Safety Science 103 (2018) 137–152

Contents lists available at ScienceDirect

Safety Science

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

A novel qualitative prospective methodology to assess human error during accident sequences

Romina D. Calvo Olivares[a,b,*], Selva S. Rivera[a], Jorge E. Núñez Mc Leod[a,b]

[a] CEDIAC, Engineering Faculty, Cuyo National University, Centro Universitario, CO M5502JMA, Mendoza, Argentina
[b] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina

ARTICLE INFO

Keywords:
Qualitative prospective model
Human error
Human reliability assessment
Accident sequences
Human-machine interface

ABSTRACT

Numerous theoretical models and techniques to assess human error were developed since the 60's. Most of these models were developed for the nuclear, military, and aviation sectors. These methods have the following weaknesses that limit their use in industry: the lack of analysis of underlying causal cognitive mechanisms, need of retrospective data for implementation, strong dependence on expert judgment, focus on a particular type of error, and/or analysis of operator behaviour and decision-making without considering the role of the system in such decisions. The purpose of the present research is to develop a qualitative prospective methodology that does not depend exclusively on retrospective information, that does not require expert judgment for implementation and that allows predicting potential sequences of accidents before they occur. It has been proposed for new (or existent) small and medium- scale facilities, whose processes are simple. To the best of our knowledge, a methodology that meets these requirements has not been reported in literature thus far. The methodology proposed in this study was applied to the methanol storage area of a biodiesel facility. It could predict potential sequences of accidents, through the analysis of information provided by different system devices and the study of the possible deviations of operators in decision-making. It also enabled the identification of the shortcomings in the human-machine interface and proposed an optimization of the current configuration.

1. Introduction

Human beings play an essential role in the reliability of the engineering systems because they are involved in not only the specification, design, implementation, installation, start-up, and maintenance, but also the operation of these systems. This makes it almost impossible to design systems in which human error is totally eliminated (Foord and Gulland, 2006; Baziuk et al., 2016). Therefore, human reliability, human error, and the tendency to make mistakes are problems of fundamental importance.

The accident at the nuclear power plant at the Three Mile Island in March 1979 (Kemeny, 1979) prompted the mandatory use of the emerging approach called 'Human Reliability Assessment' (HRA). HRA is defined as 'the probability that a job or a task is satisfactorily completed by an individual, during a specific stage of the system operation in a minimal required time, if that time requirement exists' (Meister, 1966).

Meanwhile, human error is defined as 'that action performed by an individual, which was not intended by the actor; not desired by a set of rules or an external observer; or that led the task or system outside its acceptable limits' (Senders and Moray, 1991). Negligence and violations are not considered as human errors. Negligence involves incompetence and carelessness in carrying out the tasks. A violation is a deliberate (intentional) deviation from safe operating practices, procedures, standards, or established rules (Reason, 1990).

The beginning of the studies on human error dates back to the late 50s, in the nuclear and military domains. During the 60s, a series of publications related directly or indirectly to human reliability and error was published (Meister, 1971). In the same decade, and extending into the 70s, systems of human error classification and even databases of human error, which were mainly used for the military domain and in some early developments of nuclear power plants, were developed (Isaac et al., 2002). During this period, the cognitive approach emerged, and humans were beginning to be considered as information processors. It was also found that the functions of solving problems and decision-making are predominant in abnormal situations, in which human failure has severe consequences (Amyotte and Khan, 2005). The major development of HRA techniques occurred in the 80s. In addition, a deep understanding of human errors, including causes, manifestation, and consequences, arose (Hollnagel, 2005). In the 90s, some of the HRA techniques reached maturity, and human error models were expanded

* Corresponding author at: Eng. Faculty, Cuyo National University, Centro Universitario, CO M5502JMA, Ciudad, Mendoza, Argentina.
E-mail addresses: rcalvo@cediac.uncu.edu.ar (R.D. Calvo Olivares), srivera@cediac.uncu.edu.ar (S.S. Rivera), jnmcleod@cediac.uncu.edu.ar (J.E. Núñez Mc Leod).

https://doi.org/10.1016/j.ssci.2017.10.023
Received 31 March 2017; Received in revised form 29 September 2017; Accepted 30 October 2017

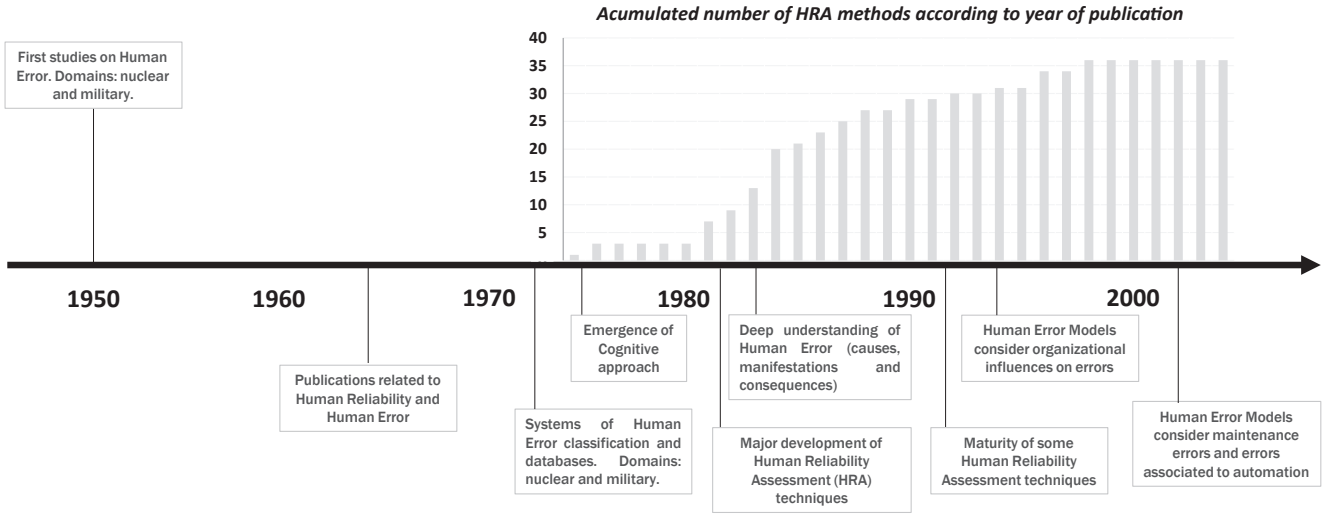

Fig. 1. Timeline of human error and human reliability studies.

to consider organizational influences on errors and, more recently, on maintenance errors and errors associated with automation (Isaac et al., 2002). Fig. 1 shows a graphical summary of studies on human error and human reliability over time. Data about accumulated number of Human Reliability Assessment methods according to year of publication were extracted from (Hollnagel, 2005, p.160).

Today, as a result of years of research on human error, numerous theoretical models, taxonomies and techniques have been developed (Isaac et al., 2002):

1. Taxonomies based on the task: They allow classification of human errors into different categories based on the Error Modes (Swain and Guttmann, 1983; Swain, 1982) or the System (Spurgin et al., 1987).
2. Taxonomies of information processing: They assess human performance when trying to localize the flow of information across several processing stages, from information input to output response (Broadbent, 1998; Payne and Altman, 1962; Wickens, 1992).
3. Taxonomies and models of symbolic processing: This approach considers humans and computers as systems of symbolic manipulation for general purposes. Known examples are Rasmussen's models such as *SKR* (Rasmussen, 1981), Multifaceted taxonomy (Rasmussen, 1982), and *Step-ladder* model (Rasmussen, 1986); Murphy diagrams (Pew et al., 1982); the Systematic Human Error Reduction and Prediction Approach or SHERPA (Embrey, 1986; Stanton et al., 2005), and Reason's models as Slips, Lapses, Mistakes and Violations (Reason, 1990), Actions Not as Planned (Reason, 1979) and the Generic Error-modelling System (Reason, 1987, 1990). Other taxonomies included in this classification are those that categorizes slips of actions (Norman, 1981), the Seven-step Model of Human Action (Norman, 1986), and the Situation Awareness Error Taxonomy (Endsley, 1988).
4. HRA techniques for quantification of human error: According to Bell and Holroyd (2009), they are classified as follows:

– First-generation methods: These methods focused on the rules and ability levels of human action, and they do not consider the cognitive causes of human error (Baziuk et al., 2016). They are characterized by dividing tasks into their components and then considering the potential impact of modifying factors such as time pressure, equipment design and stress. The combination of these elements allows determining nominal Human Error Probabilities (HEPs). Examples of this type of techniques are THERP (Swain and Guttmann, 1983; Swain, 1964), ASEP (Swain, 1987), HEART (Williams, 1985, 1986, 1988), SPAR-H (Gertman et al., 2005), HRMS, JHEDI (Kirwan, 1996, 1997), and INTENT (Gertman et al., 1992).
– Second-generation methods: They are under development and have not been validated empirically. They focus on human behaviour and cognitive causes of human error (Baziuk et al., 2016). They incorporate the context and commission errors in the prediction of human error. Examples of these methods are ATHEANA (Cooper et al., 1996; Forester et al., 2007; U.S. Nuclear Regulatory Commission, 2000), CREAM (Hollnagel, 1993, 1998), CAHR (Sträter, 1997, 2000), and MERMOS.
– Third-generation methods: They are based on the first-generation methods and are under development. Example: NARA.
– Expert judgment methodologies: These tools provide structured methods to the experts to analyse the probability of a human error in a particular scenario. Although the validity of some of these tools has been questioned, they continue to be used to determine error probabilities. Examples of these techniques are APJ (Seaver and Stillwell, 1983), PC (Kirwan, 1994), and SLIM-MAUD (Embrey, 1983).

Table 1 shows a summary of models, taxonomies and techniques for human error analysis.

There have also been developed accident analysis models such as STAMP (Leveson, 2011). STAMP was built on basic Systems Theory and focuses on inadequate control or enforcement of safety-related constraints on the system design, development and operation. Unlike traditional techniques, it has the ability to view systems as dynamic processes with continuous changes in product/process design, technologies, workforce, etc. (Leveson, 2004). It has been utilized to analyse multiple post accident, and more hazards and potential failures in systems have been found (Leveson, 2002; Leveson and Laracy, 2007; Song, 2012). Recently, the model has been applied to analyse a case of study in the oil and gas industry (Altabbakh et al., 2014), and to the Sewol ferry tragedy in order to demonstrate the utility of applying STAMP model to the maritime transportation domain. In the first case, the model successfully identified violations against safety constraints that resulted in the accident. In the second case, some recommenations were developed for continuous improvements and actions to prevent future occurrences of such catastrophic accident (Kim et al., 2016).

The use of human reliability assessment techniques allows improving the reliability, availability, and maintainability of any system, resulting in a better cost-benefit ratio. These enhancements are included in different stages such as design, detailed engineering, and operation. This, in turn, facilitates ensuring the safety of the system, the plant staff, and the environment. However, the aforementioned methods have some deficiencies, which limit their extensive use.

According to Griffith and Mahadevan (2011), current HRA methods

Table 1
Summary of models, taxonomies and techniques for human error analysis.

Taxonomies based on the task	Error Modes	Errors of omission-required action not performed Errors of commission-required action performed incorrectly Extraneous acts – wrong or unnecessary acts are performed
	System-oriented taxonomy	Human actions classified in terms of the propagation and effects of errors over the course of an event
Taxonomies of information processing	Early Information	Input, mediation and output errors
	Wicken's model of information processing	Information processing characteristics (perceptual, mediational, communication, motor) Sensory processing (receptors), memory (long-term, working), decision and response selection, execution
Taxonomies and models of symbolic processing	SKR	Skill-, Ruled- and Knowledge-based behaviour
	Rasmusen's Multifaceted Taxonomy	Seven sub-systems of analysis: causes of human malfunction, factors affecting performance, situation factors, personnel task, mechanisms of human malfunction, internal human malfunction, external modes of malfunction
	Step-Ladder model	Eight stages of decision-making: activation, observation, identification, interpretation, evaluation, defining the task, procedure and execution
	Murphy diagrams	Graphical analysis of error modes. Illustrate underlying causes associated with cognitive decisión-making tasks
	SHERPA (Systematic Human Error Reduction and Prediction Approach)	SKR external error modes and psychological error mechanisms
	Slips, Lapses, Mistakes and Violations	Slips: actions-not-as-planned Lapses: failure in the execution and/or stage of an action sequence Mistake: intended actions that fail to achieve their intended outcome Violations: intentional deviation of actions from safe operating procedures
	Actions not as planned	Five categories of classification: discrimination failures; program assembly failures; test failures; sub-routine failures; and storage failures
	GEMS (Generic Error Modelling System)	Three basic error types: skill-based slips and lapses, rule-base mistakes and knowledge-based mistakes
	Categorization of Action slips	Slips during the formation of an intention Slips that result from faulty activation of schemas Slips that result from faulty triggering of active schemas
	Seven-step model of Human action	Seven stages of mental activity in the control of action at an interface: perception, interpretation, evaluation, goals, intention, action, specification, execution
	Situation Awareness Error Taxonomy	Three levels of error: L1-fail to perceive or misperception of information; L2-improper comprehension of information; L3-incorrect projection of information of future actions on the system
HRA techniques for quantification of human error	First-generation	Focus on the rules and ability levels of human action. Do not consider the cognitive causes of human error. Examples: THERP, ASEP, HEART, SPAR-H, HRMS, JHEDI, INTENT
	Second-generation	Centered on human behaviour and cognitive causes of human error. Incorporate the context and commission errors in the prediction of human error. Examples: ATHEANA, CREAM, CAHR, MERMOS
	Third-generation	Based on the first-generation methods. Under development. Example: NARA
	Expert judgment	Based on expert opinión to obtain human error probability in a particular scenario. Examples: APJ, PC, SLIM-MAUD

have four main sources of deficiencies:

1. Scarcity of empirical data for model development and validation.
2. Lack of inclusion of human cognition.
3. Lack of common parameters between different methods (they heavily rely on the methodology used).
4. Strong dependence on expert judgment in selecting Performance Shaping Factors (PSFs) and their use to obtain HEP in human reliability analysis.

Additionally, in the case of quantitative techniques, the human error rate is calculated as the combination of different values estimated by subjective expert judgment and by information from accident and incident databases and prescribed probability tables. In other words, a strong operational database or knowledge of human error is required to estimate the probability of human error occurrence. This makes it difficult to apply these methods in most industrial facilities because the complete databases or knowledge required to implement reliability assessment techniques are nonexistent or incomplete (Vanderhaegen, 2001). Similar problems arise with some human error models that need detailed information about accidents or incidents for implementation (Calvo Olivares et al., 2014, 2015).

However, note that although data about accidents or incidents are available, the development of a model that only takes into account that information, limits the scope against potential occurrence of different accidents. According to Leveson (2009), retrospective analysis of adverse events is necessary and is the best way to improve industrial process safety. However, it is limited by the dynamism of systems and organizations (Rasmussen, 1997). Technological innovations can modify certain process conditions or human-machine interface features, increasing the complexity and understanding by operators. Therefore, availability of information about past events, while important, is not sufficient to address potential occurrences of accidents and incidents. Further, because the impact of consequences in the new complex systems can be very meaningful when an accident occurs not only from an economical view, but also from a social perspective, it is not possible to wait until they occur to determine how to prevent their occurrence.

Finally, the little influence of human reliability approaches upon many industries, in particular those focused on managerial and organizational contexts that create latent conditions for failures, is largely due to the problems of system development not being seriously considered. According to Johnson (1999), there exist several problems such as poor methodological support, analyst subjectivity, poor support for error prediction, focus on accidents and not incidents, individual operator/system focus, and difficulty in reaching consensus on the contextual sources of latent failures. Unless these problems are addressed, the theoretical models of cognitive and organizational failure will be of little practical benefit.

The problems outlined above demonstrate the need to develop a technique or methodology that not only is of practical use for

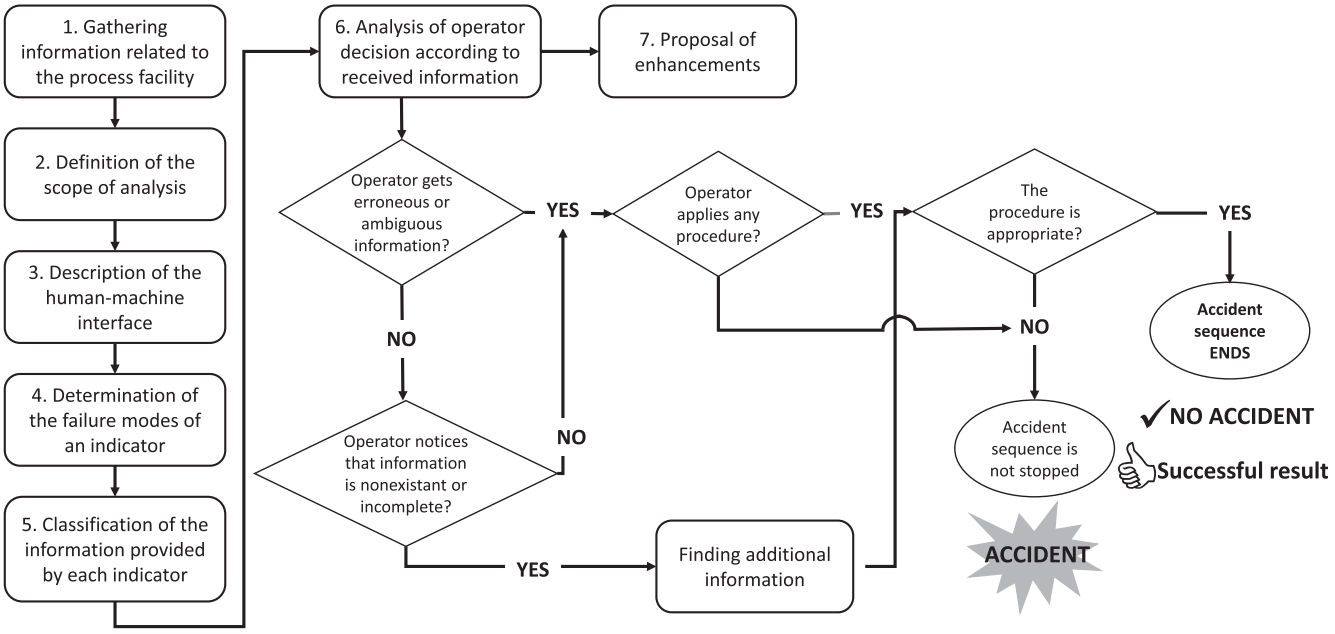

Fig. 2. Flow diagram of the qualitative prospective methodology to assess human error.

industries, but also does not depend exclusively on retrospective information about accidents and incidents, or expert judgment.

The aim of this work is to provide a qualitative prospective methodology that allows predicting potential sequences of accidents before they occur, based on objective engineer elements. The methodology allows identifying the elements from the human-machine interface or procedures that may divert the operator from the accident sequence resolution. It includes two general assessment stages: the first one centred on the system to identify the kind of information provided by the different measurement devices; and the second one centred on the analysis of the operator, evaluating his/her answers according to the type of information received from the process. These operator's decisions based on received data can involve human error, diverting him/her from the accident sequence resolution. The methodology has been developed for new small and medium-scale facilities whose processes are simple, but can also be applied for existing plants.

The proposed methodology aims to be prospective in nature, i.e. it should allow predicting a possible sequence of accident before it occurs.

Etymologically, the word prospective comes from the Latin *prospectus* that means, 'to look forward'. The prospective methodology, as an intellectual discipline, was born in France, initiated by one of its creators Berger in 1957 (Godet, 1998). Essentially, it allows seeing the future and making decisions at present. It does not intend to guess the occurrence of an event, but it looks for significantly reducing uncertainty about its occurrence, showing the actions to be taken in the present.

There exist several techniques of predictive nature (Baber and Stanton, 2002; Center for Chemical Process Safety CCPS, 2004; De Felice et al., 2016; Shorrock and Kirwan, 2002) or of prospective nature (Funk, 2009; Leveson, 2003, 2004), but none of them has these characteristics or proposes a human error analysis based on the type of information that the operator gets from the process.

The implementation of the proposed methodology will contribute to the identification of those parts of the system that require substantial changes in design, operation, and maintenance, in order to avoid human errors. In particular, process and plant design contribute considerably (50–79%) to accidents occurring in chemical process industries (Kidam et al., 2015). The proposed technique may contribute to reducing this percentage by facilitating the identification of the process stages whose design leads to errors by operators and consequent accidents.

It will also allow modifying working procedures, so that the new procedures when implemented, properly contribute to reducing the incidence of human error. Finally, the methodology is a useful tool to train plant operators to avoid deviations produced because of a decision-making based on inappropriate information.

2. Materials and methods (theory/calculation)

2.1. General characteristics of the qualitative prospective methodology

The present work proposes a methodology that tries to answer the following questions:

Which part or elements from the process are critical in terms of safety or risk?
Which are the events that can initiate an incidental or accidental sequence?
Which elements of the human-machine interface or procedures should be observed?
What are their failure modes?
What kind of information do those elements provide?

The answers to these questions will be provided by performing *Steps* 1–5 (see Fig. 2) of the proposed methodology. They allow determining the type of information provided by each element or indicator in an accidental sequence.

Which of these elements, according to the type of information provided, will deviate the operator from the accident sequence and in consequence, from the correct problem solution?

The answer to this question will be provided by performing Step 6 (see Fig. 2). It allows explaining possible human error causes, since according to the information received by the operator, it is the decision he/she is going to made in order to stop an accident sequence. If this information is not correct, decisions taken will not stop the accident sequence.

The general answer to these questions involves two evaluations: The first one centred on the system, analysing the type of information provided by the different plant indicators once the accident has begun, without considering human intervention; and the second one, focused

on the analysis of the operator, assessing his/her response according to the type of information received.

The fundamental premise is that the human-machine interface acts as a 'mediator' between the operator and the events occurring in the plant. However, this mediator does not always provide proper information, and this leads to operator making mistakes.

It is important to clarify that in this first stage of development of the methodology, only those Performance Shaping Factors (PSF) directly linked to its conception, and that reduce the performance of the operator, have been considered. That is, human-machine interface and procedures (which are the elements, whose information the methodology considers that produces the operator's deviation, once an accidental sequence is initiated) in addition to the training and operator experience (see Section 2.2.1). On the other hand, it seeks to propose a simple model, easy to implement in the industrial field. Because of that, only main PSF have been considered. According to Leiden et al. (2001), experience shows that many studies on human error modelling have failed because they consider too many factors that do not directly govern the system performance. As a result, models become too complex, difficult to implement, and unprofitable. Finally, other PSFs such as time available, complexity, workload, stress and stressors, environment, etc. although their importance, its influence will not be analysed in this first stage of the study. Instead they will be probably incorporated in future developments of the quantitative part of the methodology.

2.2. Description of the analysis methodology

The qualitative prospective methodology to assess human error developed by authors involves seven stages, as shown in Fig. 2.

All the methodology stages are described in detail in the following sections.

2.2.1. Gathering information related to the process facility

The first stage involves collecting information related to the general process of the plant. At this stage, a deep understanding of the following points is needed:

- Plant functioning, especially, thermodynamic and hydraulic operations (when applicable), to obtain information about the stages and sequences of the processes performed and to gain indications about the state of the variables that govern them, based on which the operators make decisions.
- Procedures, instructional material, and operational practices because they are the formal and informal guides used by operators. In the last case, personnel interviews are useful to determine ways of performing procedures because in the situation prevailing in the industrial sector, the way of implementing procedures does not always match what is written.
- Operator instruction and training, and training programs (if any), because they provide an idea about how operators perform tasks.
- Current supervision tasks, whether they are appropriate, and whether they are sufficient;
- Plant design, providing details about the human-machine interface, because an improper design can affect operator performance. Piping and instrumentation diagrams (P&ID) diagrams are useful at this stage.

In the case of industrial installations that have been in operation for several years and that have sufficient operative experience, the incident, accident, and shutdowns history, the delays in corrective maintenance orders, etc. can be considered as supporting information, because they provide data about recent problems, difficulties, experiences, and deviations that affected operator performance. It is also useful to consult equipment suppliers to identify early failures or malfunctioning of equipment provided to other industries of the sector.

Also, the changes introduced by technological improvements or innovations will result in changes in the processes or in the human-machine interface. According to (Leveson, 2009) the introduction of a new technology, may cause new potential causal factors. Because of this reason, any technological change should be taken into account in the analysis.

For new installations, even those that are in the design stage, information about accidents and incidents that occurred at similar plants can be collected. However, these data are not determinant for the implementation of the methodology owing to the prospective nature of the methodology and because the development of this methodology does not depend on retrospective information exclusively. This information is a possible element of support because the original premise is the proposal of a methodology to predict a sequence before it occurs. In conclusion, the methodology is independent of the existence of historical information, but if it exists, such information acts as an element of support.

To carry out this stage, an engineer with knowledge about human factors (accredited by specific training in the issue of human reliability, human error and human factors) accompanied by one or more technical experts as required according to the plant size and complexity. The first one brings together the knowledge associated with *human factors, procedures or* HMI, and understanding of operator decision-making. The second ones, provide the technical information about the process.

2.2.2. Definition of the scope of analysis

Based on the data gathered in the first stage, the starting point-initiating event- and the sequence of subsequent events that can lead to an accident must be identified. At this stage it is necessary to determine those processes or sub-processes from which an initiating event can take place and which, therefore, are critical for the complete system (plant). This means that every involved equipment failure or human error associated with such a failure may start accident sequences with severe or significant consequences not only for plant staff, but also for its environment. For example, the methanol or ethanol storage areas of a biofuels facility or the secondary feedwater system in a nuclear power plant. In the first case, the spilling or release of methanol or ethanol, either liquid or gaseous, inside a poorly ventilated area or near ignition sources may lead to an explosion or a fire. In the second example, lack of adequate control of feedwater from the secondary circuit may contribute to the reactor core uncovery.

Two well-known methodologies used for scenario analysis can be implemented for this goal: Event tree and Fault tree analysis.

Event tree analysis is an analysis technique for identifying and evaluating the sequence of events in a potential accident scenario following an initiating event. It uses a graphical structure called event tree that shows multiple outcomes and outcome probabilities. This tool allows analysing complex systems with components continuously operating or in standby mode. In an event tree, the starting point- initiating event- disrupts normal system operation, and that display the subsequent sequences of events involving success and/or failure of its components. The event tree headings are, in general, arranged in chronological order (i.e. in the same order the events are expected to occur) or causal order (i.e. events are rearranged so that the number of omitted branch points is maximized).

Fault tree analysis is a structured approach used to determine the root causes and probability of occurrence of an undesired event in a complex system. It allows to model graphically the possible combinations of malfunction and wrong actions that can cause an undesired event (accident or incident) to occur. The graphical model is organized by the logic of Boolean algebra and its symbols (AND- and OR-gates). The analysis is deductive because it develops the logical paths from the general problem-the single undesired event at the top- to the specific causes-all the possible root causes at the bottom. The advantages of this method are: it can be easily performed and understood, it provides a useful overview of the system, and shows all of the possible causes for a

problem under investigation (Ericson, 2005; Nivolianitou et al., 2004).

Additional information and development and application of these techniques can be found in literature (DeLong, 1970; Ericson, 2005; Federal Aviation Administration, 2000; Larsen, 1974).

It is important to clarify that both techniques are going to be used in order to identify the initiating event and the sequence of subsequent events that can lead to an accident. Quantification of probabilities is not involved in the present study.

Continuing with the examples presented at the beginning, a possible undesired event associated with methanol storage is the increasing of the tank level and its consequent spill. This can create an explosive atmosphere if ignition sources are present in the vicinity. With regard to the secondary feedwater system, an undesired event is the loss of feedwater either by a malfunction of the system pumps (both main and auxiliary) or by the blocking of valves that failed to open or were closed (human error), restricting the movement of the coolant from the auxiliary secondary circuit in case of failure of the main secondary circuit.

2.2.3. Description of the human-machine interface

For every critical sub-process or sequence under analysis, all the elements that are indicators of intervening variables (temperature, pressure, flow, and level) and allow controlling the process, should be identified and described. These elements may be of analogical, digital, or sound type. To ensure that all the involved indicators are taken into account, the order in which they are located can be followed, or the part of the sub-process involved as their sequence is followed can be determined.

Considering an indicator involves not only the sensor located in any part of the process, the transmitter, and the indicator (light, alarm, etc.) in the control room, but also sensors with no transmitters, for which, the operator must check the status of the variables in situ.

In this stage, plant system models such as engineering diagrams or P&ID are useful.

2.2.4. Determination of the failure modes of an indicator

In this stage, the failure modes for all the elements identified in the previous steps are determined by a Failure Modes and Effect Analysis (FMEA). According to literature (Ericson, 2005; Stamatis, 2003), the FMEA is a specific methodology that assesses a system, a design, a process, or service to identify the possible ways in which failures of different system components can occur. For this purpose, analysts develop lists of components with their potential failure modes and try to determine the effects of these modes on the system (Papadopoulus et al., 2004). The following table shows one of the models used for such studies. The table incorporates the column named 'local effect' in order to facilitate failure detection by operator. When a component has more than one failure mode, more rows, as necessary, are added.

In this particular case, the technique is used to identify the modes in which every identified indicator can fail. For example, a pressure switch may fail because of an error of excess or a defect, or may not indicate measurement; a relay can fail because of closed contact, open contact, coil wear, or short circuit.

The aim of this analysis is to generate the necessary data that allow classifying the information provided by every indicator into the following categories: ambiguous, inaccurate, or nonexistent (indicator does not display measurement lectures). FMEA will also allow identification of the failure modes causes, the local effect (detection mode), and the effect that has over the general system.

It is important to emphasize that the analysis made in this stage is useful to initiate information classification. However, there are some examples of industrial reality in which the type of provided information by indicators is not at all related to the failure modes. Additionally, information provided by one or more indicators in a system can be also incomplete, or can be a situation that is not covered by an FMEA. All of these cases will be explained in detail in the following sections.

2.2.5. Classification of the information provided by each indicator

The information provided by each element is classified into four categories:

. Erroneous
. Ambiguous
. Nonexistent
. Incomplete

Categories 1, 2, and 3 arise from FMEA. Incompleteness (category 4) was added because it has been found that in certain accident sequences, for example, in the TMI-2 accident (Kemeny, 1979), if additional elements had been available to check the displayed information and determine the real state of variables under analysis, operative decisions probably would have been different from those taken. When talking about additional elements, reference is made not only to measurement devices, but also to the defined procedures or standards for certain variables.

The four categories will be defined with examples as follows.

2.2.5.1. Erroneous information. Following the meaning of the term, an indicator is said to display erroneous information when it is inaccurate or wrong. This definition involves the following situations:

a. Recorded values are not the actual values because of a failure of the indicator. This fact can be verified by FMEA. Failures can occur because of the constructive features of the measurement and transmission elements, or because of their use under conditions for which they were not constructed. For example, thermocouples are devices to measure temperature; however, if they are used at temperatures higher than 1373 K (Rempe and Knudson, 2014), the accuracy of the readings decreases, and the measured values do not match the actual conditions.
b. Recorded values are not the actual values, without any failure during functioning. These cases cannot be determined through an FMEA, but it is necessary to consider them because they are part of the industrial reality. For example, consider the level gauge in one of the TMI reactor's vapour generators. The pressure transmitter was incorrectly installed, and as a result, it recorded erroneously low values when the generator was steaming (Rempe and Knudson, 2014). Another example is the use of a mass flow meter in a pipe in which normally a liquid is circulated. This device uses liquid density for flow calculation, which, in turn, is calculated based on the temperature. If there is a sudden increase in temperature, the liquid turns into steam, and meter readings will be erroneous because the meter will be still considering liquid density and not steam density.

In both cases, it can be verified that erroneous readings are not due to the inadequate internal functioning of the device.

2.2.5.2. Ambiguous information. The information provided by an indicator is ambiguous when it does not show what is truly happening to the state of the variable or element under control (e.g. valve). The following examples are considered as ambiguous:

a. Sensor goes out of range: Either at the end, or at the beginning of it. In this case, the operator cannot know if the readings of the variable are higher or lower than that indicated by the instrument.
b. When the indicator shows a state or situation that is not the actual state or situation occurring in the process. The following examples correspond to incidents some of them with adverse consequences. These incidents occurred because the operator received ambiguous information.
   b.1 In the nuclear power plant Crystal River unit 3 (Forester et al., 2007), during reactor start up, a pressure transitory of the cooling system occurred. This was followed by an increase in power.

Because of this increase, the pressurizer spray valve opened to control a slight increase in pressure. The spray valve actuator failed, and left valve opened partially. However, the lights indicating valve position showed that it was closed. The pressure of the reactor cooling system started to drop, and as a result, operators failed to identify the cause. Clearly, it can be verified that an ambiguity existed in the case of the light indicator because it did not indicate the actual valve position.

b.2 In this example, the thermometer (because of its localization) did not indicate the operator reactor temperature, but showed the temperature of a nearby pump. This led to an explosion (Kletz, 1998). A glycerine stream entered a reactor and circulated through a heat exchanger that could work to cool as well as to heat the substance. At the beginning of the process, the heat exchanger was used to heat glycerine, and when the temperature reached 388 K, addition of ethylene oxide to the reactor initiated an exothermic chemical reaction. Once the reaction occurred, the heat exchanger was used to cool the product. Fig. 3 shows a simplified diagram of the plant identifying not only the ambiguous information, but also the incomplete information.

The pump that supplied ethylene oxide could not be turned on unless the circulation pump was working; the temperature was over 388 K because ethylene oxide would not react otherwise; or temperature was under 398 K, to avoid the reaction proceeding too quickly. Despite these precautions, an explosion occurred because of the ambiguity of the information received by the process operator. The plant was in operation; ethylene oxide was added, and the reactor pressure increased. The last data indicated that ethylene oxide was not reacting. The operator decided that the temperature reading value was low or that more heat was necessary to initiate the reaction, so he set a configuration and allowed the temperature to increase to 473 K. Pressure continued to rise. Suspecting an error in his theory, he checked the valve position in the reactor base. He found that it was closed, so he decided to open it. Three tons of unreacted ethylene oxide and glycerine went through the heat exchanger (working as a heater) and catalyser, causing a violent and uncontrolled reaction that culminated in reactor explosion and gas escape. The operator noted from the temperature indicator that the temperature had increased; however, the temperature of the reactor content had not increased. The circulation pump was working, but the valve in the suction line was closed, warming up the pump, and this heat affected the temperature sensor because of its proximity to the pump.

In this case, there was clearly an ambiguity without a failure in the measurement device because the operator understood that the sensor displayed the temperature of the reactor when it actually displayed that of the pump. The operator could have turned to the observation of other indicators of temperature throughout the process to gain a better understanding of the situation; however, ambiguous information caused a deviation, making the operator focus only on this information.

c. When different devices are located in an area, they measure the same variable at different points, and adequate identification is lacking. That is, it is not known certainly, if the measurements came from one or other device. For example, during TMI accident, the strip-chart prints from radiation measurement monitors inside the reactor building were ambiguous because operators did not know if the registered data corresponded to one monitor or the other (Rempe and Knudson, 2014).

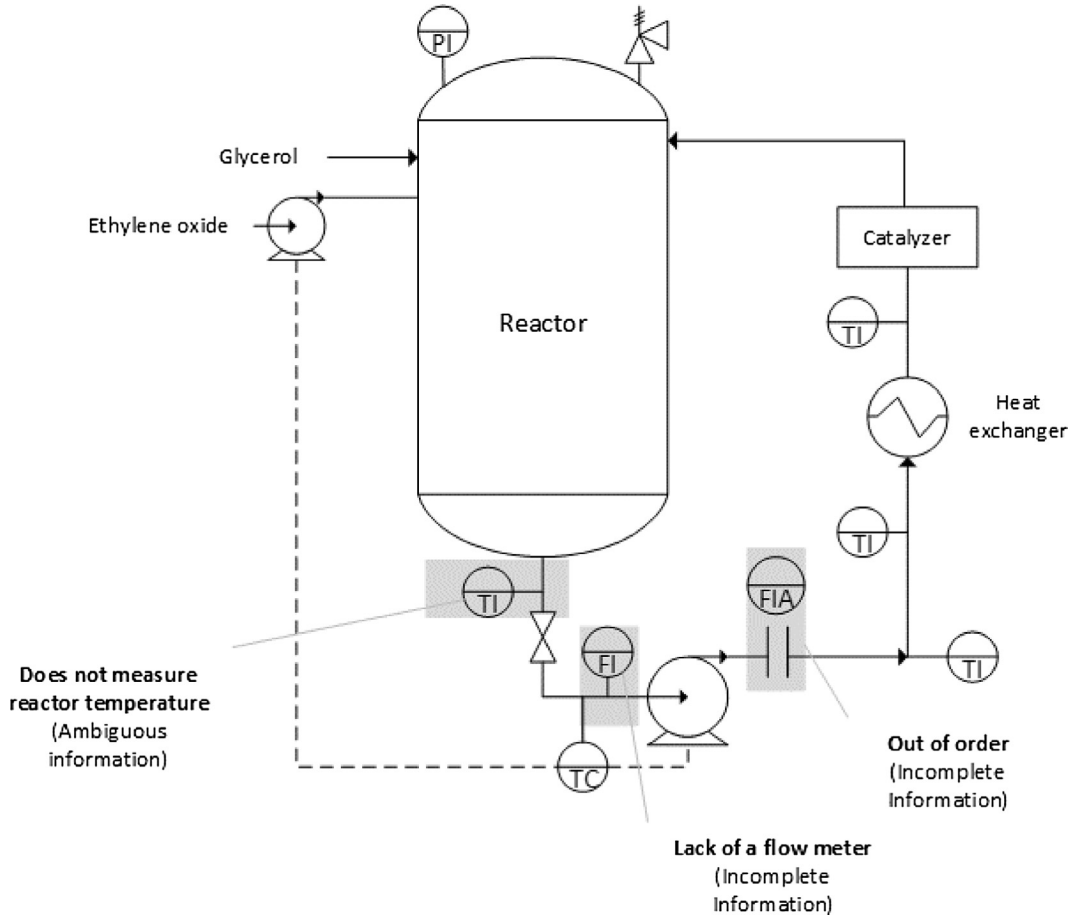

Fig. 3. Process diagram of the chemical plant. (Adapted from Kletz, 1998).

2.2.5.3. Nonexistent information. This occurs when the indicator does not record data either because of a fault (identified by FMEA), or because the element has been disconnected or turned off. The last situation may be as consequence of repairing or maintenance tasks, after which the various devices do not return to their normal or operative position. In other cases, the data storing capacity of the equipment being used may not be adequate for an accidental event because it is not possible to store complete information. For example, consider the accident sequence at TMI: information about system alarms was lost because the printer that recorded information from different indicators was turned off during a certain time. This happened because the printer capacity and memory system could not process large amounts of data.

2.2.5.4. Incomplete information. The indicator provides incomplete information when additional data are not available, for instance, about other process measurement variables, procedures, or instructions from the supervisor that allow defining the state of the system correctly. In other words, it involves not only the lack of contrast information that allow checking the real state of a variable, but also the lack of procedures or instructions indicating what certain conditions or process variables mean, and how to make decisions according to them. Considering again the example of the ethylene oxide process, information was incomplete because the lack of a flow meter in the pump suction tapping did not allow the operator to detect the closed valve and to know the fact that there was no circulation from the reactor to the heat exchanger. Even this knowledge would have warned him that the glycerine had not reached the indicated temperature for the reaction to occur. On the other side, other elements such as the level indicator and the alarm that indicated a low flow were out of operation.

2.2.6. Analysis of operator decision according to received information

This stage involves the analysis of possible decisions that an operator can make based on the received information, taking into account the sub-process or critical task sequences and the initial event determined in previous stages. Therefore, once the sequence has begun, the manner in which it could continue, if the operator makes decisions based on erroneous, ambiguous, or incomplete information, or if there is no information on which the operator can base his/her decisions, is determined.

According to the type of information previously defined, two analyses are possible:

1. The operator receives erroneous or ambiguous information: He/she tries to solve the problem based on the error or the ambiguity:
   - The corresponding procedure according to the information received is implemented. However, because the information is erroneous or ambiguous, the procedure that the operator thinks is correct is inappropriate for the system, and its implementation may result in aggravating the accident sequence or a deviation from its resolution.
   - The operator does not do anything.
2. The operator receives incomplete information or does not receive data:
   - Operator notices the fact: He/she looks for additional information for decision making (previous experience in similar situations or problems, consultations to the supervisor, on manuals and procedures). This information may or may not exist.
     → The appropriate resolution procedure is applied.
     → Inappropriate or incomplete procedure is applied (commission, omission error)
   - Operator does not realize about the event:
     → The corresponding procedure according to the information received is implemented. However, because the information is incomplete or nonexistent, it is understood the procedure that operator thinks is correct, though it is not really appropriate for the system, and its implementation may result in aggravating the accident sequence or a deviation from its resolution.
     → The operator does not do anything.

According to the examples presented in the stage *Classification of the information provided by each indicator*, the following points are noted:

– In the nuclear power plant, owing to the ambiguity, operators did not identify the cause of decrease in pressure.
– In the chemical plant, once the accident sequence had begun, because of the ambiguity, the operator did not realize that the adequate temperature to initiate the reaction had not been reached in the reactor. However, by observing the indicator and the valve position, the operator applied the procedure that he/she believed was appropriate, and opened the afore-mentioned valve. Further, because of incomplete information, the operator did not quickly realize that the valve connecting the reactor and the circulation pump was closed, and that there was no fluid flow from the reactor to the pump. Therefore, the operator did not notice in time that the valve was closed, and in consequence, it remained in the wrong position.

Note that in the presented examples, past events were analysed to define the type of information and its characteristics. However, the technique is prospective in nature, and its aim is to identify which part of a sub-process, task sequence or information can be erroneous, ambiguous, incomplete, or nonexistent, and to assess the possible decisions of the operator based on it, once the accident event is initiated.

The methodology proposes that the cause of human error and the consequent deviation from the resolution of the accident sequence are associated with the type of information that the operator receives. Thus, the commission error occurred, not because the operator decided to apply the procedure that he/she thought correct, but because the information received might not have been appropriate in all cases.

2.2.7. Proposal of enhancements

According to the type of information identified and the possible operator behaviours, modifications that should be implemented are proposed. These involve design, structural, or layout changes; incorporation of new procedures or upgrading of existing ones; incorporation of supervision and improvement of operator training and expertise; or incorporation of training programs that consider the analysed situations as potential accident scenarios.

For the examples analysed in Section 2.2.5, the following improvements may be recommended:

- Perform programmed maintenance of different system devices to avoid failures.
- Check that the system in which devices are installed meets the recommended conditions for their use.
- Supervise installation procedures of measurement devices so that they are installed correctly, following the manufacturer's instructions, and make the corresponding adjustments according to the process.
- Avoid setting the measuring ranges of sensors only for normal operating conditions, and use their operating limits, or install sensors with ranges covering the unanticipated conditions of an accident.
- Ensure that the equipment to process and store information has enough capacity for data backup and proper operation during emergencies.
- Depending on the type of variable being measured, avoid installing the measurement devices at locations close to other devices that may influence it and modify its measurements. In the chemical plant, for instance, the temperature should have been measured in the reactor or as close as possible to it.
- Through corrective maintenance, ensure that all the process control devices work properly.
- In the operator training, include the reading review sequence of the

different devices needed for proper diagnosis of the process state.
- Ensure proper identification of human-machine interface elements, and check, when applicable, the existence of adequate correspondence with respective devices in the control panel.
- In the process, add all the nonexistent elements, whose absence may cause the operator to receive incomplete information. In the chemical plant, the installation of a flow meter was recommended.

2.3. Advantages and disadvantages of the methodology

Next, the advantages and disadvantages of the methodology are detailed.

Advantages:
- Easy to implement
- Since the methodology has been developed for medium- and small-scale installations with simple processes, an engineer trained in human factors is sufficient to carry out the analysis. (The fact of involving a specialist, makes the analysis costly and, in consequence, these types of installations do not perform analysis about human error, human reliability or human factor). However, if the installation, beyond its size, has a high complexity in its processes, it will be necessary to hire a specialist in human factors to perform the analysis.
- Does not depend exclusively on retrospective information. When the methodology is going to be used for new installations, the lack of information is not an impediment for its implementation. If previous data exist, it could be used as support element.
- Allows identifying potential error sequences once the accident event has begun.
- Does not involve expert judgment.
- Is applicable to any technological system, regardless of its complexity and innovation, because it relies on the analysis of information provided by different elements of the human-machine interface; that is, the methodology can be extended to other industrial domains.

Disadvantages:
- As the number of elements to be evaluated increases, the analysis may require a considerable amount of time.
- Does not address completely the dynamic nature of actual operations. Many processes may be happening simultaneously in the plant and indicators may change continuously. This is not reflected by the methodology.

3. Application of the proposed methodology

The application of the proposed methodology to a medium-capacity biodiesel plant is discussed in the following sections. The plant has an automated system consisting of sensors, controllers, and actuators for measuring and controlling the variables of interest.

3.1. Gathering information related to the process facility

3.1.1. Operative performance

The installation produces biodiesel by transesterification of vegetable oil. Methanol and sodium hydroxide are used as raw materials. The operation equipment consists of batch reactors, pumps, centrifuges, and distillation columns. Additional equipment includes decanters, heaters, and storing tanks (Van Gerpen et al., 2004).

Biodiesel is obtained by a homogeneous catalysis reaction by using methanol as the alcohol and a basic catalyst (sodium hydroxide). The alcohol and catalyst are mixed in advance and then combined with the oil in the reactor. The mixture is stirred for approximately 1 h at 333 K in a stirred tank reactor (CSTR) in order to achieve a product stream composition identical to the composition inside the reactor. Once the chemical reaction occurs, methyl-esters and glycerine are obtained. They are separated through a decanter. The methyl-esters are carried on to the neutralization step in which the residual catalyst is neutralized by the addition of an acid, and the soap that may have formed during the reaction is separated. The soap reacts with the acid to form soluble salts and free fatty acids. Thereafter, by washing with water, all traces of residual catalyst, soap, salts, free methanol, and glycerine are removed. Methanol is removed earlier through vacuum distillation. After the washing step, residual water is removed from biodiesel by drying. The glycerine stream only contains 50% glycerine, excess methanol, and most of the catalyst and soap. Glycerine is refined by adding acid to separate the soaps into salts and free fatty acids. Then, methanol is removed by evaporation.

The methanol obtained from methyl-esters and glycerine streams tends to collect all the water entering the process, and this water must be removed in a distillation column before the methanol re-enters the process (Van Gerpen, 2005).

3.1.2. Control devices

For continuous processes, control variables involve temperature, pressure, level, and flow.

The temperature at a specific point is measured using a thermocouple. It is an electrical device, consisting of two metal conductors bonded by welding or torsion. When this junction is heated, a voltage in the order of millivolts is set between the wires. This voltage is proportional to the junction temperature. The metals used in the junction and their different combinations are appropriate for the different temperature ranges that characterize these devices. A thermocouple is usually enclosed in a pod in order to obtain a correct reading. Thermocouples may be used to monitor and to control the process. When process temperature is to be measured, one end of the thermocouple should be in contact with the process (hot junction) and the other with a constant temperature (cold or reference junction). A transmitter is needed to convert the voltage to a standard 4–20 mA current (CNSC Technical Training Group, 2003; Van Gerpen et al., 2004).

Pressure is measured by means of strain gauges. A strain gauge is a device that measures the external force (pressure) applied to a thin wire, which is generally in the form of a mesh. A pressure change causes a change in the resistance because of the distortion of the wire; thus, the pressure value is obtained by measuring the change in resistance of the metal mesh. This change in resistance is used as the resistance variable in a bridge circuit that provides an electrical signal for displaying the pressure value (CNSC Technical Training Group, 2003; US Department of Energy—US DOE, n.d.; Van Gerpen et al., 2004). Such sensors have a temperature-compensating meter to compensate the heat produced by the current flowing through the wire.

The level measure is obtained using differential pressure gauges that measure the difference in pressure between two pressure connectors located in a container. Level measures depend on liquid density, and hence, any change in density can affect readings. Measurement and control of the level in a vessel generally require two points of reference within the vessel. Level measurements can be converted to electrical signals and used for control.

Flow is measured using differential pressure flow meters that can be used for monitoring and control. These elements measure the difference in pressure between the two sides of a restriction in a confined fluid stream. This restriction can be imposed by different kind of devices such as Venturi or Pitot tubes, orifice plates or flow nozzles (CNSC Technical Training Group, 2003; US Department of Energy—US DOE, n.d.; Van Gerpen et al., 2004). In such systems, the flow reading is a signal proportional to the differential pressure; however, this relationship is not linear: the differential pressure increases according to the square of the flow, or in other words, the flow is proportional to the square root of the differential pressure. To convert the signal of the flow transmitter, the square root must be extracted by an electronic (or pneumatic) device to obtain a linear flow signal in the 4–20 mA range.

3.1.3. Procedures

- Lack of operative procedures or standard instructions, mainly in medium- and small-scale installations. This leads to the use of inappropriate mixtures to carry out chemical reactions or to the erroneous setting of control variables as temperature and pressure.
- Scarcity or lack of maintenance procedures for outsourced personnel to warn the personnel about existing risks at the site of work (Calvo Olivares et al., 2014).

3.1.4. Operator training and qualification

- Lack of training and understanding of the process and its possible deviations
- Inadequate supervision
- Lack of awareness about the health risks involved in handling of certain chemicals, such as methanol, sodium hydroxide, and sulphuric acid
- Performance of tasks without personnel protection equipment

3.2. Definition of the scope of analysis

According to failure tree analysis, an initiating event is an increase of the level in the methanol tank, in the methanol storage area of the plant. The analysis may focus on this initiating event to determine a possible sequence of adverse events that leads to an accident.

The analysis will be applied to a critical sub-process: methanol storage. The importance of this sub-process lies in the fact that this chemical substance may cause fires owing to its flammability and may seriously affects the health of the operators (Alliance Consulting International, 2008).

3.3. Description of the human-machine interface

A simplified schema of the storing methanol area was considered for implementing the methodology (see Fig. 4).

The storage tank is filled by a one-step centrifugal pump and has a level gauge that acts also as a controller. When the tank level reaches the necessary level for the next step of the process (transesterification reaction), as detected by the level control, a signal is sent to the pump to stop it automatically. If the pump does not stop functioning, the operator can notice a high level in the tank in situ through the visual level indicator and can stop the pump by using the control panel button to switch it off or manually. If the pump does not stop, the level may increase until it reaches the orifice through which methanol reaches a buried tank that contains it safely via a pipe. A block valve is located on the pipe, located between the tanks. The position of this valve can be checked in the control panel through a light indicator. The block valve can be opened or closed manually. If the orifice is clogged or in the event of an accidental closing of the block valve, methanol does not reach the buried tank, and the level in the storing tank will continue to rise until it reaches the venting, leading to an unwanted spill.

From the above description, the following human-machine interface elements can be identified:

A. Level controller
B. Actuator for automatic pump shutdown
C. Visual level indicator
D. Block valve light indicator (incorporated into the valve command system)

3.4. Determination of the failure modes of an indicator

For the elements identified in the previous step, FMEA was conducted using the model introduced in Table 2. The results of the analysis are presented in Table 3. Different failure modes were obtained from various references (CNSC Technical Training Group, 2003; Panchangam and Naikan, 2013; U.S. Department of Energy, 1992a, 1992b).

3.5. Classification of the information provided by each indicator

A. *Level Controller:*
   1 Erroneous: Not applicable.
   2 Ambiguous: When the sensor goes out of scale, and readings are inaccurate, it is not possible to know certainly if the level is higher (or lower) than the reading.
   3 There is no information: When there is no element actuation because of problems in the electronic circuits, the level readings are not registered, and therefore, the stop signal (or start) may not be sent to the pump.
   4 Incomplete: Not applicable.
B. *Actuator for automatic pump shutdown*: It is not possible to implement information classification in this case, because it is an actuator that stops functioning correctly when some of the analysed failure modes occur, but it does not display the information to the operator. The operator will only realize that the pump has not stopped (and therefore, failed) upon checking the level in the tank.
C. *Visual level indicator*
   1 Erroneous: Not applicable.
   2 Ambiguous: Not applicable.
   3 There is no information: Not applicable.
   4 Incomplete: Nonexistence of an alarm in the control room that alerts the operator if the tank level has reached the value established as safe, in order to avoid spills. Another alternative could be using a differential pressure transmitter that allows measuring and verifying the level in the control room.
D. *Block valve light indicator*
   1 Erroneous: Not applicable.
   2 Ambiguous: If the valve is stuck in the closed position, and the light indicator in the control room is off because of a failure (for example, it is burned out) the information will be ambiguous for the operator because according to the indicator, the valve is opened when it is actually closed.
   3 There is no information: Not applicable.
   4 Incomplete: Lack of a flow meter downstream the valve that allows verifying if methanol is circulating to the containment vessel.

3.6. Analysis of operator decision according to received information

For the actual analysis, a possible scene is proposed according to the gathered information.

In the second stage, it was proposed that an initial event of an incident sequence could be an increase in the methanol tank level that if uncontrolled, could end in a spill.

Thereafter, the possible operational decisions based on the type of information provided by the interface elements were studied. Furthermore, a series of unfavourable, but likely assumptions was made.

First, the block valve that allowed circulation to the containment tank was assumed to be left closed after a maintenance task to the containment vessel to avoid leakages. In such installations, according to the analysis made in the first stage, supervision tasks are limited or virtually nil, and most of the maintenance tasks are performed by outsourced personnel. Hence, it might be possible that the valves were not set into their normal position, that is, open position.

Initially, the necessary quantity of methanol is transferred to the storage tank, and this methanol is to be then transferred to the mixing reactor, in which the methoxide solution is prepared for oil transesterification. According to the analysis of information, the level controller may fail, or the connection between the controller and the pump that prevents the pump from stopping may fail. Further, the pump may

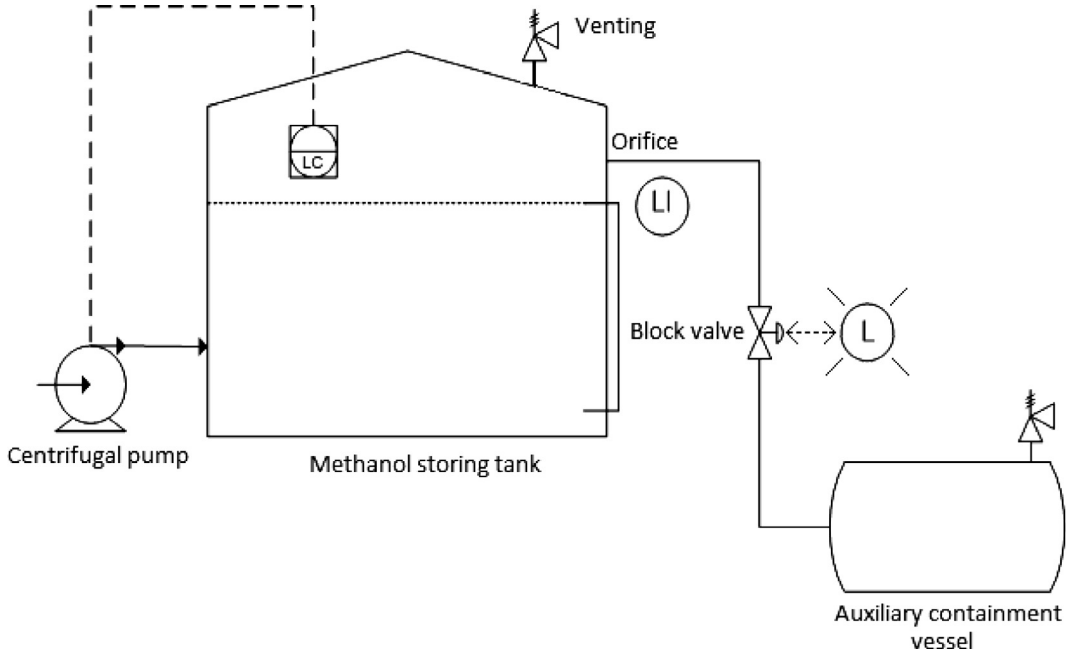

Fig. 4. Simplified scheme of the methanol storage sub-process.

Table 2
Model list used for FMEA.

Item	Component	Function	Failure Mode	Failure Cause	Local Effect (Detection Mode)	Effect on the system

undergo a failure to stop; that is, the pump receives the order to stop, but it does not stop. In either situation, the consequence will be an increase in the level of the tank.

Operator analysis No. 1:

When the tank level increases, the visual level indicator is analysed. In stage five, it was found that the information provided by this element is incomplete. In this case, two possibilities exist:

1. *The operator notices the situation*:
   →From the visual level indicator, the operator detects that the level is increasing and applies the corresponding procedure to stop the pump manually. Result: The incidental sequence is stopped, and there is no spill.
   → From the visual level indicator, the operator detects that the level is increasing and applies an inappropriate or incomplete procedure and the pump does not stop working. Result: The level continues to increase over the reference level.
2. *The operator does not notice the situation*
3. Owing to lack of attention, or because the operator is performing another activity, he/she does not observe the visual level indicator and does not stop the pump. Consequently, the level inside the tank continues to rise. In this case, the incompleteness of the information (nonexistence of an alarm in situ or in the control room that warns the operator about the increase in level) diverts the operator from resolving the problem. Result: The level continues to increase over the reference level.

The methanol level continues to increase until it reaches the connection orifice with the pipe that allows it to flow the containment vessel.

Operator analysis No. 2:

The analysis of the visual level indicator continues.

1. *The operator notices the fact:*
   1.1. In a later visual checking of the level, the operator notices that the actual level is over the reference level, and stops the pump manually. Result: The incident sequence is stopped, and there is no spill.
   1.2. In a later visual checking of the level, the operator notices that the actual level is over the reference level, but as the operator knows that the methanol will be transferred to the containment tank, he/she may decide to not stop the pump. However, as an immediate step, the operator should check the block valve light indicator. Result: The incident sequence does not stop, and the tank level continues to increase.
2. *The operator does not notice the situation*
3. The operator does nothing. Result: The incident sequence does not stop, and the tank level continues to rise.

Operator analysis No. 3:

Next, the block valve light indicator is analysed. In a previous study, it was found that the type of information provided by this indicator was ambiguous (in the control room, the indicator displays an opened valve when the valve was actually closed because of a failure or human error) and incomplete (no flow meter was available downstream to verify methanol circulation through the pipe to the containment tank).

If the information is ambiguous, the operator may take the following actions:

1. Apply the procedure that he/she understands is appropriate according to the received information.
2. Do nothing because the light indicator shows that the valve is opened.

In either case, methanol will spill.

Additionally, the information is incomplete. The operator may take the following actions:

1. *The operator notices the fact:*
   →The operator can look for additional monitoring data, for example, regarding the valve in situ and checking if it is opened or closed. If the operator notices that the valve is closed, he/she opens it, or shuts the pump to stop the flow of methanol. Result: The methanol flows into the containment vessel, or the flow of methanol

Table 3
Failure modes and effects analysis for the biodiesel plant (CNSC Technical Training Group, 2003; Panchangam and Naikan, 2013; U.S. Department of Energy, 1992a, 1992b).

Item	Component	Function	Failure Mode	Failure Cause	Local Effect (Detection Mode)	Effect on the system
A	Level controller	Controlling differences in level and sending a signal to turn the pump on or off	The sensor goes to the lower/higher values of the scale	Malfunctioning of electronic circuits	Inaccurate readings. The controller stops the pump before/after corresponding signal	The pump does not turn on/off or does not stop
			No action. Breaking		No readings, no signal sending	
B	Actuator for automatic pump shutdown	Stopping methanol circulation to the storage tank	The pump continues to drive methanol after receiving the stop signal	Failure in the connection with the level indicator Failure to stop the pump Failure in manual stopping of the pump (human error)	The level of the tank continues to rise	Loss of control of methanol tank level
C	Visual level indicator	Allowing the visualization of methanol level in the tank	Not applicable	Not applicable	Not applicable	Not applicable
D	Block valve light indicator (incorporated into the valve command system)	Enabling the verification or checking of opening or closing valve	Failure in the command to close the valve (stuck in the open position)	Spring damaged; too much friction between the stem and its seals, or between the gate and the seat. Presence of foreign elements in the valve cavity	No effect	Methanol spill. Generation of an ignition source
			Failure in the command to open the valve (stuck in the closed position)	Losses in the control line; too much friction between the stem and its seals, or between the gate and the seat. Presence of foreign elements in the valve cavity Corrosion or erosion or both of the gate or valve seat.	The light indicator shows the order of opening, but the valve is stuck in the close position (there is no methanol circulation to the containment vessel)	
			Leaks/ Internal losses	–	–	
			Leaks/External losses	Misalignment between the gate and the valve seat	Fluid losses at the location of the valve	

to the tank is stopped, and there is no spill.
→ The operator can look for additional monitoring data but applies an inappropriate or incomplete procedure. The pump does not stop working and the valve is not opened. Result: there is a spill.

2. *The operator does not notice the situation:* Owing to incompleteness (no additional information is available for decision-making); any procedure may be applied. Result: With the pump functioning, transferring methanol to the tank, and the block valve closed, the level in the tank increases, causing a spill in the facility.

A summary of operator decisions according to received information is shown in Table 4.

4. Results of the application of the methodology

4.1. Potential accident sequences according to operator's decision

Based on the study of operator's decisions, 18 potential decision sequences were identified:

1. Level of the tank increases → Operator notices the situation → Applies correct procedure → **No methanol spill.**
2. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies correct procedure → **No methanol spill.**
3. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies incorrect procedure (does not turn the pump off) → Checking of the block valve light indicator → Operator applies the procedure he/she understands is appropriate → Methanol spill.
4. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies incorrect procedure (does not turn the pump off) → Checking of the block valve light indicator → Operator does nothing → Methanol spill.
5. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies correct procedure → **No methanol spill.**
6. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies an incorrect procedure → Checking of the block valve light indicator → Operator applies the procedure he/she understands is appropriate → Methanol spill.
7. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies an incorrect procedure → Checking of the block valve light indicator → Operator does nothing → Methanol spill.
8. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator does not notice the situation → Operator does nothing → Checking of the block valve light indicator → Operator applies the procedure he/she understands is appropriate → Methanol spill.
9. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator does not notice the situation → Operator does nothing → Checking of the block valve light indicator → Operator does nothing → Methanol spill.
10. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies incorrect

Table 4
Analysis of operator decisions according to received information. Methanol storage area in a biodiesel plant.

Event	Element	Type of information	Potential operator decision		Result
The level of the tank increases	Visual level Indicator	*Incomplete* (lack of an alarm in the control room)	1. Operator notices the situation	Look for additional information: he/she checks visual level indicator. He/She applies corresponding procedure to stop the pump manually	The accidental sequence is stopped. There is no spill
				Look for additional information: he/she checks visual level indicator. He/She applies an incorrect procedure	**The level inside the tank continues to rise**
			2. Operator does not notice the situation	The operator does nothing	**The level inside the tank continues to rise**
The level of the tank reaches the connection orifice	Visual level Indicator	*Incomplete* (lack of an alarm in the control room)	1. Operator notices the situation	– Look for additional information: he/she checks visual level indicator. He/She applies corresponding procedure, the pump stops	The accidental sequence is stopped. There is no spill
				–The operator does not turn the pump off because he/she understand that there is a containment tank for metanol. Next step: operator should check the block valve light indicator	**The level inside the tank continues to rise**
			2. Operator does not notice the situation	The operator does nothing	The level inside the tank continues to rise
Checking of the block valve light indicator	Block valve light indicator	*Ambiguous* (in the control room, the indicator displays an opened valve when the valve was actually closed because of a failure or human error)	1. Operator applies the procedure he/she understands is appropriate according to the received information		**METHANOL SPILL**
			2. The operator does nothing (because the light indicator shows that the valve is opened)		
		Incomplete (no flow check is available)	1. Operator notices the situation	– Look for additional information: visual inspection of the valve. He/she checks the valve is closed and open it and/or turn the pump off	Methanol flows into the containment vessel, or the flow of methanol to the tank is stopped. There is no spill
				– Look for additional information but apply an incorrect procedure	**METHANOL SPILL**
			2. Operator does not notice the situation	The operator does nothing	**METHANOL SPILL**

procedure (does not turn the pump off) → Checking of the block valve light indicator → Operator notices the situation → Applies the correct procedure → **No methanol spill.**

11. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies incorrect procedure (does not turn the pump off) → Checking of the block valve light indicator → Operator notices the situation → Applies an incorrect procedure → Methanol spill.
12. Level of the tank increases → Operator notices the situation → Applies an incorrect procedure → Level of the tank reaches the orifice → Operator notices the situation → Applies incorrect procedure (does not turn the pump off) → Checking of the block valve light indicator → Operator does not notice the situation → Operator does nothing → Methanol spill.
13. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies an incorrect procedure → Checking of the block valve light indicator → Operator notices the situation → Applies the correct procedure → **No methanol spill.**
14. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies an incorrect procedure → Checking of the block valve light indicator → Operator notices the situation → Applies an incorrect procedure → Methanol spill.
15. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator notices the situation → Applies an incorrect procedure → Checking of the block valve light indicator → Operator does not notice the situation → Operator does nothing → Methanol spill.
16. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator does not notice the situation → Operator does nothing → Checking of the block valve light indicator → Operator notices the situation → Applies the correct procedure → **No methanol spill.**
17. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator does not notice the situation → Operator does nothing → Checking of the block valve light indicator → Operator notices the situation → Applies an incorrect procedure → Methanol spill.
18. Level of the tank increases → Operator does not notice the situation → Operator does nothing → Level of the tank reaches the orifice → Operator does not notice the situation → Operator does nothing → Checking of the block valve light indicator → Operator does not notice the situation → Operator does nothing → Methanol spill.

Six of these eighteen sequences are successful, and there is no methanol spill, while the other twelve may lead to a methanol spill. In six of the potential failure sequences, the incompleteness of the information provided by the indicators causes the operator to deviate from making a decision to resolve the incident. In the other six failure sequences, the incompleteness and ambiguity of the information provided by the indicator has a similar effect.

If the area where the spill occurs is not properly ventilated or if there are ignition sources nearby, the spill may lead to an explosion and fire with serious consequences for the personnel, installations, and surroundings.

The identification of potential sequences also allows explaining the causes of human error in each case and helps take decisions to make the necessary changes to avoid such error. According to the American Institute of Chemical Engineers (2004), in critical or emergency situations, it is necessary to manage all the aspects that play a great role in human performance under stress; for instance, it is necessary tooptimize aspects of control panel design as 'grouping of information' and 'overview of critical parameters' in order to avoid cognitive tunnel vision. The analysis of information provided by different measurement devices and the study of the possible deviations of the operator in making a decision enables the identification of the shortcomings in the human-machine interface elements, and thus, allows us to propose an optimization of their current configuration.

4.2. Proposal of enhancements

In order to avoid the incident sequences previously described, the following enhancements are proposed:

- Incorporate an alarm to indicate that the level in the tank is higher than the desired level (check or reference point).
- Implement the concept of redundancy by placing a second controller to stop the pump in case of failure of the first controller.
- If the time interval between the increase in the level beyond the desired level, and the moment at which the level reaches the orifice is known, an operator round can be scheduled in that time interval.
- Place a flow meter downstream the block valve to detect any flow.
- Instruct the operator that if a level increment is detected, the safest option is to stop the pump, regardless of the presence of the containment tank. Instructions should be documented in a procedure and incorporated into operator training.
- Incorporate supervision tasks in order to ensure that once the maintenance tasks are concluded, all instruments and equipment are returned to their normal or functioning positions.
- Eliminate all ignition sources near methanol storage areas, and ensure proper ventilation of the storage area.

5. Discussion

The methodology was implemented for a biodiesel plant, considering a possible initiating event in the methanol storage area. It has served to give answer all the questions raised at ection 2.1 of the article:

– It identifies all the elements of the human-machine interface and procedures that, according to information provided may affect operator's decisions.
– It allows finding the potential accidental sequences based on possible operator decisions: eighteen potential accident sequences were found. Twelve of these sequences would have culminated in a methanol spill accident.
– It allows verifying the way in which the type of information received by the operator can influence his/her decision and lead him/her to make a human error. For example, owing to an ambiguity, the operator believes that the valve is opened, when it is actually closed, and he/she does nothing to stop methanol circulation.

The proposed methodology uses an engineer complementary tool, FMEA, to identify those elements of the system that may not provide data or may provide erroneous or ambiguous information. FMEA is a broadly developed technique and is used in the industrial field. According to the present work, FMEA analysis allows determining the kind of information provided by the different indicators in the methanol storage area of a biodiesel plant.

The last step of the methodology focuses on a series of recommendations based on the analysis results, that is, the different accident sequences; the objective of the recommendations is to avoid potential occurrences. These recommendations can involve design changes, modifications of the operation and maintenance procedures, operator training, improvement or adding of supervisory tasks, etc. The

basic idea is to modify or improve all the elements in the process that can cause the operator to deviate from resolving the accident sequence.

It is important to highlight that proposed recommendations are engineering solutions to the problem and that positively improve the situation of the plant. They are an 'intermediate' solution and feasible to start solving the problem. They may be perfectible or susceptible of improvement but are clearly a step in improving the installation situation. According to the complexity and involved risks of the installation, later analysis related to Human Factors may be required (e.g. study of alarm philosophy, common cause failures, the convenience of using digital or analogue instruments, the kind of supervision and verification tasks, etc.). A Human Factors person should be involved in this analysis to ensure adequate consideration of Human Factors aspects of the potential accident sequences, and to ensure that any improvement recommendations developed do not create new/hidden human error possibilities.

6. Conclusions

This paper presents a qualitative prospective methodology for analysing human error. Incorporating the concept of prospective does not mean 'divination' of the occurrence of an event, but rather looks for reducing the uncertainty about its occurrence. In this sense, the proposed analysis technique allows identifying possible accident scenarios that can arise as a result of decision-making based on erroneous, ambiguous, incomplete, or nonexistent information. This classification is not based on expert judgment, but on the study of the different configurations and designs of human-machine interfaces in a plant. It is important to emphasize that retrospective information can be a supporting element to the proposed accident analysis methodology. However, it does not determine its implementation.

This new approach tries to provide answers to the problems raised at the beginning by eliminating the subjectivity of the analyst, supporting the prediction of accidents, and focusing on the human-system interaction in an integrated manner. It is also a practically applicable methodology for the industry: it provides an answer for those plants or installations that have no implemented human reliability approaches, since specific and costly resources and techniques are required. At this first stage, it has been designed for small or medium-scale facilities, whose processes involved are simple, such as biodiesel production.

The technique was applied to an area at a biodiesel plant. However, its use can be extended to other installations or part of them with automated human-machine interfaces, provided that levels of complexity are similar to those studied. For installations or plants of higher complexity (e.g. chemical and petrochemical industries, refineries, and nuclear power plants) the adequacy of the methodology should be further studied.

In principle, the methodology proposes to analyse all elements identified in an accidental sequence. However, when the number of elements is such as to hinder or make the analysis more complex, a way of choosing those elements that, because of the information provided, causes human errors involving a high risk to the system, must be determined. Future work is necessary in order to determine the way of doing this analysis and improve the methodology.

Finally, the methodology, in this first development, utilizes some traditional accident analysis techniques that rely on a chain-of-event paradigm of causation (Qureshi, 2007), and deal with systems and the environment as a static design and unchanging structure (Leveson et al., 2003). Further work is needed to improve the proposed methodology in this sense.

Formatting of funding sources

This work was supported in part by a PhD scholarship and a post-doctoral fellowship awarded by CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas), and by funding from a project of SeCTyP (Secretaría de Ciencia, Tecnología y Posgrado, National University of Cuyo, Argentina).

References

Alliance Consulting International, 2008. Methanol Safe Handling Manual. Methanol Institute, Virginia, USA.

Altabbakh, H., AlKazimi, M.A., Murray, S., Grantham, K., 2014. STAMP – Holistic system safety approach or just another risk model? J. Loss Prev. Process Ind. 32, 109–119. http://dx.doi.org/10.1016/j.jlp.2014.07.010.

American Institute of Chemical Engineers (Ed.), 2004. Guidelines for Preventing Human Error in Process Safety. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, NY.

Amyotte, P., Khan, F., 2005. Development of a Human Error Probability Index for Offshore Platform Evacuations. Petroleum Research Atlantic Canada.

Baber, C., Stanton, N.A., 2002. Task analysis for error identification: theory, method and validation. Theor. Issues Ergon. Sci. 3, 212–227.

Baziuk, P., Núñez Mc Leod, J., Calvo Olivares, R., Rivera, S., 2016. Modeling Human Reliability: The Underlying Cognitive Abilities. International Association of Engineering; Lecture Notes in Engineering and Computer Science, London, UK, II, pp. 790–795.

Bell, J., Holroyd, J., 2009. Review of Human Reliability Assessment Methods. Health and Safety Laboratory, HSE Books Retrieved from. <http://www.hse.gov.uk/research/rrpdf/rr679.pdf>.

Broadbent, D.E., 1998. Perception and Communications. Springer, London.

Calvo Olivares, R.D., Rivera, S.S., Núñez Mc Leod, J.E., 2014. Database for accidents and incidents in the biodiesel industry. J. Loss Prev. Process Ind. 29, 245–261. http://dx.doi.org/10.1016/j.jlp.2014.03.010.

Calvo Olivares, R.D., Rivera, S.S., Núñez Mc Leod, J.E., 2015. Database for accidents and incidents in the fuel ethanol industry. J. Loss Prev. Process Ind. 38, 276–297. http://dx.doi.org/10.1016/j.jlp.2015.10.008.

Center for Chemical Process Safety CCPS, 2004. Guidelines for Preventing Human Error in Process Safety (First). Wiley-Aiche, United States.

CNSC Technical Training Group, 2003. Basic Instrumentation Measuring Devices and Basic PID Control (Science and Reactor Fundamentals Instrumentation & Control).

Cooper, S., Ramey-Smith, A.M., Wreathall, J., Parry, G.W., Bley, D., Luckas, W.J., Ellipsis Barriere, M.T., 1996. A Technique for Human Event Analysis (ATHEANA) – Technical Basis and Methodological Description (No. NUREG/CR-6350.). U.S. Nuclear Regulatory Commission, Brookhaven National Laboratory.

De Felice, F., Petrillo, A., Zomparelli, F., 2016. A hybrid model for human error probability analysis. IFAC-PapersOnLine 49 (12), 1673–1678. http://dx.doi.org/10.1016/j.ifacol.2016.07.821.

DeLong, T., 1970. A Fault Tree Manual. Research Report. (Research Report No. AD739001). Industrial Engineering Department of Texas A&M University, Texas, USA.

Embrey, D.E., 1983. The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal (No. NUREG/CR-2986). Brookhaven National Laboratory.

Embrey, D.E., 1986. SHERPA – a systematic human error reduction and prediction approach. In: Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems. American Nuclear Society (ANS), La Grange Park, Ill, USA, pp. 184–193.

Endsley, M., 1988. Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 32, no. 2, pp. 97–101.

Ericson, C.A., 2005. Hazard Analysis Techniques for System Safety. Wiley-Interscience, Hoboken, NJ.

Federal Aviation Administration, 2000. Analysis Techniques. In FAA System Safety Handbook (Chapter 9).

Foord, A.G., Gulland, W.G., 2006. Can technology eliminate human error? Process Saf. Environ. Prot. 84 (3), 171–173. http://dx.doi.org/10.1205/psep.05208.

Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., Lois, E., 2007. ATHEANA User's Guide. Final Report. Washington, DC 20555–0001: U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research.

Funk, K., 2009. A methodology and tools for the prospective identification of nextgen human factor issues. In: Proceedings of the 15th International Symposium on Aviation Psychology, pp. 27–30.

Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., 2005. The SPAR-H Human Reliability Analysis Method (No. NUREG/CR-6883 INL/EXT-05-00509). Idaho National Laboratory.

Gertman, D.I., Blackman, H.S., Haney, L.N., Seidler, K.S., Hahn, H.A., 1992. INTENT: a method for estimating human error probabilities for decision-based errors. Reliab. Eng. Syst. Saf. 35 (2), 127–136. http://dx.doi.org/10.1016/0951-8320(92)90032-G.

Godet, M., 1998. De La Anticipación a La Acción. Manual De Prospectiva Estratégica.

Griffith, C.D., Mahadevan, S., 2011. Inclusion of fatigue effects in human reliability analysis. Reliab. Eng. Syst. Saf. 96 (11), 1437–1447. http://dx.doi.org/10.1016/j.ress.2011.06.005.

Hollnagel, E., 1993. Human Reliability Analysis: Context and Control. Academic Press Retrieved from. <https://books.google.com.ar/books?id=jGtRAAAAMAAJ>.

Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method. Elsevier Science Ltd, Oxford, UK.

Hollnagel, E., 2005. Human Reliability Assessment in Context.

Isaac, A., Shorrock, S.T., Kennedy, R., Kirwan, B., Andersen, H., Bove, T., 2002. Technical Review of Human Performance Models and Taxonomies of Human Error in ATM

(HERA). European Organization for the Safety of Air Navigation.
Johnson, C., 1999. Why human error modeling has failed to help systems development. Interact. Comput. 11 (5), 517–524. http://dx.doi.org/10.1016/S0953-5438(98)00041-1.
Kemeny, J.G., 1979. Final Report of the President's Commission on the Accident at Three Mile Island. Washington, D.C., USA.
Kim, T., Nazir, S., Øvergård, K.I., 2016. A STAMP-based causal analysis of the Korean Sewol ferry accident. Saf. Sci. 83, 93–101. http://dx.doi.org/10.1016/j.ssci.2015.11.014.
Kirwan, B., 1996. The validation of three human reliability quantification techniques — THERP, HEART and JHEDI: Part 1 — technique descriptions and validation issues. Appl. Ergon. 27 (6), 359–373. http://dx.doi.org/10.1016/S0003-6870(96)00044-0.
Kirwan, B., 1997. The development of a nuclear chemical plant human reliability management approach: HRMS and JHEDI. Reliab. Eng. Syst. Saf. 56 (2), 107–133. http://dx.doi.org/10.1016/S0951-8320(97)00006-9.
Kirwan, B., 1994. A Guide to Practical Human Reliability Assessment. Taylor & Francis, London.
Kletz, T.A., 1998. What Went Wrong? Case Histories of Process Plant Disasters, fourth ed. Gulf Pub, Houston, Tex.
Larsen, W.F., 1974. Fault Tree Analysis (Technical Report No. 4556). U. S. Army Picatinny Arsenal, Dover, New Jersey.
Leiden, K., Ronald Laughery, K., Keller, J., French, J., Warwick, W., Wood, S.D., 2001. A Review of Human Performance Models for the Prediction of Human Error. Moffett Field, CA 94035–1000: National Aeronautics and Space Administration System-Wide Accident Prevention Program Ames Research Center.
Leveson, N., Daouk, M., Dulac, N., Marais, K., 2003. In: Applying STAMP in Accident Analysis NASA Conference, pp. 177–198. < http://esd.mit.edu/WPS/esd-wp-2003-02.pdf > (retrieved June 9, 2015).
Leveson, N.G., 2011. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.
Leveson, N.G., 2009. Applying systems thinking to analyse and learn from events. Saf. Sci. 49 (1), 55–64. http://dx.doi.org/10.1016/j.ssci.2009.12.021.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 237–270.
Leveson, N., 2003. A new approach to hazard analysis for complex systems. In: Proceedings of the International Conference of the System Safety Society.
Leveson, N., 2002. System Safety Engineering: Back to the Future. MIT Press.
Leveson, N., Laracy, J., 2007. Apply STAMP to critical infrastructure protection. In: IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability. Woburn, pp. 215–220.
Meister, D., 1966. Human Factors in Reliability. In: Reliability Handbook. W.G. Ireson, McGraw Hill Book Company, New York, pp. 400–415.
Meister, D., 1971. Human Factors: Theory and Practice. John Wiley and Sons, New York.
Nivolianitou, Z.S., Leopoulos, V.N., Konstantinidou, M., 2004. Comparison of techniques for accident scenario analysis in hazardous systems. J. Loss Prev. Process Ind. 17 (6), 467–475. http://dx.doi.org/10.1016/j.jlp.2004.08.001.
Norman, D.A., 1981. Categorisation of action slips. Psychol. Rev. 88, 1–15.
Norman, D.A., 1986. Cognitive engineering. In: User Centred System Design. Lawrence Erlbaum Associates, Hillsdale, NJ, pp. 31–62.
Panchangam, S.P., Naikan, V.N.A., 2013. Reliability analysis of temperature sensor system. Int. J. Reliab. Qual. Saf. Eng. 20 (01), 1350003. http://dx.doi.org/10.1142/S0218539313500034.
Papadopoulus, Y., Parker, D., Grante, C., 2004. Automating the failure modes and effects analysis of safety critical systems. In: Proceedings of the Eighth IEEE International Symposium on High Assurance Systems Engineering (HASE'04). Retrieved from < http://www.fmeainfocentre.com/papers/20940310.pdf > .
Payne, D., Altman, J., 1962. An Index of Electronic Equipment Operability: Report of Development (No. Report No.AIR-C-43-1/62.). American Institute of Research, Pittsburgh. Pennsylvania.
Pew, R.W., Miller, D.C., Feehrer, C.S., 1982. Evaluation of Proposed Control Room Improvements through Analysis of Critical Operator Decisions. Electric Power Research Institute, Palo Alto, CA.
Qureshi, Z.H., 2007. A review of accident modelling approaches for complex socio-technical systems. In: Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-related Programmable Systems, vol. 86, Mawson Lakes, South Australia, pp. 47–59.
Rasmussen, J., 1981. Human Errors. A Taxonomy for Describing Human Malfunction in Industrial Installations. Risø National Laboratory, DK-4000, Roskilde, Denmark.
Rasmussen, J., 1982. Human errors: a taxonomy for describing human malfunction in industrial installations. J. Occup. Accid. 4, 311–335.
Rasmussen, J., 1986. Information Processing and Human-machine Interaction: An Approach to Cognitive Engineering. North-Holland, New York.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27 (2/3), 183–213.
Reason, J., 1990. Human Error. Cambridge University Press, New York.
Reason, J.T., 1979. Actions not as planned: the price of automatization. In: Underwood, G., Stevens, R. (Eds.), Aspects of Consciousness. Academic Press, pp. 1–67.
Reason, J.T., 1987. Generic error-modelling system: a cognitive framework for locating common human error forms. In: Rasmussen, J., Duncan, K., Leplat, J. (Eds.), New Technology and Human Error. Wiley, Chichester, England.
Rempe, J.L., Knudson, D.L., 2014. TMI-2 – A Case Study for PWR Instrumentation Performance During a Severe Accident (No. INL/EXT-13-28043). Idaho National Laboratory, Idaho, USA, p. 118. Retrieved from < http://www.inl.gov > .
Seaver, D.A., Stillwell, W.G., 1983. Procedures for Using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plant Operations (No. NUREG/CR-2743). Washington, DC 20555.
Senders, J., Moray, N., 1991. Human Error: Cause, Prediction, and Reduction. L. Erlbaum Associates, Hillsdale, New Jersey, USA.
Shorrock, S.T., Kirwan, B., 2002. Development and application of a human error identification tool for air traffic control. Appl. Ergon. 33, 319–336.
Song, Y., 2012. Applying System-Theoretic Accident Model and Processes (STAMP) to hazard analysis. University. Open access dissertations and theses, 6801. McMaster.
Spurgin, A., Lydell, B.D., Hannaman, G., Lukic, Y., 1987. Human reliability assessment: a systematic approach. Presented at the Reliability '87, NEC, Birmingham, England.
Stamatis, D.H., 2003. Failure Mode and Effect Analysis. FMEA from Theory to Execution (Second). ASQ Quality Press Milwaukee, Wisconsin.
Stanton, N., Salmon, P., Walker, G., Baber, C., Jenkins, D. (Eds.), 2005. Human Factors Methods: A Practical Guide for Engineering and Design. Ashgate Pub. Co., Aldershot, England; Burlington, VT.
Sträter, O., 1997. Evaluation of Human Reliability on the Basis of Operational Experience (Report GRS-138). Germany.
Sträter, O., 2000. Evaluation of Human Reliability on the Basis of Operational Experience (Translation of the Report GRS-138). Germany.
Swain, A.D., 1964. THERP (No. SC-R-64-1338). Sandia National Laboratories, Albuquerque, NM.
Swain, A.D., 1982. Modelling of response to nuclear power plant transients for probabilistic risk assessment. In: Proceedings of the 8th Congress of the International Ergonomics Association. Tokyo.
Swain, A.D., 1987. Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772. US Nuclear Regulatory Commission, Washington, DC.
Swain, A.D., Guttmann, H.E., 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, USNRC, Washington, DC 20555.
U.S. Department of Energy, 1992a. DOE Fundamentals Handbook Instrumentation and Control (Volume 1 de 2) (No. DOE-HDBK-1013/1-92). Washington, D.C., p. 132. Retrieved from < http://energy.gov/sites/prod/files/2013/06/f2/h1013v1.pdf > .
U.S. Department of Energy, 1992b. DOE Fundamentals Handbook Instrumentation and Control (Volume 2 de 2) (No. DOE-HDBK-1013/2-92). Washington, D.C., p. 168. Retrieved from < http://energy.gov/sites/prod/files/2013/06/f2/h1013v2.pdf > .
U.S. Nuclear Regulatory Commission, 2000. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA) (No. NUREG-1624, Rev. 1). Washington, DC 20555-0001.
US Department of Energy—US DOE, n.d. Alternative Fuels—Ethanol. Retrieved May 25, 2007, from < http://www.eere.energy.gov/afdc/altfuel/ethanol.html > .
Van Gerpen, J., 2005. Biodiesel processing and production. Fuel Process. Technol. 86 (10), 1097–1107. http://dx.doi.org/10.1016/j.fuproc.2004.11.005.
Van Gerpen, J., Shanks, B., Pruszko, R., Clements, D., Knothe, G., 2004. Biodiesel Production Technology. 1617 Cole Boulevard, Golden, CO: National Renewable Energy Laboratory.
Vanderhaegen, F., 2001. A non-probabilistic prospective and retrospective human reliability analysis method — application to railway system. Reliab. Eng. Syst. Saf. 71 (1), 1–13. http://dx.doi.org/10.1016/S0951-8320(00)00060-0.
Wickens, C., 1992. Engineering Psychology and Human Performance, second ed. Harper-Collins, New York.
Williams, J.C., 1985. HEART – a proposed method for achieving high reliability. In: Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society. Southport, pp. 87–109.
Williams, J.C., 1986. A proposed method for assessing and reducing human error. In: Proceedings of the 9th Advance in Reliability Technology Symposium. University of Bradford pp. B3/R/1-B3/R/13.
Williams, J.C., 1988. A data-based method for assessing and reducing human error to improve operational experience. In: Proceedings of IEEE 4th. Conference on Human Factors in Power Plants. Monterey, California, pp. 436–450.