Safety Science 84 (2016) 37–45

Contents lists available at ScienceDirect

Safety Science

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

Learning from major accidents to improve system design

Raphael Moura [a,b,*], Michael Beer [a,b], Edoardo Patelli [a,b], John Lewis [a,b], Franz Knoll [c,d]

[a] *Institute for Risk and Uncertainty, University of Liverpool, United Kingdom*
[b] *Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom*
[c] *NCK Inc., Montreal, Canada*
[d] *1200 Avenue McGill College, Montreal, Quebec H3B 4G7, Canada*

ARTICLE INFO

Article history:
Received 31 August 2015
Received in revised form 30 October 2015
Accepted 26 November 2015

Keywords:
Accident analysis
MATA-D
Human factors
Human reliability analysis
Risk & safety in design
CREAM

ABSTRACT

Despite the massive developments in new technologies, materials and industrial systems, notably supported by advanced structural and risk control assessments, recent major accidents are challenging the practicality and effectiveness of risk control measures designed to improve reliability and reduce the likelihood of losses. Contemporary investigations of accidents occurred in high-technology systems highlighted the connection between human-related issues and major events, which led to catastrophic consequences. Consequently, the understanding of human behavioural characteristics interlaced with current technology aspects and organisational context seems to be of paramount importance for the safety & reliability field. First, significant drawbacks related to the human performance data collection will be minimised by the development of a novel industrial accidents dataset, the Multi-attribute Technological Accidents Dataset (MATA-D), which groups 238 major accidents from different industrial backgrounds and classifies them under a common framework (the Contextual Control Model used as basis for the Cognitive Reliability and Error Analysis Method). The accidents collection and the detailed interpretation will provide a rich data source, enabling the usage of integrated information to generate input to design improvement schemes. Then, implications to improve robustness of system design and tackle the surrounding factors and tendencies that could lead to the manifestation of human errors will be effectively addressed.

1. Introduction

1.1. The human contribution to major accidents

Recent major accidents in complex industrial systems, such as in oil & gas platforms and in the aviation industry, were deeply connected to human factors, leading to catastrophic consequences. A striking example would be the investigation report from the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011) of the April 2010 blowout, in which eleven men died and almost five million barrels of oil were spilled in the Gulf of Mexico. The investigators unarguably emphasised the human factors role: features such a failure to interpret a pressure test and delay in reacting to signals were found to have interacted with poor communication, lack of training and management problems to produce this terrible disaster. Other contemporary investigation reports, such as the Rio-Paris Flight 447 (Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2011) and Fukushima (Kurokawa et al., 2012), share the same characteristics regarding the significance of human-related features to the undesirable outcome.

Thus, the understanding of the interactions between human factors, technology aspects and the organisational context seems to be vital, in order to ensure the safety of engineering systems and minimise the possibility of major accidents. A suitable Human Reliability Analysis (HRA) technique is usually applied to approach the human contribution to undesirable events.

1.2. Human reliability analysis: a brief review

Human Reliability Analysis (HRA) can be generally defined as a predictive tool, intended to estimate the probability of human errors and weigh the human factors contribution to the overall risk by using qualitative and/or quantitative methods.

In the early 60s, the first structured method to be used by industry to quantify human error was presented by Swain

[*] Corresponding author at: Office G79 Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom. Tel.: +44 (0)151 794 4837.

E-mail addresses: rmoura@liverpool.ac.uk (R. Moura), mbeer@liverpool.ac.uk (M. Beer), epatelli@liverpool.a.uk (E. Patelli), johnlewis010452@gmail.com (J. Lewis), franz.knoll@nck.ca (F. Knoll).

http://dx.doi.org/10.1016/j.ssci.2015.11.022
0925-7535/© 2015 Elsevier Ltd. All rights reserved.

(1963), which later evolved to the well-known Technique for Human Error Rate Prediction – THERP (Swain and Guttmann, 1983). This technique was initially developed to deal with nuclear plant applications, using in-built human error probabilities adjusted by performance-shaping factors and dependencies (inter-related errors) to deliver a human reliability analysis event tree. Some researchers (e.g. Reason, 1990; Kirwan, 1997; Everdij and Blom, 2013) refer to THERP as the most well-known method to assess human reliability and provide data to probabilistic safety assessments.

The accident model acknowledged as the "Swiss Cheese model", developed by Reason (1990), can be addressed as the most influential piece of work in the human factors field. It has been widely used to describe the dynamics of accident causation and explain how complex systems can fail through a combination of simultaneous factors (or as a result of the alignment of the holes of the Swiss cheese slices (Fig. 1).

Many Human Reliability Analysis subsequently developed were, to some extent, inspired by this model. Examples are the Human Factors Analysis Methodology – HFAM (Pennycook and Embrey, 1993), the Sequentially Outlining and Follow-up Integrated Analysis – SOFIA (Blajev, 2002), the Human Factors Analysis and Classification System – HFACS (Shappell et al., 2007), extensively used to investigate military and commercial aviation accidents, and the Systematic Occurrence Analysis Methodology – SOAM (Licu et al., 2007).

The concept that accidents arise from an arrangement of latent failures, later renamed to latent conditions (Reason, 1997), and active failures in complex systems demonstrated accuracy and practicality to guide prevention measures (Hopkins, 1999). Reason's studies of human errors have focused on the work environment, human control processes and safe operation of high-technology industrial systems, and included management issues and organisational factors.

There are several methods to assess human performance in different domains, and the development of such tools was notably triggered by the advances in high-technology industrial systems, particularly nuclear plants, aerospace, offshore oil and gas, military and commercial aviation, chemical and petrochemical, and navigation. Some of them were assessed by Bell and Holroyd (2009), who reported 72 different techniques to estimate human reliability and considered 35 to be potentially relevant. Further analysis highlighted 17 of these HRA tools to be of potential use for major hazard directorates in the United Kingdom. These techniques are usually separated by generations, which basically reflect the focus of the analysis.

The first generation methods, developed between the 60s and early 90s, are mainly focused on the task to be performed by operators. Essentially, potential human erroneous actions during the task sequence are identified, and the initial probability is then adjusted by internal and external factors (performance shaping factors, error-forcing conditions, scaling factors or performance influencing factors, depending on the methodology) to deliver a final estimation of human error probabilities. The key step in this approach is selecting the critical tasks to be performed by operators, which are considered to be elements or components subjected to failure due to inborn characteristics, thus having an "inbuilt probability of failure". These methods are widely recognised and commonly preferred by practitioners, probably because they provide a straightforward output such as an event tree or a probability value that can be directly integrated to Probabilistic Risk Assessments. Some examples are THERP, HEART (Human Error Assessment and Reduction Technique), presented by Williams (1986), and JHEDI (Justification of Human Error Data Information), introduced by Kirwan and James (1989).

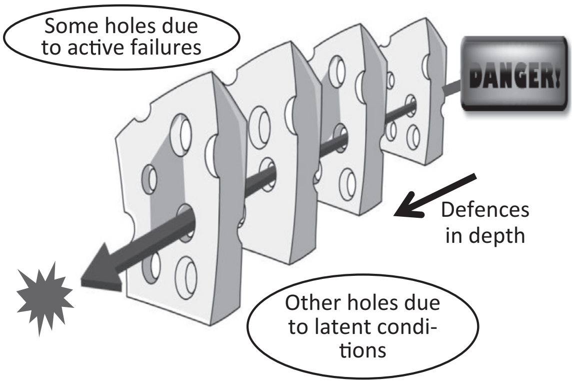
Some holes due to active failures
DANGER!
Defences in depth
Other holes due to latent conditions

Fig. 1. "Swiss Cheese Model" after Reason (1997).

Alternatively, second generation techniques have been developed from late 90's and are based on the principle that the central element of human factors assessments is actually the context in which the task is performed, reducing previous emphasis on the task characteristics *per se* and on a hypothetical inherent human error probability. "A Technique for Human Error Analysis" – ATHEANA (Cooper et al., 1996), the Connectionism Assessment of Human Reliability (CAHR) based on Sträter (2000) and the Cognitive Reliability and Error Analysis Method (CREAM) by Hollnagel (1998) are good examples of this kind of approach, all reflecting the focus shift from tasks to context to provide a better understanding of human error and integrate engineering, social sciences and psychology concepts. More recent literature (e.g. Kirwan et al., 2005; Bell and Holroyd, 2009) alludes to the Nuclear Action Reliability Assessment – NARA (Kirwan et al., 2005) as the beginning of the third generation methods. However, it seems to be merely an update of first generation techniques, i.e. HEART, using more recent data from newer databases such as CORE-DATA (Gibson and Megaw, 1999).

All these methods provide a number of taxonomies to handle possible internal and external factors that could influence human behaviour. Modern data classification taxonomies are mostly derived from Swain's (1982) work, in which he organised human errors in errors of omission and errors of commission, being the former a failure to execute something expected to be done (partially or entirely), while the latter can be translated as an incorrect action when executing a task or a failure to execute an action in time. The issue modelling human errors through the prediction of human behaviour during complex rare events was addressed by Rasmussen (1983), who envisioned the Skill–Rule–Knowledge (SRK) model. He differentiated three basic levels of human performance: skill-based, when automated actions follow an intention (sensory–motor behaviour); rule-based, when there is a procedure or technique guiding the action; and knowledge-based, represented by actions developed to deal with an unfamiliar situation. Reason (1990) split human errors in slips and lapses, when an execution failure or an omission occurs, and mistakes, which result from judgement processes used to select an objective, or the means to accomplish it. Later, Rasmussen's theory was encompassed by Reason to further categorise mistakes in rule-based mistakes, when a problem-solving sequence is known, but an error choosing the right solution to deal with the signals occurs; and knowledge-based mistakes, when the problem is not under a recognisable structure thus a stored troubleshooting solution cannot be immediately applied. Reason also highlighted an alternative behaviour from a social context, called "violation". This concept was split in exceptional and routine violations, both emerging from an intentional deviation from operating procedures, codes of practice or standards.

Although the classification schemes are usually connected to the industrial domain for which they were originally developed,