system after the activation
2	Detect problem on panel	2.1	During identification of the button and its activation, detect the failures revealed by its general aspects	N / D		9. Check the general conditions of the activation buttons
		2.2	After the button is pressed, detect a response different from expected	N / D		11. Monitor the behavior of the system after the activation
3	Detect the unavailability of pumps	N / D		N / D		6. Perform pump test

N / D: Detail of objective not developed up to the indicated level

Three phases in the operational procedure can be identified in the sequence of activities depicted in Fig. 11. The first, prior to the insertion of the FE in the FSP, is characterized by the possibility of repairing the system, thus solving possible anomalies – being considered that the maintenance procedure, carried out prior to the start-up, is successful (see Section 4.1.3). The second, subsequent to the insertion of the FE in the FSP, is characterized by a cycle of monitoring actions (both the temperature in the FSP and the FSPCS state) and actuation. The third phase refers to the possible operation of the system in a degraded mode, due to the identification of anomaly in the second operational phase. Thus, activities from 19d to 28d refer to a transient period in which the water cooling by the FSPCS may not be occurring. Note that the FE damage can occur in the last two phases – due to recoverable failures and due to unrecoverable failures.

Specifically for activity 1, it is important to emphasize that the execution depends on factors which are not being considered in this application, i.e., the need for cooling depends on the states of the FE to be cooled, and the evaluation of the state of the FE is outside the scope of this application. Although maintained in the analysis, this activity was not considered in the quantification of FSPCS reliability.

Three cyclic groups of activities can be identified in Fig. 11. The first involves activities from 1 to 11 and includes the non-modeled activity "Solve the anomaly". In this activity cycle, when an anomaly is found (e.g., valve stuck in activity 2), it is solved and the cycle is restarted. The second cycle involves activities from 12 to 17, and refers to the activities of temperature monitoring (activity 12, when the temperature is between 37 °C and 41 °C), deciding about acting on the system (activity 16, when the temperature is close to 37 °C or 41 °C) and acting on the system (activity 17), interspersed with activities aiming at meeting anomalies (activities 13, 14 and 15), which can start the operation in a degraded mode. The third cycle involves activities 29d, 30d, and 31d, and is similar to the second, except for assuming the absence of activities

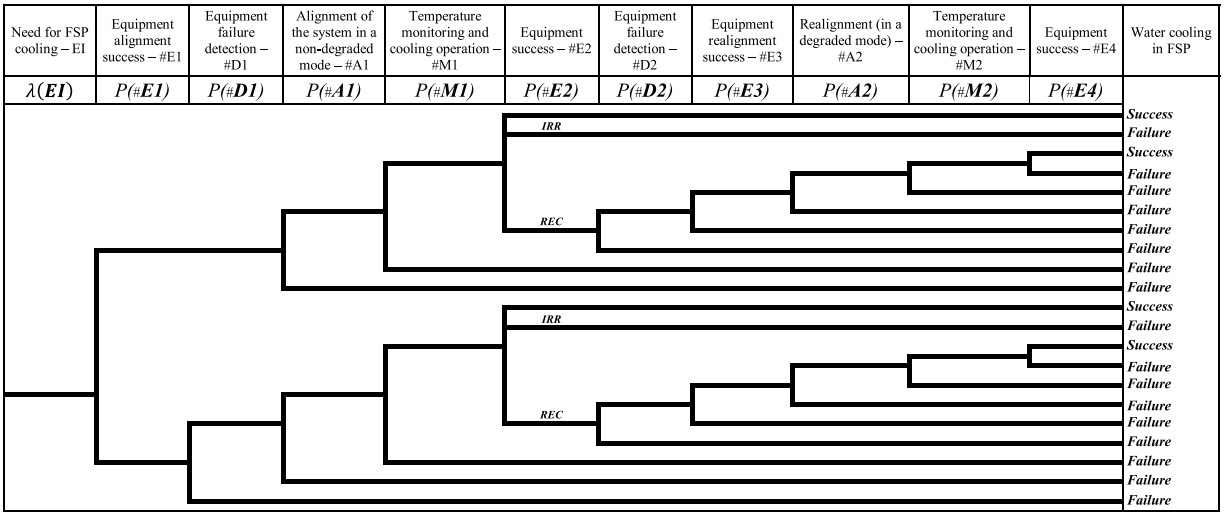


Fig. 11. Initial sequence of activities in the FSPCS operational procedure.

Table 14
Objectives of the recoverable failure detection task related to event #D2 and human activities.

Primary		Secondary		Tertiary		Quaternaries		Possible Human Activities
1	Detect FSPCS failure	1.1	Detect the lack of pumping	1.1.1	Detect low flow light signal	N / D		13. Monitor flow in FSPCS
				1.1.2	Detect low flow sound signal	N / D		
				1.1.3	Detecting low flow in local displays	N / D		
				1.1.4	Detect through the temperature rise in the FSP	1.1.4.1	Detect the high temperature light signal	12. Monitor the temperature of the FSP
						1.1.4.2	Detect the high temperature beeper	
						1.1.4.3	Detect high temperature in local displays	
		1.2	Detect the fluid routing problem	1.2.1	Detect leak at local inspection	N / D		14. Check the status of FSPCS components
				1.2.2	Detect leak through the radiation signal	N / D		15. Monitor radiation in FSPCS
				1.2.3	Detect leak through the radiation beeper	N / D		
				1.2.4	Detect leakage through local displays (radiation)	N / D		
				1.2.5	Detect the obstruction through the low flow light signal	N / D		13. Monitor flow in FSPCS
				1.2.6	Detect the obstruction through the low flow sound signal	N / D		
				1.2.7	Detect the obstruction through local flow displays	N / D		
				1.2.8	Detect through the temperature rise in the FSP	1.2.8.1	Detect the high temperature light signal	12. Monitor the temperature of the FSP
						1.2.8.2	Detect the high temperature beeper	
						1.2.8.3	Detect high temperature in local displays	
		1.3	Detect the lack of electricity	Not modeled				
		1.4	Detect the lack of cooling in SWCS water	Not modeled				
2	Evaluate the possibility of recovery	2.1	Evaluate recovery possibilities after lack of pumping	2.1.1	Detect the spurious low flow signal	2.1.1.1	Detect sensor spurious signal	19d. Check the pumps operation
						2.1.1.2	Detect spurious controller signal	20d. Evaluate the possibility of spurious / low-flow signal
				2.1.2	Detect the spurious signal from the control panels	N / D		19d.Check the pumps operation 21d. Evaluate the possibility of panel spurious signal
				2.1.3	Detect failure in the low flow signal	2.1.3.1	Detect sensor failure	19d. Check the pumps operation
						2.1.3.2	Detect controller failure	20d. Evaluate the possibility of spurious / low-flow signal
						2.1.3.3	Detect human error in system alignment*	
		2.2	Evaluate the recovery possibility after a problem in routing the fluid	2.2.1	Detect obstructions (valves, pipes, connections and heat exchangers)	N / D		19d. Check the pumps operation 23d. Perform the flow test on the pipe sections
				2.2.2	Detect leaks (valves, pipes, connections and heat exchangers)	N / D		22d. Inspect pipelines

N / D: Detail of objective not developed up to the indicated level;
()*: The failure to achieve this goal is considered in the quantification of failure and success probabilities in event #A1 (see Table 9).

which aim to meet anomalies.

4.2.2. Phases 3 and 4 – applicable technology and equipment functions

This work does not aim at designing the complete FSPCS – i.e., encompassing the equipment and the operation – but at designing the operational procedure without altering the equipment considered in Phase 1 (see item 4.1). The functional and reliability data for the equipment considered in Phases 3 and 4 are those presented in Phase 1.

4.2.3. Phase 5 – human functions

The human performance data considered in the design of the FSPCS operational procedure were obtained from the model presented in Section 3. For any action, this can be done according to the following procedure: (1) classify the action according to Bloom's taxonomy; (2) correlate the action with a generic action of the prospective model of human performance presented in Table 1 or Table 2 by the similarity of their classifications – according to Bloom's taxonomy; (3) define the level of performance for the action according to the SRK model, and; (4) take the distribution of the HEP presented in Table 9 for the generic

Table 15
Objectives of the alignment task related to event #A1 and human activities.

Primary		Secondary		Possible Human Activities
1	Align the FSPCS valves and components consistently with appropriate operational mode	1.1	Align the valves	3. Align the valves according to the operational mode
		1.2	Align the pumps	5. Align the pumps according to the operational mode
		1.3	Align heat exchangers	7. Align the heat exchangers according to the operational mode
		1.4	Align the control systems	8. Align the control systems according to the operational mode

Table 16
Objectives of the alignment task related to the event # A2 and human activities.

Primary		Secondary		Possible Human Activities
1	Select the appropriate operational mode	1.1	List unavailability in the system	24d. List system outages
		1.2	Set the operational mode	25d. Define a new operational mode
2	Align FSPCS valves and components consistently with the selected operational mode	2.1	Align the valves	26d. Align the valves according to the operational mode
		2.2	Align the pumps	27d. Align the pumps according to the operational mode
		2.3	Align the heat exchangers	28d. Align the heat exchangers according to the operational mode

action and for the performance level, which were correlated to the action.

4.2.4. Solution development– Cycle 1

Phases 6–8 are considered in solution development cycles – red phases in Fig. 1. Two development cycles were performed in this iteration (items 4.2.4 and 4.2.5).

Phase 6 – grouping agents: In this first grouping of agents, it was assumed that the performance time of the tasks in the FSPCS is not a critical variable – in the most adverse condition, in the transient between a normal mode operation and the operation in a degraded mode, the FSP water can reach the limit temperature only if the transient lasts longer than 38 hours (time required to raise the temperature from 41°C to 60°C, see Section 4.1). Thus, in principle, only one operator for the FSPCS operation, which will carry out the activities one by one, was considered, i.e., operations in parallel were not considered. Thus, Table 19 presents the correlation between the activities in Fig. 11 sequence to be performed by this agent, and the actions of the prospective model of human performance.

The activities listed in the first column of Table 19 were correlated to performance domains, categories and cognitive processes (specifically for the cognitive domain) according to the taxonomy presented in Section 2. This was done by considering the characteristics of the activities listed in Phase 2 (see tables in 4.2.1). Thus, it was possible to associate the performance levels and actions of the prospective model of human performance with the actions to be performed by the FSPCS operator, as presented in the last columns of Table 19. The reliability data for the human actions considered in Table 19 are presented in Table 9.

Phase 7 – cost-benefit analysis: The altering of the equipment which compose the FSPCS is not considered in this work. Therefore, the choice to be made may be related to the number of operators and the type of task to be performed by them. Such choices were made in the previous phases (see 4.2.4.1), and an action was associated with each activity – therefore, there was no choice between preconceived alternatives. The next phase, however, presents some considerations on the effects of the HEP context on the actions of the operational procedure.

Phase 8 – system reliability: This phase analyzes the adequacy of the associations presented in the previous phases regarding the reliability goal established in item 4.1.1. By defining the activities of the sequence in Fig. 11 associated with the prospective model of human performance (see Table 19), it was possible to develop the BN illustrated in Fig. 12 and check whether this design criterion was reached and, through Bayesian inference, point out alternatives for the improvement of the design proposal. The BN seen in Fig. 12 was obtained throughout this case study, being reviewed every time Phase 8 was performed. Therefore, the BN presented in Fig. 12 does not refer only to this first solution development cycle (of the first iteration in the cyclic phases). For space saving, this paper does not present all versions of this BN. The added or changed nodes, however, were detailed in the description of each cycle, as well as their CPTs. The CPTs were presented in Appendix I (including their versions for each cycle).

The BN illustrated in Fig. 12 was obtained by: (a) converting the event tree in Fig. 10 into a BN – green nodes in Fig. 12; (b) feeding the nodes referring to the performance of the equipment with the data

Table 17
Objectives of the monitoring and activation task related to event #M1 and human activities.

Primary		Secondary		Tertiary		Possible Human Activities
1	Activate FSPCS	1.1	Activate FSPCS via P1 / P2	N / D		10. Activate FSPCS via P1 / P2
		1.2	Activate FSPCS locally (in case of panel failure)	N / D		
2	Monitor the temperature in the FSP and operate in the FSPCS (after the initial activation)	2.1	Monitor the temperature	2.1.1	Monitor the temperature on the panel	12. Monitor the temperature of the FSP
				2.1.2	Monitor the temperature in the local display	
		2.2	Decide to act in the system	N / D		16. Decide to act in the system
		2.3	Activate the system	N / D		17. Act in the FSPCS via P1 / P2
		2.4	Put the system in standby	2.4.1	Activate the FSPCS via P1 / P2	18. Switch the system to standby
				2.4.2	Activate FSPCS locally (in case of panel failure)	

Table 18
Objectives of the monitoring and activation task related to event #M2 and human activities.

Primary		Secondary		Tertiary		Possible Human Activities
1	Activate the FSPCS	1.1	Activate the FSPCS via P1 / P2	N / D		29d. Act in the FSPCS
		1.2	Activate the FSPCS locally (in case of panel failure)	N / D		
2	Monitor the temperature in the FSP and operate in the FSPCS (after the initial activation)	2.1	Monitor the temperature	2.1.1	Monitor the temperature in the panel	30d. Monitor the FSP temperature
				2.1.2	Monitor the temperature in the local display	
		2.2	Decide to act in the system	N / D		31d. Decide to act in the system
		2.3	Activate the system	2.3.1	Activate the FSPCS via P1 / P2	29d. Act in the FSPCS
				2.3.2	Activate FSPCS locally (in case of panel failure)	
		2.4	Switch the system to standby	2.4.1	Switch on the FSPCS via P1 / P2	32d. Switch the system to standby
				2.4.2	Activate the FSPCS locally (in case of panel failure)	

discussed in item 4.1.2; (c) adding parent nodes for the human performance events related to the activities presented in the Fig. 11 sequence – blue nodes in Fig. 12, identified by the number of the activity preceded by the letter S, in reference to the sequence of activities (Activity 11 is in a different color because it was included in this cycle, but reworked in the last cycle, see item 4.3.4), and (d) aggregating the performance model's actions presented in Table 19 – represented by the yellow nodes in Fig. 12. The nodes with other colors were included in later cycles. The topology of this network and the completion of the CPT were carried out observing the dependencies presented in Table 20.

In the BN of Fig. 12, the nodes for the activities (blue nodes) are deterministic, i.e., the failure to perform the associated action leads to inadequate results in the activity. The HEPs associated with the nodes for such actions were obtained from Table 9, "Median" column.

The probability of failure of FSPCS (given the need to use this system) was estimated to be 51.42%, being greater than the probability established in item 4.1.1 – i.e., 0.1% – thus concluding that, as conceived, the operational procedure for the FSPCS represented in this BN is inadequate. Through Bayesian inference, considering the evidence of FSPCS failure, the most impacted BN nodes – which showed higher probability of failure – were found, given the evidence. Table 21 shows the results obtained consequently.

Table 21 shows that, given the evidence of FSPCS failure, the most impacted events, i.e., with the highest probability of failure, are #M1 and #A1. Such result was expected, since the influence of the other events on FSPCS failure is more sensitive to the occurrence of equipment failure (see Table 36 in Appendix I). Thus, the most impacted activities are related to events #A1 and #M1 (nodes "S3", "S5", "S7", "S8", "S10",

Table 19
Correlation with the actions of the prospective model of human performance (cycle 1, first iteration).

Activities	Domain	Category	Cognitive Process	Code	Performance Level
1. Associate the need for cooling to an operational mode	Cognitive	Understanding	Interpreting	A_C_2a	Rule
2. Check the presence of stuck valve (on identification)	Cognitive	Evaluating	Checking	A_C_5a	Rule
3. Align the valves according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
4. Check the presence of a stuck valve (in the activation)	Cognitive	Evaluating	Checking	A_C_5a	Rule
5. Align the pumps according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
6. Perform the pump test	Cognitive	Applying	Executing	A_C_3a	Skill
7. Align the heat exchangers according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
8. Align the control systems according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
9. Check the general conditions of the activation buttons	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
10. Activate FSPCS via P1 / P2	Psychomotor	Basic Movement	-	A_P_2	Skill
11. Monitor the behavior of the system after the activation	Cognitive	Evaluating	Checking	A_C_5a	Rule
12. Monitor the temperature of the FSP	Cognitive	Evaluating	Checking	A_C_5a	Rule
13. Monitor flow in FSPCS	Cognitive	Evaluating	Checking	A_C_5a	Rule
14. Check the status of FSPCS components	Cognitive	Evaluating	Checking	A_C_5a	Rule
15. Monitor radiation in FSPCS	Cognitive	Evaluating	Checking	A_C_5a	Rule
16. Decide to act in the system	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
17. Act in the FSPCS via P1 / P2	Psychomotor	Basic Movement	-	A_P_2	Skill
18. Switch the system to standby*	Psychomotor	Basic Movement	-	A_P_2	Skill
19d. Check the operation of the pumps	Cognitive	Evaluating	Checking	A_C_5a	Rule
20d. Evaluate the possibility of spurious / low flow signal	Cognitive	Analyzing	Differentiate	A_C_4a	Knowledge
21d. Evaluate the possibility of panel spurious signal	Cognitive	Analyzing	Differentiate	A_C_4a	Knowledge
22d. Inspect pipelines	Cognitive	Analyzing	Differentiate	A_C_4a	Knowledge
23d. Perform the flow test on the pipe sections	Cognitive	Applying	Executing	A_C_3a	Skill
24d. List system outages	Cognitive	Applying	Executing	A_C_3a	Skill
25d. Define a new operational mode	Cognitive	Applying	Implementing	A_C_3b	Rule
26d. Align the valves according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
27d. Align the pumps according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
28d. Align the heat exchangers according to the operational mode	Cognitive	Applying	Executing	A_C_3a	Skill
29d. Act in the FSPCS	Psychomotor	Basic Movement	-	A_P_2	Skill
30d. Monitor the FSP temperature	Cognitive	Evaluating	Checking	A_C_5a	Rule
31d. Decide to act in the system	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
32d. Switch the system to standby*	Psychomotor	Basic Movement	-	A_P_2	Skill

()* Actions in this activity were not considered in the next phases – it is considered that the error in this activity will not impact the cooling of the FE (it will be performed after the 10-day operation period when the FE will no longer produce significant residual heat).

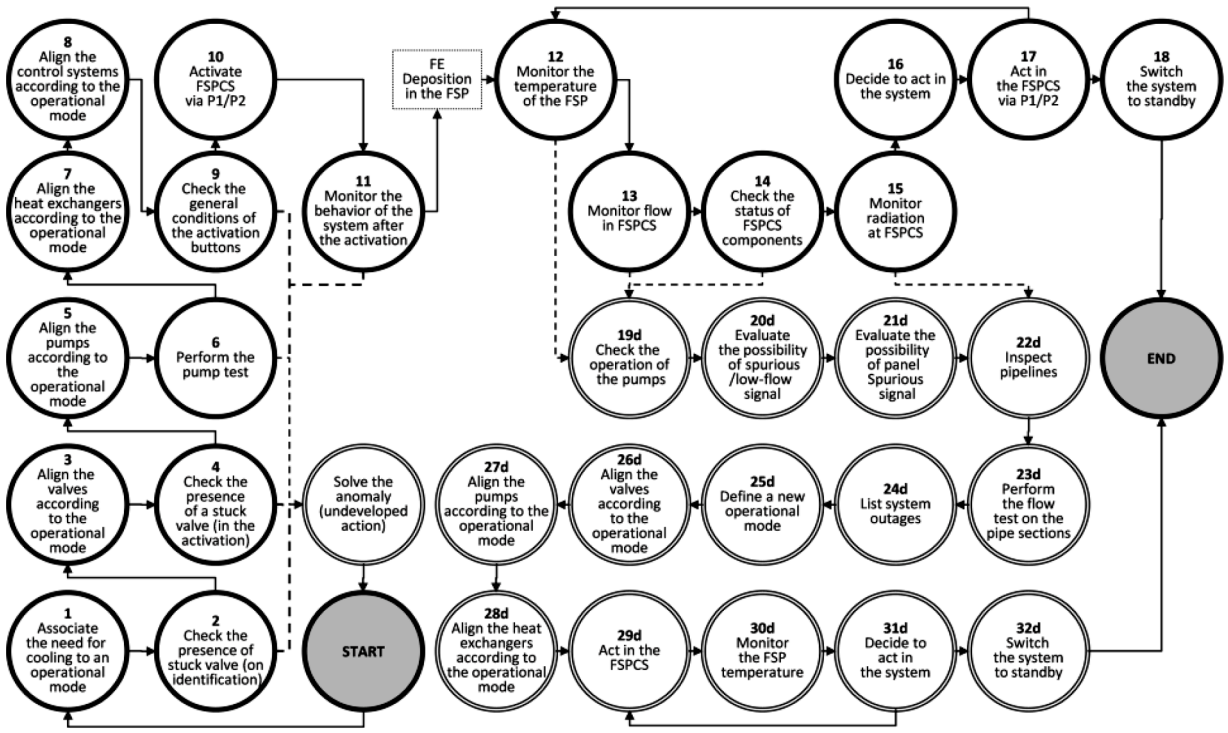


Fig. 12. BN for the reliability goal evaluation.

Table 20
Dependencies considered in the BN of Fig. 12.

Events	Description
¬#A1	The initial alignment failure will occur if there is an inadequate performance of one of the possible activities listed in Table 15
¬#A2	Failure to realign the system will occur if there is an inadequate performance of one of the possible activities listed in Table 16
¬#M1	Monitoring failure will occur if there is an inadequate performance of any of the activation and monitoring activities listed in Table 17, except activity 18 – it is considered that the error in this activity will not impact the FE cooling since it will be performed after the period of 10 days of operation (by then the FE will no longer produce significant residual heat). Note that in this first cycle, actions for the recovery of the human error in the monitoring were not considered, and the detection activities (related to event #D2) refer to the equipment failure – the need to consider redundant actions is evaluated in the end of this phase
¬#M2	Failure to monitor in a degraded condition will occur if there is an inadequate performance of any of the activation and monitoring activities listed in Table 18, except activity 32d – such as activity 18, it is considered that the error in this activity will not impact the FE cooling. Note that in this first cycle, no actions were taken for the recovery of human error in monitoring
¬#D1	Detection failure is considered to be conservative if there is an inadequate performance of the activities listed in Table 13 (subject to the combinations shown in Table 36 of Appendix I), regardless of the type of equipment which may have failed
¬#D2	As seen in Table 14, some types of equipment failures can be detected by different activities – e.g., lack of pumping can be detected by activity 12 and activity 13. Therefore, it is considered that event ¬#D2 will occur if there is an inadequate performance of one or more of the following combinations of activities: (a) 12 and 13: obstruction not detected; (b) 12 and 14: leakage to the environment not detected; (c) 15: leakage in the heat exchanger not detected; (d) 19d: pumps malfunction not considered; (e) 20d: controller malfunction not considered; (f) 21d: panel malfunction not considered; (g) 22d: piping leakage not considered, or (h) 23d: pipeline obstruction not considered. The BN conservatively considers inadequate detection if any of these combinations exist, regardless of the type of equipment which may have failed. Additionally, the contribution of sensor failure to the failing of activities 12, 13 and 15 was disregarded in the BN – the HEPs for actions associated with these activities (see Table 9) are three orders of magnitude greater than the probabilities of failure of these equipment

"S12", "S16", and "S17"). For a greater relative increase in system reliability, these results suggest changes in the human actions associated with these activities – nodes "A_C_3a", "A_C_3a_1", "A_C_3a_2", "A_C_3a_3", "A_P_2", "A_P_2_1", "A_C_5a_4" and "A_C_5b" in the Fig. 12 BN. The probability of FSPCS failure was estimated to be 15.62% for these actions using the HEP data from the "5-th Percentile" column of Table 9.

Assuming that the employment of the 5-th percentile for the probability of error in an action is associated with evident proper conditions for its performing – e.g., experienced operators, good organizational conditions [22] –, the conclusion is that solely the improvement in the performing conditions is not sufficient for the reliability of the FSPCS to assume an acceptable value. Thus, it is necessary to change the sequence of activities defined in Phase 2 (i.e., perform another iteration in the cyclic phases) or associate actions not yet considered in Phase 6 (i.e., carry out another solution development cycle). Since redundant activities (e.g., human error recovery) were ignored in this first cycle, returning to Phase 6 was deemed necessary, as can be seen in section 4.2.5.

4.2.5. *Solutions development – Cycle 2*

Phase 6 – grouping agents: The most impacted activities described in item 4.2.4.3 – see Table 21 – were as follows: (a) Prior to the FE positioning in the FSP: 3, 5, 7, 8, 10 and 11; (b) Subsequent to the positioning of the FE in the FSP: 12, 16 and 17. Verification actions and redundant actions were added to these activities, regardless of those included in item 4.2.4.1, as described in Table 22 – the shaded actions were included. This table also shows the correlation between the included actions and the actions of the prospective model of human performance.

Another agent was required in the FSPCS operation for executing the actions included in this phase. Therefore, operators OP1 and OP2 were identified for actions in this cycle which may occur at the same time or must be performed by different operators. In the activities 11, 12, 16 and 17, it is considered that the two operators have autonomy to decide and act on the system, being that while one operator acts, the other one checks (activity 17).

Phases 7 and 8 – cost-benefit analysis and system reliability: As in cycle

Table 21
Probability of "Failure" or "Inadequate" states for the BN nodes without and with evidence of FSPCS failure.

Node	Without Evidence	With Evidence	Variation	Node	Without Evidence	With Evidence	Variation
S3	7.00E-02	1.36E-01	94.49%	S25d	9.00E-02	9.00E-02	0.01%
S5	7.00E-02	1.36E-01	94.49%	S29d	5.00E-02	5.00E-02	0.01%
S7	7.00E-02	1.36E-01	94.49%	S23d	7.00E-02	7.00E-02	0.01%
S8	7.00E-02	1.36E-01	94.49%	S24d	7.00E-02	7.00E-02	0.01%
M1	3.50E-01	6.81E-01	94.48%	S26d	7.00E-02	7.00E-02	0.01%
S10	5.00E-02	9.72E-02	94.48%	S27d	7.00E-02	7.00E-02	0.01%
S17	5.00E-02	9.72E-02	94.48%	S28d	7.00E-02	7.00E-02	0.01%
Water Cooling in FSP	5.14E-01	1.00E+00	94.48%	S15	1.00E-01	1.00E-01	0.01%
S12	1.00E-01	1.94E-01	94.48%	S19d	1.00E-01	1.00E-01	0.01%
S16	2.00E-01	3.89E-01	94.48%	S30d	1.00E-01	1.00E-01	0.01%
A1	2.52E-01	4.90E-01	94.48%	S31d	2.00E-01	2.00E-01	0.01%
D2	3.46E-01	3.58E-01	3.47%	S9	2.00E-01	2.00E-01	0.00%
D1	2.63E-02	2.64E-02	0.06%	S6	7.00E-02	7.00E-02	0.00%
S11	1.00E-01	1.00E-01	0.02%	S13	1.00E-01	1.00E-01	0.00%
M2	3.16E-01	3.16E-01	0.01%	S14	1.00E-01	1.00E-01	0.00%
A2	3.19E-01	3.19E-01	0.01%	S18	5.00E-01	5.00E-01	0.00%
S20d	4.00E-02	4.00E-02	0.01%	S2	1.00E-01	1.00E-01	0.00%
S21d	4.00E-02	4.00E-02	0.01%	S32d	5.00E-01	5.00E-01	0.00%
S22d	4.00E-02	4.00E-02	0.01%	S4	1.00E-01	1.00E-01	0.00%

Table 22
Correlation with the actions of the prospective model of human performance (cycle 2, first iteration).

Activities	Actions	Domain	Category	Cognitive Process	Code	Performance Level
3. Align valves according to the operational mode	3.1.Align (OP1)	Cognitive	Applying	Executing	A_C_3a	Skill
	3.2.Check (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
5. Align pumps according to the operational mode	5.1.Align (OP1)	Cognitive	Applying	Executing	A_C_3a	Skill
	5.2.Check (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
7. Align heat exchangers according to the operational mode	7.1.Align (OP1)	Cognitive	Applying	Executing	A_C_3a	Skill
	7.2.Check (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
8. Align control systems according to the operational mode	8.1.Align (OP1)	Cognitive	Applying	Executing	A_C_3a	Skill
	8.2.Check (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
10. Activate FSPCS via P1 / P2	10.1 Activate (OP1)	Psychomotor	Basic Movement	-	A_P_2	Skill
	10.2.Check (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
11. Monitor the behavior of the system after activation	11.1Monitor (OP1)	Cognitive	Evaluating	Checking	A_C_5a	Rule
	11.2 Monitor (OP2)	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
12. Monitor the temperature in the FSP	12.1 Monitor (OP1)	Cognitive	Evaluating	Checking	A_C_5a	Rule
	12.2 Monitor (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule
16. Decide to act on the system	16.1 Decide (OP1)	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
	16.2 Decide (OP2)	Cognitive	Evaluating	Critiquing	A_C_5b	Knowledge
17. Act on FSPCS via P1 / P2	17.1 Activate (OP1 or OP2)	Psychomotor	Basic Movement	-	A_P_2	Skill
	17.2.Check (OP2 or OP1)	Cognitive	Evaluating	Checking	A_C_5a	Rule

Table 23
Probability of "Failure" or "Inadequate" states for BN nodes without and with evidence of FSPCS failure.

Node	Without Evidence	With Evidence	Variation	Node	Without Evidence	With Evidence	Variation
A1	2.77E-02	3.24E-01	1067.61%	S27d	7.00E-02	7.01E-02	0.13%
M1	5.91E-02	6.90E-01	1067.60%	S28d	7.00E-02	7.01E-02	0.13%
S10	5.00E-03	5.84E-02	1067.60%	S20d	4.00E-02	4.01E-02	0.13%
S12	1.00E-02	1.17E-01	1067.60%	S21d	4.00E-02	4.01E-02	0.13%
S16	4.00E-02	4.67E-01	1067.60%	S22d	4.00E-02	4.01E-02	0.13%
S17	5.00E-03	5.84E-02	1067.60%	S25d	9.00E-02	9.01E-02	0.13%
S3	7.00E-03	8.17E-02	1067.60%	S29d	5.00E-02	5.01E-02	0.13%
S5	7.00E-03	8.17E-02	1067.60%	S15	1.00E-01	1.00E-01	0.13%
S7	7.00E-03	8.17E-02	1067.60%	S19d	1.00E-01	1.00E-01	0.13%
S8	7.00E-03	8.17E-02	1067.60%	S30d	1.00E-01	1.00E-01	0.13%
Water Cooling in FSP	8.56E-02	1.00E+00	1067.60%	S31d	2.00E-01	2.00E-01	0.13%
D2	3.35E-01	3.49E-01	4.17%	S9	2.00E-01	2.00E-01	0.01%
D1	5.27E-03	5.31E-03	0.72%	S6	7.00E-02	7.00E-02	0.01%
S11	2.00E-02	2.00E-02	0.18%	S13	1.00E-01	1.00E-01	0.00%
A2	3.19E-01	3.20E-01	0.13%	S14	1.00E-01	1.00E-01	0.00%
M2	3.16E-01	3.16E-01	0.13%	S18	5.00E-01	5.00E-01	0.00%
S23d	7.00E-02	7.01E-02	0.13%	S2	1.00E-01	1.00E-01	0.00%
S24d	7.00E-02	7.01E-02	0.13%	S32d	5.00E-01	5.00E-01	0.00%
S26d	7.00E-02	7.01E-02	0.13%	S4	1.00E-01	1.00E-01	0.00%

Table 24
Objectives of the alignment task related to event #A1 and human activities (2nd Iteration).

Primary		Secondary		Possible Human Activities
1	Align the FSPCS valves and components consistently with appropriate operational mode	1.1	Align valves	3. Align valves according to the operational mode
		1.2	Align pumps	5. Align pumps according to the operational mode
		1.3	Align heat exchangers	7. Align heat exchangers according to the operational mode
		1.4	Align control systems	8. Align control systems according to the operational mode
2	Detect the alignment problem resulting from human action (after alignment)	N / D		11. Monitor the behavior of the system after the activation

1, Phase 7 was not considered in this cycle 2 – see justification presented in 4.2.4.2. The BN resulting from Phase 8 of cycle 1 was reviewed to consider the changes presented in 4.2.5.1 – illustrated in Fig. 12, as explained in 4.2.4.3. In the Fig. 12 network, the nodes in orange refer to the actions added to cycle 2 (4.2.5.1). The CPTs for the nodes of this network are presented in Appendix I, in which the changes are indicated in relation to cycle 1. The HEPs associated to the nodes for the actions added in this cycle were obtained from Table 9, "Median" column.

According to the obtained BN, the FSPCS failure rate was calculated to be 8.56%. Through Bayesian inference, considering the evidence of FSPCS failure, the most impacted BN nodes were found. Table 23 shows the results obtained consequently.

Table 23 shows that, given the evidence of FSPCS failure and considering the changes proposed in this cycle, events #A1 and #M1 remain the most impacted, followed by event #D2. Therefore, activities related to these events remain as the activities to be altered so that there is a greater relative increase in system reliability, in spite of the significant reduction in the probability of failure in these events (e.g., probability of failure in event #A1 went from 2.52E-01 to 2.77E-02 after the changes proposed in this cycle).

Specifically for the most impacted actions (related to activities 3, 5, 7, 8, 10, 12, 16 and 17), the FSPCS probability of failure was estimated to be 0.92%, considering the FSPCS failure and using data for HEP from "5-th Percentile" column of Table 12 instead of the "Median" column. Thus, the proposed changes in cycle 2 – redundancy or checking for the most impacting activities – and the improvement in the performing conditions (of the most impacting actions) were considered not enough to meet the goal established in item 4.1.4. Therefore, the search for the system operational procedure solution must continue.

4.3. Cyclic phases– second iteration

The choice made was to return to Phase 2 and change the sequence of initially proposed activities, by performing a new iteration in the cyclic phases of the methodology. Thus, this second iteration was developed based on the results of the first iteration.

4.3.1. Phase 2 – task analysis, and phases 3–5

In order to reduce the impact of the events #M1 and #A1 in the FSPCS reliability, the sequence of activities presented in Fig. 11 can be altered focusing on the activities related to these events. Thus, keeping the objectives of tasks related to other events unchanged, the following objectives can be added to the tasks related to events #A1 and #M1: (1) Event #A1: detect the alignment problems resulting from human action, and (2) Event #M1: detect the initial activation mismatch – i.e., the system response which is different from expected for the operational mode – and activate the FSPCS 8 h after the last cooling (regardless of temperature monitoring). The inclusion of these objectives is expected to reduce the impact of activities related to the other objectives. Tables 15 and 17 were changed to consider such changes, resulting in the Table 24 and Table 25, respectively, – the included lines are shaded. In Table 25, the objective of detecting the inadequacy of the initial activation (converted to objective 1.3.After the activation, detect a different response than expected) was included as a secondary objective related to objective 1.Activate FSPCS. Thus, the objective 1.Activate FSPCS refers both to the activation and to the guarantee of its suitability in this second iteration.

The possibility of recovering improper alignment was considered for the alignment task related to event #A1 (Table 24), and, thus, the activity 11 (previously considered only for equipment failures detection, see Table 24) was considered for detection of deviations caused by operator; this monitoring represents an opportunity to observe the manifestation of latent errors.

The possibility of inappropriate activation recovery was considered for the task of activating and monitoring the FSPCS related to event #M1 (Table 25), and, thus, activity 11 was considered for the detection of deviations caused by the operator during the activation. Additionally, activity 33.Measure time was included, thus constituting a redundant activity for the monitoring and decision-making related activities in relation to objective 2.Monitor temperature in FSP and act on FSPCS (after the initial activation).

Note that some of the added objectives did not give rise to new activities, since such objectives were added to activities already

Table 25
Objectives of the monitoring and activation task related to event #M1 and human activities (2nd Iteration).

Primary		Secondary		Tertiary		Possible Human Activities
1	Activate FSPCS	1.1	Activate FSPCS via P1 / P2	N / D		10. Activate FSPCS via P1 / P2
		1.2	Activate FSPCS locally (in case of panel failure)	N / D		
		1.3	After the activation, detect a different response than expected	N / D		11. Monitor the behavior of the system after the activation
2	Monitor the temperature in the FSP and act in the FSPCS (after the initial activation)	2.1	Monitor temperature	2.1.1	Monitor temperature on panel	12. Monitor temperature in the FSP
				2.1.2	Monitor temperature in the local display	
		2.2	Decide to act in the system	N / D		16. Decide to act on system
		2.3	Activate system	N / D		17. Act in the FSPCS via P1 / P2
		2.4	Set system to standby	2.4.1	Activate FSPCS via P1 / P2	18. Switch system to standby
				2.4.2	Activate FSPCS locally (in case of panel failure)	
3	Monitor the time and activate FSPCS 8 hours after cooling	3.1	Monitor time	N / D		33. Measure time
		3.2	Activate system	N / D		17. Act on FSPCS via P1 / P2

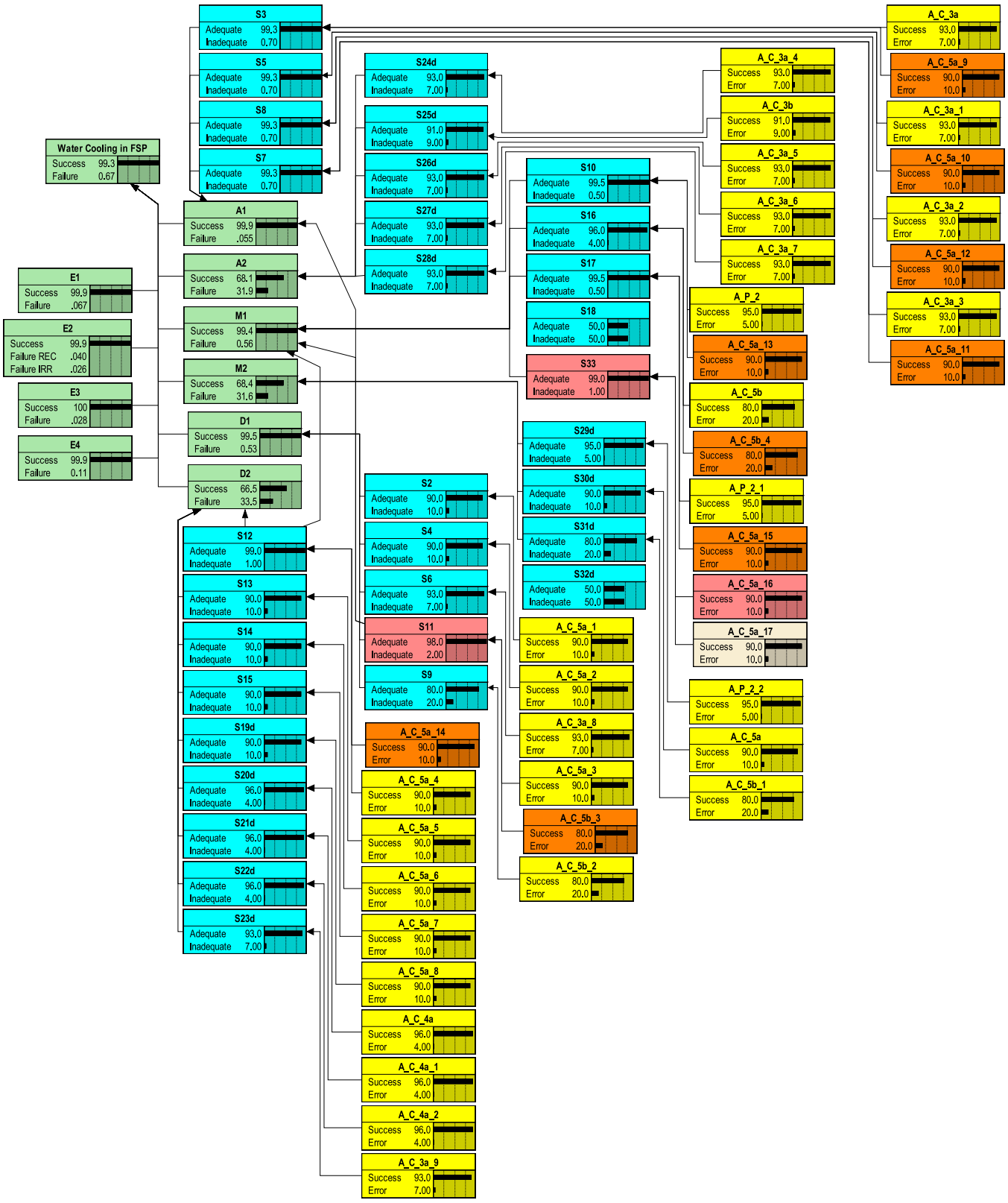


Fig. 13. Sequence of activities in the FSPCS operational procedure (2nd Iteration).

considered in the first iteration (Section 4.2). The characteristics of such activities (e.g., type of activity, operator involvement, execution time, chronological position in the sequence in Fig. 11) allow for the inclusion of human actions (performed in Phase 6 of the methodology), thus increasing the volume of work in the activity without significantly changing its characteristics.

A logical sequence for performing activities by the operators was organized, based on the sequence illustrated in Fig. 11, as well as on the activities and objectives presented in the tables in this topic. Such sequence is in accordance with the scenario proposed in Phase 1 (see

Table 26
Correlation with the action of the performance model.

Activity	Domain	Category	Cognitive Process	Code	Performance Level
33. Measure time	Cognitive	Evaluating	Checking	A_C_5a	Rule

Section 4.1), and is presented in Fig. 13.

The comments presented in items 4.2.2 and 4.2.3, respectively, for Phases 3–5 of the first iteration were maintained for this second iteration.

4.3.2. Solutions development – cycle 1 (2nd iteration)

Phases 6 and 7 – grouping agents and cost-benefit analysis: Given the similarity between the sequences presented in Figs. 11 and 13, in cycle 1 of the second iteration, the actions considered in cycle 2 of the first iteration (see item 4.2.5.1) were repeated, and the action related to activity 33 was added. Table 26 shows the correlation between the action of the agent involved in this activity and the action of the prospective model of human performance. Activities 11 and 17 were changed in Phase 2 of this second iteration – two objectives were added to activity 11 and one objective to activity 17. However, adding objectives did not significantly change the characteristics of the actions, which must be performed in order for all the objectives associated with these activities to be achieved. Thus, the actions considered in Table 22

Table 27
Probability of "Failure" or "Inadequate" states for BN nodes without and with evidence of FSPCS failure.

Node	Without Evidence	With Evidence	Variation	Node	Without Evidence	With Evidence	Variation
M1	1.00E-02	9.03E-01	8896.21%	S23d	7.00E-02	7.08E-02	1.10%
Water Cooling in FSP	1.11E-02	1.00E+00	8896.04%	S24d	7.00E-02	7.08E-02	1.10%
S17	5.00E-03	4.50E-01	8896.00%	S26d	7.00E-02	7.08E-02	1.10%
A1	5.54E-04	4.99E-02	8895.94%	S27d	7.00E-02	7.08E-02	1.10%
S12	1.00E-02	9.50E-02	849.88%	S28d	7.00E-02	7.08E-02	1.10%
S16	4.00E-02	3.80E-01	849.70%	M2	3.16E-01	3.19E-01	1.10%
S33	1.00E-01	4.99E-01	399.09%	S25d	9.00E-02	9.10E-02	1.10%
D1	5.27E-03	2.05E-02	289.90%	S15	1.00E-01	1.01E-01	1.10%
S11	2.00E-02	7.71E-02	285.62%	S19d	1.00E-01	1.01E-01	1.10%
S3	7.00E-03	1.91E-02	172.21%	S30d	1.00E-01	1.01E-01	1.10%
S5	7.00E-03	1.91E-02	172.21%	S31d	2.00E-01	2.02E-01	1.10%
S7	7.00E-03	1.91E-02	172.21%	S6	7.00E-02	7.01E-02	0.09%
S8	7.00E-03	1.91E-02	172.21%	S9	2.00E-01	2.00E-01	0.08%
S10	5.00E-03	1.36E-02	172.20%	S13	1.00E-01	1.00E-01	0.01%
D2	3.35E-01	3.49E-01	4.32%	S14	1.00E-01	1.00E-01	0.01%
A2	3.19E-01	3.23E-01	1.10%	S2	1.00E-01	1.00E-01	0.01%
S20d	4.00E-02	4.04E-02	1.10%	S4	1.00E-01	1.00E-01	0.01%
S21d	4.00E-02	4.04E-02	1.10%	S18	5.00E-01	5.00E-01	0.00%
S22d	4.00E-02	4.04E-02	1.10%	S32d	5.00E-01	5.00E-01	0.00%
S29d	5.00E-02	5.06E-02	1.10%				

Table 28
Correlation with the actions of the prospective model of human performance.

Activity	Actions	Domain	Category	Cognitive Process	Code	Performance Level
33. Measure time	33.1. Measure time (OP1)	Cognitive	Evaluating	Checking	A_C_5a	Rule
	33.2. Measure time (OP2)	Cognitive	Evaluating	Checking	A_C_5a	Rule

Table 29
Probability of "Failure" or "Inadequate" states for BN nodes without and with evidence of FSPCS failure.

Node	Without Evidence	With Evidence	Variation	Node	Without Evidence	With Evidence	Variation
S17	5.00E-03	7.49E-01	14870.80%	S27d	7.00E-02	7.13E-02	1.84%
Water Cooling in FSP	6.68E-03	1.00E+00	14870.73%	S28d	7.00E-02	7.13E-02	1.84%
M1	5.59E-03	8.37E-01	14870.68%	S25d	9.00E-02	9.17E-02	1.84%
A1	5.54E-04	8.30E-02	14870.68%	S20d	4.00E-02	4.07E-02	1.84%
S33	1.00E-02	8.31E-02	730.57%	S21d	4.00E-02	4.07E-02	1.84%
D1	5.27E-03	3.08E-02	484.59%	S22d	4.00E-02	4.07E-02	1.84%
S11	2.00E-02	1.15E-01	477.45%	S15	1.00E-01	1.02E-01	1.84%
S3	7.00E-03	2.72E-02	287.87%	S19d	1.00E-01	1.02E-01	1.84%
S5	7.00E-03	2.72E-02	287.87%	S29d	5.00E-02	5.09E-02	1.84%
S7	7.00E-03	2.72E-02	287.87%	S30d	1.00E-01	1.02E-01	1.84%
S8	7.00E-03	2.72E-02	287.87%	S31d	2.00E-01	2.04E-01	1.84%
S10	5.00E-03	1.94E-02	287.86%	S9	2.00E-01	2.00E-01	0.14%
S12	1.00E-02	2.42E-02	141.75%	S6	7.00E-02	7.01E-02	0.14%
S16	4.00E-02	9.66E-02	141.40%	S13	1.00E-01	1.00E-01	0.01%
D2	3.35E-01	3.43E-01	2.38%	S14	1.00E-01	1.00E-01	0.01%
M2	3.16E-01	3.22E-01	1.84%	S2	1.00E-01	1.00E-01	0.01%
A2	3.19E-01	3.25E-01	1.84%	S4	1.00E-01	1.00E-01	0.01%
S23d	7.00E-02	7.13E-02	1.84%	S18	5.00E-01	5.00E-01	0.00%
S24d	7.00E-02	7.13E-02	1.84%	S32d	5.00E-01	5.00E-01	0.00%
S26d	7.00E-02	7.13E-02	1.84%				

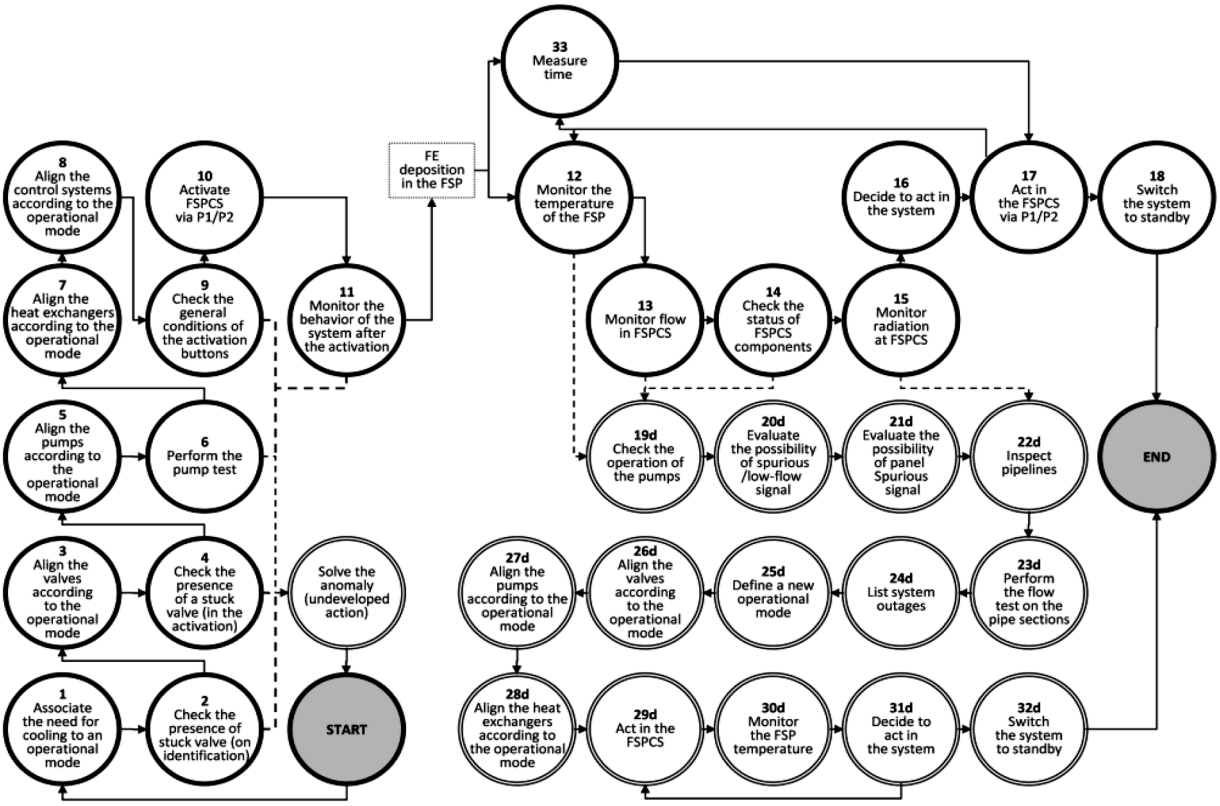


Fig. 14. Variability for P(FSPCS failure), condition "a".

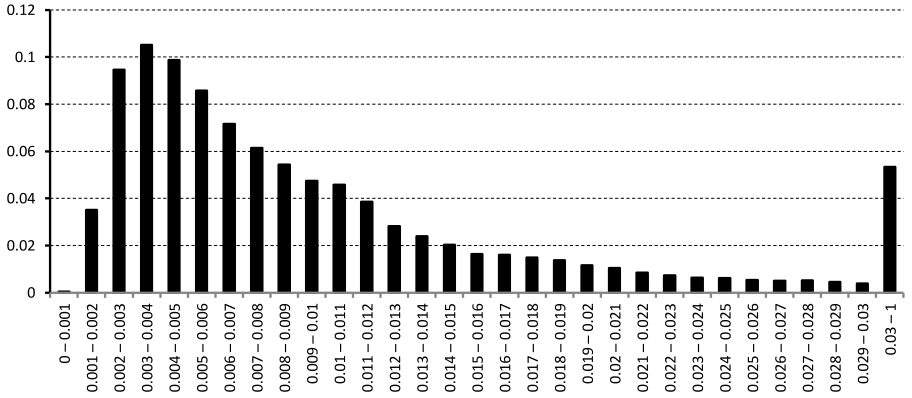


Fig. 15. Variability for P(FSPCS failure), condition "b".

were maintained for these activities, as well as their correlation with the actions of the prospective model. Agent OP1, introduced in 4.2.5.1 was considered for the execution of the action included in this phase. Phase 7 was not considered in this cycle – see justification presented in 4.2.4.2.

Phase 8 – system reliability: The BN considered in 4.2.5.2 was revised to consider the changes presented in 4.3.1 and 4.3.2.1 – illustrated in Fig. 12, as explained in 4.2.4.3. In the Fig. 12 network, the nodes in red refer to the activity added in this second iteration (node "S33"), the action added in this cycle (node "A_C_5a_16"), and the activity associated with other events (the node "S11", previously associated with event #D1, which was also associated with events #A1 and #M1, see 4.3.1). The CPTs for the nodes of this network are presented in Appendix I. The HEP associated with the node for the action added in this cycle was also obtained from Table 9, "Median" column.

According to the resulting BN, the FSPCS failure frequency was calculated to be 1.11%. The most impacted BN nodes were found through Bayesian inference, considering the evidence of FSPCS failure. Table 26 shows the results obtained.

Note in Table 27 that, given the evidence of FSPCS failure, and considering the proposed changes in this iteration, events #A1 and #M1 remain the most impacted – followed by event #D1. Thus, the activities related to these events remain as the activities to be changed in order for a more expressive increase in the system reliability. The FSPCS failure probability was estimated to be 0.12% when the HEP data from the "5-thPercentile" column of Table 9 was employed for the most impacted actions (related to event #M1), instead of "Median" column. The probability of FSPCS failure was estimated to be 0.11% when the same procedure was done for the actions related to event #A1. In spite of the proximity of such results with the goal established in 4.1.1, another cycle of solution development was carried out, as seen in the following section.

4.3.3. Development of solutions – cycle 2 (2nd iteration)

Phases 6 and 7 – grouping agents and cost-benefit analysis: Among the activities related to event #M1 in 4.3.2.1, activity 33 was the only one which was not associated with a verification or redundant action. Thus, for this activity, a redundant action was added regardless of the one included in 4.3.2.1 (Table 26), as described in Table 28. Additionally, this table shows the correlation between the included action and the action of the prospective model of human performance. For the execution of the action included in this phase, the agent OP2 introduced in 4.2.5.1 was considered. Phase 7 was not considered in this cycle – see justification presented in 4.2.4.2.

Phase 8 – system reliability: The BN resulting from the cycle 1 (2nd interaction) was revised to consider the changes presented in 4.3.3.1, resulting the in Fig. 12 BN. In this network, the brown node refers to the action added in this cycle (node "A_C_5a_17") – the other nodes have been previously presented. The CPTs for the nodes of this network are presented in Appendix I. The HEP associated to the node added in this cycle was obtained from Table 9 in the "Median" column.

According to the BN in Fig. 12, the FSPCS failure frequency was calculated to be 0.67%. The most impacted BN nodes were found through Bayesian inference, considering the evidence of FSPCS failure. Table 29 shows the results.

Observe in Table 29 that, given the evidence of FSPCS failure, and considering the proposed change in this cycle, events #A1 and #M1 are the most impacted – followed by event #D1. The probability of FSPCS failure was estimated to be 0.1% when the HEP data from the "5-th Percentile" column of Table 9 was used instead of the "Median" column for some actions related to event #A1 and #M1, i.e., related to the activities most impacted according to Table 29 (activities 11, 17 and 33: "A_C_5a_15", "A_C_5a_16", "A_C_5a_17", "A_C_5a_3", "A_C_5b_3" and "A_P_2_1" in Fig. 12 BN). Such result meets the goal established in 4.1.1. The change in the solution obtained in this cycle is not being proposed in this work.

The evidence of failure in the BN (Fig. 12) demonstrates that event #E2 is the most impacted among the events directly related to equipment failures, i.e., #E1, #E2, #E3 and #E4. Additionally, the most impacted equipment are the pumps, the flow sensors and the connections, when considering the evidence of failure in the BN discussed in 4.1.3. On the other hand, when considering the evidence of success in node "E2"in Fig. 12, the probability of failure in cooling falls from 0.1% to 0.05%. Thus, an alternative to improve FSPCS conditions would be to change equipment configuration or automation. Such proposal, however, is not being considered in this work, and will be approached in a similar context – for the design of a complete system – in a forthcoming paper.

Additionally, note that the use of the data from the "5-th percentile" column (from Table 9; for the HEP of an action) was associated with the evidence of proper conditions for its execution – to be reached during the operation. Such conditions refer to the performance factors which influence the operator in a significant way, for example [22]: (1) Management and Organizational Factors (MOF): e.g., training, selection of personnel; (2) Environmental factors: e.g., visibility, heat, and (3) Internal factors (to the operator): e.g., fatigue, intelligence. These contextual factors should be evaluated in the implementation of the operational procedure as part of an HRA, thus assuring the proper conditions for performing the actions to which the most optimistic HEP were associated.

4.4. Phase 9 – description of the solution for the system

The results presented in the previous phases (4.3.2) propose that the operation of the FSPCS could be carried out by at least two operators – i.e., that two operators could be maintained during the period in which the FSP needs the FSPCS –, identified by OP1 and OP2 in the description of the activities, which must be concomitantly performed. In order for a greater independence of such operators, their distribution in different areas of the plant, as well as the performance of one operator without the presence of the other in the verification activities (e.g., action 3.2 of Table 22) are a sugestion.

The data from Table 29 show that activities 2, 4, 6, 9, 13 and 14 have a low impact on the reliability of the FSPCS operation. The probability of FSPCS failure increases by only 0.22% on evidence of failure in these activities. This result suggests that these activities can be simplified (or even eliminated), and the reliability goal established will still be met.

The results presented in the previous phases can be considered conservative when using the following hypotheses. Such position can be verified, for example, in item 4.1.3 (event tree and equipment failure) and 4.2.4.3 (BN for goal of reliability evaluation), in the calculation of the FSPCS failure probability: (a) The frequency of need for cooling λ(EI) is 1/year (see item 4.1.3); (b) Interface systems (see 4.1.2) do not significantly influence in the FSPCS operation (except for the components considered in 4.1.2 and 4.1.3); (c) The time available for carrying out the activities in the FSPCS is not a critical variable – it was considered that, in the worst case scenario, in the transient between operation in a normal mode and operation in a degraded mode, the FSP water may reach the limit temperature only if the transient lasts more than 38 h (time required to raise the temperature from 41°C to 60°C, see Section 4.1), e; (d)The reliability data for the FSPCS components are those discussed in item 4.1.2.

In addition to the uncertainties associated with these hypotheses, the uncertainties of the prospective model of human performance are added to the results of the previous phases. These uncertainties were represented in the probability functions for the HEPs of the actions included in this model. These functions can be used to estimate the variability of the probability of FSPCS failure. In the solution of the BN shown in Fig. 12, the probability of FSPCS failure was obtained by applying the MCM [79]. This was done under the following conditions: a) by varying the HEPs of all network actions (e.g., node "A_C_3a") according to the performance model probabilities functions (see 3.2.4), and b) by varying the HEPs of all actions in the network according to the performance model probabilities functions, except for the actions related to activities 11, 17 and 33 (actions A_C_5a_15, A_C_5a_16, A_C_5a_17, A_C_5a_3, A_C_5b_3 and A_P_2_1), which maintained the HEPs values according to the "5-thpercentile" column of Table 12. The results are shown in Fig. 14 and Fig. 15, respectively, for condition "a" and condition "b".

Thus, the median for the curve in Fig. 14 equals 7.13E-03, the 5-th percentile equals 2.19E-03, and the 95-thpercentile equals 3.09E-02 – thus showing that the percentile for 1.00E-3 is lower than the 5-th percentile.

For the curve in Fig. 15, the median equals 1.08E-03, the 5-thpercentile equals 8.00E-04, and the 95-thpercentile equals 1.35E-03. In this curve, the probability 1.00E-03 (defined as the conception goal) was obtained for the 28-th percentile.

5. Conclusions and future work

When designing complex systems, considering the human factor is essential to achieving solutions that present acceptable risk and performance. The early consideration of human performance at the design stage may potentially improve the control of risk and costs related to a system – which can be observed throughout its life cycle. Despite the limited availability of resources for the quantitative consideration of human performance in the design phase, over the years several HRA techniques have been developed for risk analysis in general and, as pointed out throughout this paper, the information available in these techniques, in particular its quantitative data (e.g., simulation, experience and expert opinion), can be explored in the development of an updatable model for prospecting human performance.

Overall, this paper discusses the feasibility of quantitatively considering human reliability in the initial design stage, the type of resource needed, and proposes solutions for this consideration. This was done in two parts, focusing on the development of a generic human performance

model and its application in the context of a design methodology aimed at considering human reliability at an early design stage.

5.1. Model for prospecting human performance

This paper discussed the modeling to obtain the probability curves of human error types starting from the HEP of quantified actions and also for the combination of these curves, resulting in the variability of the a priori probability of the error types and, through these estimates, in the a priori HEPs of actions not yet empirically quantified. In addition, this paper presented the modeling for updating this variability by evidence of human performance (data obtained a posteriori) specific to the design system application area – it is emphasized that this modeling does not require defining a family of probability functions for the variables involved in order to allow variability upgrading. Among the difficulties found to obtain this prospective model of human performance, it is highlighted:

- Shortage of "raw" human error data: all the information used in the development of the performance model was extracted from HRA techniques, already processed by its authors. The use of this information made it difficult to associate the error types with the actions of this database.
- Details presented in the literature for the psychomotor and affective domains of Bloom's taxonomy: also related to the association of the types of error to the action, this detailing was considered insufficient to allow the association of the error types, so that all error types were associated to actions at a given performance level, and.
- Approximate method to quantify HEPs: the impossibility of generating an exact and rapid process of calculation and updating – necessary for use in the design phase – led to the use of the MCM.

The application exposed in this paper explored the flexibility of BNs to combine probability distributions concentrated in different orders of magnitude. The analysis of the sensitivity of this model to the sizes of the intervals for the HEPs in the data sources was not presented in this work, being a proposal for future work. Likewise, as a future work, it is considered the comparison of the results of the model in BN with those presented in the sources not used in its elaboration, and the exploration of data from additional sources (e.g., expert opinion) to isolate the source that best fits the FSPCS operator performance.

An expected effect of the application of the performance model presented in this paper is to bring the question of training activities to the design phase of the system. This is because Bloom's taxonomy, used in the model for the classification of human actions, was designed to characterize the objectives of educational experiences, focusing on the expected training that can be observed after submission of the individual to a training process. Thus, educational objectives can be associated with actions still in the design phase, correlating with human reliability data, which is a measure of success in learning.

5.2. FSPCS operational procedure

Using the referred human performance model, a design for the FSPCS operational procedure was obtained considering pre-established characteristics for the reliability of said system. The technique presented in this paper is compatible with the proposed development of a prospective model of human performance by means of a BN, which facilitates integrating the technical results of the process of designing proposed by Martins et al. [40].

The following positive aspects of the applied methodology, which were not aforementioned in this work, were identified: (1) The use of BN in the probabilistic models facilitated the prioritization of the design points which can be improved, particularly because it is easy to perform Bayesian inference; and (2) The use of the prospective model of human performance – using Bloom's taxonomy to classify human actions –simplified the association of the actions to be performed with the quantitative data available in the model, even with incipient information about the operational context.

Alternatively, common techniques in PSA such as FT, for example, could be explored – and features such as importance measures (e.g., Risk Achievement Worth, Risk Reduction Worth and Fussell-Vesely) could be explored using available tools (e.g., CAFTA, Risk Spectrum). The benefits of applying the BNs, however, go beyond the aforementioned ease of integration with the human performance model, and are difficult to achieve with these common techniques, including, as seen in the case study, the possibility of exploring Bayesian inference directly in the system model, the possibility of updating the BN and having an immediate prediction of the effects on the system without the need to change the model, in addition to the possibility of exploring multiple states for the different variables of the model, allowing uncertainty propagation and the presentation of the model results as a non-parametric distribution (as exemplified in Fig. 14) instead of a point data.

Since this is about an operational procedure design, this application has not fully exploited the phases related to the survey of the components, which can compose the system, as well as the study of its functions. Additionally, the applying of Phase 7 (cost-benefit analysis) was deemed unnecessary due to the easiness in associating the operator with a given pre-established equipment composition. Thus, a decision tree was not followed in this design process – though it did not prevent the use of the results of previous iterations in the different phases.

This paper seeks to contribute to the topic (consideration of reliability information during system design) by demonstrating some ways of handling uncertainty during the methodology use. Conservative results for the evaluation of the FSPCS performance were considered, with respect to the assumptions made during analyses, and considering the uncertainties related to the probabilistic models developed in this conception process. Such conservatism could be reduced, for example, if the following were considered:

- A greater detail of the probabilistic models developed: smaller results for the probabilities of failure considered in this work could be found – e.g., in a less conservative alternative, the equipment failures could be detailed in the BN so that their detection could be considered according to the failure mode.
- A greater flexibility for the design: in compliance with the initial proposal for not changing the equipment of the system, the hypothesis of automation, for example, was not considered in this application. By the results analysis, however, it is possible to identify activities which could be automated to reduce the probability of failure in the FSPCS operation – e.g., activity 33 followed by 17 could be automated without significantly changing the FSPCS configuration.
- Further elaboration of the system objectives: by weighing the objectives defined in Phase 2 of the methodology, and in line with the prospective model of human performance, only one complex action was associated with each of the activities of the operational procedure (for each operator). With more detailed objectives, in advanced phases of the design, these activities could be re-evaluated considering the simpler actions which make up the proposed actions in the conception, or the performance model could be altered to consider the specific errors which may occur in these activities.
- Recovery action: possibility of recovery by the operator itself (in this case, if the time to the recovery action is known, the development of dynamic RBs for the calculation of system reliability should be considered in Phase 8 of the methodology).

In a forthcoming paper, the application of this methodology will be presented for the design of a complete system – i.e., for the same FSPCS function, determining the system configuration considering both the insertion of human factor and equipment, and comparing the results with those presented in this first paper and with a solution generated

without the aid of this methodology,.

CRediT authorship contribution statement

Marcos Coelho Maturana: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Visualization. **Marcelo Ramos Martins:** Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Supervision. **Paulo Fernando Ferreira Frutuoso e Melo:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing.

Declaration of Competing Interest

On behalf of all the authors, I declare there is not any competing interests to declare that could inappropriately influence (bias) the development of the work presented.

Acknowledgments

Prof. Marcelo Martins gratefully wishes to acknowledge his support by the Brazilian National Council for Scientific and Technological Development (CNPq) through grant 308712/2019-6.

APPENDIX I – Probabilities for the BNs for reliability goal evaluation

This appendix presents the probabilities and CPTs of the BNs used in Phase 8 of each solution development cycle. Since these BNs are altered versions of each other – i.e., they consist of many nodes with common characteristics –, this appendix presents (1) Data of the cycle 1 (1st iteration) BN: Table 30 presents the probabilities for the parent nodes without CPT, and Tables 31–38 show the CPTs for the other nodes; (2) Data changed and added to the cycle 1 (1st iteration) BN to obtain the cycle 2 (1st iteration) BN: Table 39 presents the data for the added parent nodes without CPT, and Tables 40–47 show the CPTs for the

Table 30
Probabilities for BN nodes for cycle 1 (1st iteration) that do not have CPT.

Node	States	Probabilities	Node	States	Probabilities	Node	States	Probabilities
E1	Success	9.99E-01	A_C_3a_7	Success	9.30E-01	A_C_5b	Success	8.00E-01
	Failure	6.74E-04		Error	7.00E-02		Error	2.00E-01
E2	Success	9.99E-01	A_C_3a_8	Success	9.30E-01	A_C_5b_1	Success	8.00E-01
	Failure_REC	4.00E-04		Error	7.00E-02		Error	2.00E-01
	Failure_IRR	2.62E-04	A_C_3a_9	Success	9.30E-01	A_C_5b_2	Success	8.00E-01
E4	Success	9.99E-01		Error	7.00E-02		Error	2.00E-01
	Failure	1.13E-03	A_C_3b	Success	9.10E-01	A_C_5a_4	Success	9.00E-01
E3	Success	0.999718		Error	9.00E-02		Error	1.00E-01
	Failure	2.82E-04	A_C_4a	Success	9.60E-01	A_C_5a_5	Success	9.00E-01
A_C_3a	Success	9.30E-01		Error	4.00E-02		Error	1.00E-01
	Error	7.00E-02	A_C_4a_1	Success	9.60E-01	A_C_5a_6	Success	9.00E-01
A_C_3a_1	Success	9.30E-01		Error	4.00E-02		Error	1.00E-01
	Error	7.00E-02	A_C_4a_2	Success	9.60E-01	A_C_5a_7	Success	9.00E-01
A_C_3a_2	Success	9.30E-01		Error	4.00E-02		Error	1.00E-01
	Error	7.00E-02	A_C_5a	Success	9.00E-01	A_C_5a_8	Success	9.00E-01
A_C_3a_3	Success	9.30E-01		Error	1.00E-01		Error	1.00E-01
	Error	7.00E-02	A_C_5a_1	Success	9.00E-01	A_P_2	Success	9.50E-01
A_C_3a_4	Success	9.30E-01		Error	1.00E-01		Error	5.00E-02
	Error	7.00E-02	A_C_5a_2	Success	9.00E-01	A_P_2_1	Success	9.50E-01
A_C_3a_5	Success	9.30E-01		Error	1.00E-01		Error	5.00E-02
	Error	7.00E-02	A_C_5a_3	Success	9.00E-01	A_P_2_2	Success	9.50E-01
A_C_3a_6	Success	9.30E-01		Error	1.00E-01		Error	5.00E-02
	Error	7.00E-02						

Table 31
CPT for the activity nodes in BN for cycle 1 (1st iteration).

S2	A_C_5a_1	S9	A_C_5b_2	S17	A_P_2_1	S25d	A_C_3b
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S3	A_C_3a	S10	A_P_2	S19d	A_C_5a_8	S26d	A_C_3a_5
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S4	A_C_5a_2	S11	A_C_5a_3	S20d	A_C_4a	S27d	A_C_3a_6
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S5	A_C_3a_1	S12	A_C_5a_4	S21d	A_C_4a_1	S28d	A_C_3a_7
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S6	A_C_3a_8	S13	A_C_5a_5	S22d	A_C_4a_2	S29d	A_P_2_2
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S7	A_C_3a_3	S14	A_C_5a_6	S23d	A_C_3a_9	S30d	A_C_5a
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S8	A_C_3a_2	S15	A_C_5a_7	S24d	A_C_3a_4	S31d	A_C_5b_1
Adequate	Success	Adequate	Success	Adequate	Success	Adequate	Success
Inadequate	Error	Inadequate	Error	Inadequate	Error	Inadequate	Error
S16	A_C_5b						
Adequate	Success						
Inadequate	Error						

Table 32
CPT for the node "A1" in BN for cycle 1 (1st iteration).

A1	S3	S5	S7	S8
Success	Adequate	Adequate	Adequate	Adequate
Failure	Other combinations			

Table 33
CPT for the node "A2" in BN for cycle 1 (1st iteration).

A2	S24d	S25d	S26d	S27d	S28d
Success	Adequate	Adequate	Adequate	Adequate	Adequate
Failure	Other combinations				

Table 34
CPT for the node "M1" in BN for cycle 1 (1st iteration).

M1	S10	S12	S16	S17
Success	Adequate	Adequate	Adequate	Adequate
Failure	Other combinations			

Table 35
CPT for the node "M2" in BN for cycle 1 (1st iteration).

M2	S29d	S30d	S31d
Success	Adequate	Adequate	Adequate
Failure	Other combinations		

Table 36
CPT for the node "D1" in BN for cycle 1 (1st iteration).

D1	S11	S6	S9	S2	S4
Success	Adequate	Any combination			
Success	Inadequate	Adequate	Adequate	Adequate	Adequate
Success	Inadequate	Adequate	Adequate	Adequate	Inadequate
Success	Inadequate	Adequate	Adequate	Inadequate	Adequate
Failure	Other combinations				

Table 37
CPT for the node "D2" in BN for cycle 1 (1st iteration).

D2	S15	S19d	S20d	S21d	S22d	S23d	S12	S13	S14
Success	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate
Success	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Inadequate
Success	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Inadequate	Adequate
Success	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Inadequate	Inadequate
Success	Adequate	Adequate	Adequate	Adequate	Adequate	Adequate	Inadequate	Adequate	Adequate
Failure	Other combinations								

Table 38
CPT for the node "FSPCS" in BN for cycle 1 (1st iteration)

FSPCS	E1	D1	A1	M1	E2	D2	E3	A2	M2	E4
Success	Success	Success	Success	Success	Success	Any combination				
Success	Success	Success	Success	Success	Failure_REC	Success	Success	Success	Success	Success
Success	Success	Failure	Success	Success	Success	Any combination				
Success	Success	Failure	Success	Success	Failure_REC	Success	Success	Success	Success	Success
Success	Failure	Success	Success	Success	Success	Any combination				
Success	Failure	Success	Success	Success	Failure_REC	Success	Success	Success	Success	Success
Failure	Other combinations									

Table 39
Probabilities for BN nodes for cycle 2 (1st iteration) that do not have CPT.

Node	States	Probabilities	Node	States	Probabilities
A_C_5b_3	Success	0.8	A_C_5a_12	Success	0.9
	Error	0.2		Error	0.1
A_C_5a_9	Success	0.9	A_C_5a_13	Success	0.9
	Error	0.1		Error	0.1
A_C_5a_10	Success	0.9	A_C_5b_4	Success	0.8
	Error	0.1		Error	0.2
A_C_5a_11	Success	0.9	A_C_5a_15	Success	0.9
	Error	0.1		Error	0.1

Table 40
CPT for the node "S3" in BN for cycle 2 (1st iteration).

S3	A_C_3a	A_C_5a_9
Inadequate	Error	Error
Adequate	Other combinations	

Table 41
CPT for the node "S5" in BN for cycle 2 (1st iteration).

S5	A_C_3a_1	A_C_5a_10
Inadequate	Error	Error
Adequate	Other combinations	

Table 42
CPT for the node "S8" in BN for cycle 2 (1st iteration).

S8	A_C_3a_2	A_C_5a_12
Inadequate	Error	Error
Adequate	Other combinations	

Table 43
CPT for the node "S7" in BN for cycle 2 (1st iteration).

S7	A_C_3a_3	A_C_5a_11
Inadequate	Error	Error
Adequate	Other combinations	

Table 44
CPT for the node "S17" in BN for cycle 2 (1st iteration).

S17	A_P_2_1	A_C_5a_15
Inadequate	Error	Error
Adequate	Other combinations	

Table 45
CPT for the node "S16" in BN for cycle 2 (1st iteration).

S16	A_C_5b	A_C_5b_4
Inadequate	Error	Error
Adequate	Other combinations	

Table 46
CPT for the node "S10" in BN for cycle 2 (1st iteration).

S10	A_P_2	A_C_5a_13
Inadequate	Error	Error
Adequate	Other combinations	

Table 47
CPT for the node "S11" in BN for cycle 2 (1st iteration).

S11	A_C_5a_3	A_C_5b_3
Inadequate	Error	Error
Adequate	Other combinations	

Table 48
Probabilities for node "A_C_5a_16" for cycle 1 (2nd iteration).

Node	States	Probabilities
A_C_5a_16	Success	0.9
	Error	0.1

Table 49
CPT for the node "S33" in BN for cycle 1 (2nd iteration)

S33	A_C_5a_16
Adequate	Success
Inadequate	Error

changed nodes; (3) Data changed and added to the cycle 2 (1st iteration) BN to obtain the cycle 1 (2nd iteration) BN: Tables 48 and 49 present the data for the added nodes, and Tables 50 and 51 present the data for the altered nodes; (4) Data of the changed node and the node added in the cycle 1 (2nd iteration) BN to obtain the BN of Fig. 12: Table 52 presents the data for the added node, and Table 53 presents the data for the changed node. It is important to emphasize that there was no node elimination in this process.

Table 51
CPT for the node "A1" in BN for cycle 1 (2nd iteration)

A1	S11	S3	S5	S7	S8
Success	Adequate	Any combination			
Success	Inadequate	Adequate	Adequate	Adequate	Adequate
Failure	Inadequate	Other combinations			

Table 52
Probabilities for node "A_C_5a_17" in Fig. 10.

Node	States	Probabilities
A_C_5a_17	Success	0.9
	Error	0.1

Table 53
CPT for the node "S33" in BN of Fig. 10.

S33	A_C_5a_16	A_C_5a_17
Inadequate	Error	Error
Adequate	Other combinations	

References

[1] Norman DO, Kuras ML. Engineering complex systems. In: Braha D, Minai AA, Bar-Yam Y, editors. Complex engineered systems: science meets technology. eds. Cambridge, MA: Springer NECSI; 2006.
[2] Abbott R. Putting complex systems to work. Complexity 2007;13:30–49. i.2.
[3] Pahl G, Beitz W, Feldhusen J, Grote K-H. Engineering design: a systematic approach. London, UK: Springer; 2007.
[4] Johnson CA, Flage R, Guikema SD. Feasibility study of PRA for critical infrastructure risk analysis. Reliab Eng Syst Saf 2021;212.
[5] Parhizkar T, Vinnem JE, Utne IB, Mosleh A. Supervised dynamic probabilistic risk assessment of complex systems, Part 1: general overview. Reliab Eng Syst Saf 2021; 208.
[6] National Aeronautics and Space Administration – NASA. Probabilistic risk assessment procedures guide for NASA. 2nd Ed. Washington, DC, USA: National Aeronautics and Space Administration; 2011.
[7] Carnino A. Human reliability. Nucl Eng Des 1985;90:365–9. v.n.3.
[8] Abo EE, Maged A, Raouf A. Manual backup operations: Some behavioral aspects of human reliability. Microelectron Reliab 1979;19:141–9. v.n.1.
[9] Chang YHJ, Mosleh A. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 1: overview of the IDAC model. Reliab Eng Syst Saf 2007;92:997–1013. v.
[10] Park J, Kim Y, Jung W. Calculating nominal human error probabilities from the operation experience of domestic nuclear power plants. Reliab Eng Syst Saf 2018; 170:215–25. v.
[11] United States General Accounting Office – USGAO. EMD-80-109: three mile island: the most studied nuclear accident in history. Washington, D.C: General Accounting Office; 1980.
[12] Hollnagel E. Human reliability assessment in context. Nucl Eng Technol 2005;37: 159–66. v.n. 2.
[13] United States Nuclear Regulatory Commission – USNRC. NUREG-0800, section 19.0, revision 3: standard review plan: probabilistic risk assessment and severe accident evaluation for new reactors. Washington, D. C.: United States Nuclear Regulatory Commission, 2015.
[14] Madonna M, Martella M, Monica L, Maini EP, Tomassini L. The human factor in risk assessment: methodological comparison between human reliability analysis techniques. Prevention; 2009. p. 67–83. Today, v.5, n°1/2.
[15] Mosleh A. PRA: a perspective on strengths, current limitations, and possible improvements. Nucl Eng Technol 2014;46:1–10. v.46, n°.1.

Table 50
CPT for the node "M1" in BN for cycle 1 (2nd iteration).

M1	S11	S33	S17	S10	S12	S16
Success	Adequate	Adequate	Adequate	Any combination		
Failure	Adequate	Adequate	Inadequate	Any combination		
Success	Adequate	Inadequate	Adequate	Adequate	Adequate	Adequate
Failure	Adequate	Inadequate	Other combinations			
Success	Inadequate	Adequate	Adequate	Adequate	Other combinations	
Failure	Inadequate	Adequate	Other combinations			
Success	Inadequate	Inadequate	Adequate	Adequate	Adequate	Adequate
Failure	Inadequate	Inadequate	Other combinations			

[16] Meister D. The history of human factors and ergonomics. Mahwah, NJ: Lawrence Erlbaum Associates; 1999.
[17] Swain AD, Guttmann HE. NUREG/CR-1278: handbook of human reliability analysis with emphasis on nuclear power plant applications. Washington, D.C: United States Nuclear Regulatory Commission; 1983.
[18] Patriarca R, Ramos M, Paltrinieri N, Massaiu S, Costantino F, Di Gravio G, Boring RL. Human reliability analysis: exploring the intellectual structure of a research field. Reliab Eng Syst Saf 2020:203. v.
[19] United States Nuclear Regulatory Commission – USNRC. WASH-1400 (NUREG-75/014): reactor safety study: an assessment of accident risks in U.S. commercial nuclear power plants. Washington, D.C: USNRC; 1975.
[20] Kirwan B. A guide to practical human reliability assessment. London: Taylor & Francis; 1994.
[21] Hollnagel E. Cognitive reliability and error analysis method – CREAM. Oxford: Elsevier Science Ltd.; 1998.
[22] Martins MR, Maturana MC. Application of Bayesian belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents. Reliab Eng Syst Saf 2013:89–109. v.110.
[23] Mosleh A, Chang YH. Model-based human reliability analysis: prospects and requirements. Reliab Eng Syst Saf 2004:241–53. v.83.
[24] French S, Bedford T, Pollard SJT, Soane E. Human Reliability Analysis: a critique and review for managers. Saf Sci 2011;v.49, i.6:753–63. July.
[25] Groth KM, Smith R, Moradi R. A hybrid algorithm for developing third generation HRA methods using simulator data, causal models, and cognitive science. Reliab Eng Syst Saf 2019:191. v.
[26] Zheng X, Matthew L, Bolton ML, Dalyb C, Biltekoffa E. The development of a next-generation human reliability analysis: Systems Analysis for Formal Pharmaceutical Human Reliability (SAFPH). Reliab Eng Syst Saf 2020:202. v.
[27] Bell J, Holroyd J. Research report RR679: review of human reliability assessment methods. Buxton, Derbyshire: UK: Health and Safety Executive – HSE, Health and Safety Laboratory – HSL; 2009.
[28] Boring RL, Hendrickson SML, Forester JA, Tran TQ, Erasmia Lois E. Issues in benchmarking human reliability analysis methods: a literature review. Reliab Eng Syst Saf 2010;95:591–605. v.
[29] Liao H, Forester J, Dang VN, Bye A, Chang YHJ, Lois E. Assessment of HRA method predictions against operating crew performance: Part II: overall simulator data, HRA method predictions, and intra-method comparisons. Reliab Eng Syst Saf 2019:191. v.
[30] Oxstrand J, Boring RL. NKS-R-77: human reliability guidance – how to increase the synergies between human reliability, human factors, and system design & engineering. Phase 1: the Nordic point of view – a user needs analysis. Interim report. Roskilde, Denmark: Nordic nuclear safety research; 2009.
[31] Oxstrand J. NKS_R-2009_77: human reliability guidance - how to increase the synergies between human reliability, human factors, and system design & engineering. Phase 2: the American point of view - insights of how the US nuclear industry works with human reliability analysis. Interim report. Roskilde, Denmark: Nordic nuclear safety research; 2010. December.
[32] Mkrtchyan L, Podofillini L, Dang VN. Bayesian belief networks for human reliability analysis: A review of applications and gaps. Reliab Eng Syst Saf 2015;139:1–16. vJuly.
[33] Chandler FT, Chang YH, Mosleh A, Marble JL, Boring RL, Gertman DI. Human reliability analysis methods: selection guidance for NASA. Washington, DC: National Aeronautics and Space Administration – NASA, NASA/OSMA Technical Report; 2006. July.
[34] Abrishami S, Khakzad N, Hosseini SM. A data-based comparison of BN-HRA models in assessing human error probability: an offshore evacuation case study. Reliab Eng Syst Saf 2020;202. v.
[35] Musharraf M, Bradbury-Squires D, Khan F, Veitch B, MacKinnon S, Imtiaz S. A virtual experimental technique for data collection for a Bayesian network approach to human reliability analysis. Reliab Eng Syst Saf 2014;132:1–8. v.
[36] Podofillini L, Mosleh A. Foundations and novel domains for Human Reliability Analysis. Reliab Eng Syst Saf 2020;194. v.
[37] Hannaman GW. The role of frameworks, models, data, and judgment in human reliability analysis. Nucl Eng Des 1986;93(2):295–301. v.
[38] National Aeronautics and Space Administration – NASA. Practice n° PD-ED-1273: quantitative reliability requirements used as performance-based requirements for space systems. Washington, DC, USA: National Aeronautics and Space Administration; 1995.
[39] Papin B. Balancing human and technical reliability in the design of advanced nuclear reactors. Nucl Eng Des 2011;241:5238–44. v.
[40] Martins MR, Melo PFF, Maturana MC. Methodology for system reliability analysis during the conceptual phase of complex system design considering human factors. In: Proceeding of the ANS PSA 2015 international topical meeting on probabilistic safety assessment and analysis; 2015. April 26-30, 2015on CD-ROM, American Nuclear Society, LaGrange Park, IL.
[41] International Atomic Energy Agency – IAEA. IAEA-TECDOC-1200, applications of Probabilistic Safety Assessment (PSA) for nuclear power plants. Vienna, Austria: International Atomic Energy Agency; 2001.
[42] Montewka J, Goerlandt F, Innes-Jones G, Owen D, Hifi Y, Puisa R. Enhancing human performance in ship operations by modifying global design factors at the design stage. Reliab Eng Syst Saf 2017;159:283–300. v.
[43] Ibánez L, Hortal J, Queral C, Gómez-Magán J, Sánchez-Perea M, Fernández I, Meléndez E, Expósito A, Izquierdo JM, Gil J, Marrao H, Villalba-Jabonero E. Application of the integrated safety assessment methodology to safety margins. Dynamic event trees, damage domains and risk assessment. Reliab Eng Syst Saf 2016;147:170–93. v.
[44] International Atomic Energy Agency – IAEA. IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA). Vienna: Austria: IAEA; 1999.
[45] Greenberg M, Haas C, Cox Jr. A, Lowrie K, McComas K, North W. Ten most important accomplishments in risk analysis, 1980–2010. Risk Anal 2012;32:5. vn.
[46] International Maritime Organization – IMO. Revised guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process, MSC-MEPC.2/Circ.12. London: International Maritime Organization; 2013.
[47] National Aeronautics and Space Administration – NASA. Practice n° PD-AP-1313: system reliability assessment using block diagramming methods. Washington, DC: USA: National Aeronautics and Space Administration; 1995.
[48] Modarres M, Kaminskiy M, Krivitsovs V. Reliability engineering and risk analysis: a pratical guide. USA: CRC Press, Taylor & Francis Group; 2010.
[49] International Atomic Energy Agency – IAEA. IAEA-TECDOC-1264, reliability assurance programme guidebook for advanced light water reactors. Vienna: Austria: IAEA; 2001.
[50] Maturana MC, Martins MR. Technique for early consideration of human reliability: applying a generic model in an oil tanker operation to study scenarios of collision. J Offshore Mech Arct Eng Trans ASME 2019;141:051607. v.
[51] Martins MR, Maturana MC. Human error contribution in collision and grounding of oil tankers. Risk Anal 2010;30(4):674–98. v.
[52] Rausand M, Hoyland A. System reliability theory: models, statistical methods, and applications. 2nd ed. Hoboken, New Jersey: John Wiley & sons, Inc.; 2004.
[53] Bloom BS, Engelhart MD, Furst EJ, Hill WH, Krathwohl DR. Taxonomy of educational objectives: the classification of educational goals. Handbook I: cognitive domain. New York, USA: David McKay Company; 1956.
[54] Jansen BJ, Booth D, Smith B. Using the taxonomy of cognitive learning to model online searching. Inf Process Manag 2009;45:643–63. v.
[55] Krathwohl DR, Bloom BS, Masia BB. Taxonomy of educational objectives: the classification of educational goals. Handbook II: the affective domain. New York, USA: David McKay Company; 1964.
[56] Harrow AJ. A taxonomy of the psychomotor domain: a guide for developing behavioral objectives. New York, USA: David McKay Company; 1972.
[57] Simpson EJ. The classification of educational objectives: psychomotor domain. Ill J Home Econ 1966:110–44. v.10, n.4.
[58] Dave RH. Psychomotor levels. In: Armstrong RJ, editor. Developing and writing behavioral objectives. Ed. Tucson, AZ: Educational Innovators Press; 1970.
[59] Anderson LW, Krathwohl DR. A taxonomy for learning, teaching and assessing: a revision of Bloom's taxonomy of educational objectives. Nova York, USA: Addison Wesley Longman; 2001.
[60] Krathwohl DR. A revision of Bloom's taxonomy: an overview. Theory Pract 2002:212–8. v.41, n. 4.
[61] Newton, P. M.; Da Silva, A.; Peters, L. G. A pragmatic master list of action verbs for Bloom's taxonomy. Front Educ, v. 5, 2020.
[62] Baziuk PA, Rivera SS, Leod JNM. Towards human factor taxonomy with cognitive generic terms. In: Proceedings of the world congress on engineering 2014 – WCE 2014; 2014. July 2-4.
[63] Rasmussen J, Duncan K, Leplt J. New technology and human error. Ed. Chichester: John Wiley and Sons; 1987.
[64] Reason J. Human error. Cambridge: Cambridge University Press; 1990.
[65] Wood SD. Extending GOMS to human error and applying it to error-tolerant design. Michigan: University of Michigan; 2000. PhD Dissertation.
[66] Shorrock ST, Kirwan B. Development and application of a human error identification tool for air traffic control. Appl Ergon 2002;(33):319–36. n.
[67] Rasmussen J, Pedersen OM, Carnino A, Griffon M, Mancini C, Gagnolet P. Classification system for reporting events involving human malfunctions, Report Risø-M-240, DK-4000. Roskilde, Denmark: Risø National Laboratories; 1981.
[68] Burns KJ, Bonaceto C. An empirically benchmarked human reliability analysis of general aviation. Reliab Eng Syst Saf 2018;194. v.
[69] Reason JT, Embrey DE. Human factors principles relevant to the modelling of human error in abnormal conditions of nuclear and major hazardous installations, report ECI-1164-B7221-84-UK. Parbold, Lancs: England: Human Reliability Associates Ltd; 1985.
[70] Norsys Software Corp. Application for belief networks and influence diagrams, user's guide. Vancouver, BC: Canada: Norsys Software Corp.; 1996.
[71] Martorell P, Martón I, Sánchez AI, Martorell S, Sanchez-Saez F, Saiz M. Evaluation of risk impact of completion time changes combining PSA and DSA model insight and human reliability analysis. Reliab Eng Syst Saf 2018;178:97–107. v.
[72] Park J, Chang YJ, Kim Y, Choi S, Kim S, Jung W. The use of the SACADA taxonomy to analyze simulation records: Insights and suggestions. Reliab Eng Syst Saf 2017;159:174–83. v.
[73] Chang YJ, Bley D, Criscione L, Kirwan B, Mosleh A, Madary T, Nowell R, Richards R, Roth EM, Sieben S, Zoulis A. The SACADA database for human reliability and human performance. Reliab Eng Syst Saf 2014;125:117–33. v.
[74] Jung W, Park J, Kim Y, Choi SY, Kim S. HuREX – A framework of HRA data collection from simulators in nuclear power plants. Reliab Eng Syst Saf 2020;194. v.
[75] Kirwan B, Gibson HCARA. A human reliability assessment tool for air traffic safety management – technical basis and preliminary architecture. In: Redmill F, Anderson T, editors. The safety of systems: proceedings of the fifteenth safety-critical systems symposium. Ed. London: Springer; 2007. p. 13–5. February2007.
[76] Williams JC. HEART – a proposed method for achieving high reliability in process operation by means of human factors engineering technology. In: Proceedings of a symposium on the achievement of reliability in operating plant, southport: safety and reliability society; 1985. 16 September.

[77] Gertman DI, Blackmann HS, Haney LN, Seidler KS, Hahn HA. INTENT: a method for estimating human error probabilities for decision based errors. Reliab Eng Syst Saf 1992;35:127–36. v.
[78] Bello GC, Colombari V. Empirical technique to estimate operator's error (TESEO). Reliab Eng 1980;1(3):3–24. v.
[79] Robert CP, Casella G. Monte Carlo statistical methods. 2nd Ed. New York: Springer; 2004.
[80] Center for Chemical Process Safety – CCPS. Guidelines for process equipment reliability data with data tables. New York, NY: Center for Chemical Process Safety – American Institute of Chemical Engineers; 1989.
[81] SINTEF. Offshore reliability data handbook, OREDA-2009, SINTEF industrial management. 5th Ed., 1. Norway: Det Norske Veritas; 2009.
[82] Kirwan B, Ainsworth LK. A guide to task analysis. London: Taylor & Francis; 1994.
[83] Shepherd A. Analysis and training in information technology tasks. In: Diaper D, editor. Task analysis for human-computer interaction. Ed. Chichester: Ellis Horwood; 1989. p. 15–55.
[84] Stanton NA. Hierarchical task analysis: developments, applications, and extensions. Appl Ergon 2006;37:55–79.