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

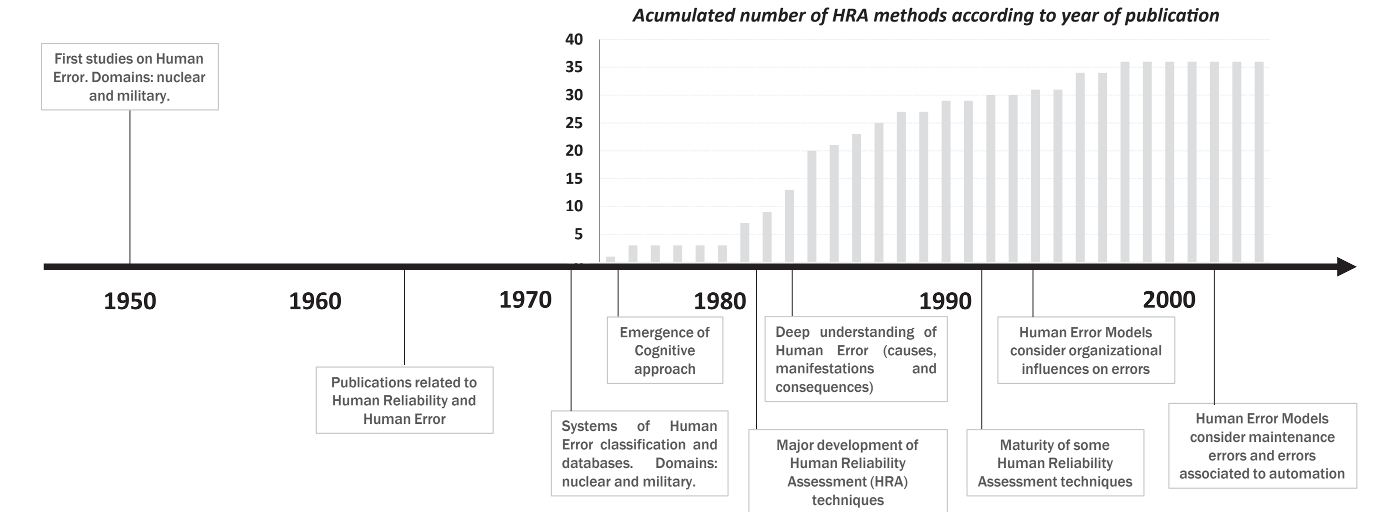

Fig. 1. Timeline of human error and human reliability studies.

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