Learning from accidents: human errors, preventive design and risk mitigation

Thesis submitted in accordance with the requirements of
the University of Liverpool for the degree of Doctor in Philosophy

by

Raphael N. Moura

August 2017

www.manaraa.com

ProQuest Number: 28208925

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent on the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 28208925

Published by ProQuest LLC (2020). Copyright of the Dissertation is held by the Author.

All Rights Reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

www.manaraa.com

Acknowledgements

Firstly, it is with immense gratitude that I acknowledge the extremely friendly, professional and valuable guidance from Professor Michael Beer, Dr. Edoardo Patelli and Mr. John Lewis throughout my research period at the University of Liverpool's Institute for Risk and Reliability. I could not think of a better advisory and mentoring research team for any PhD candidate! I really appreciate all knowledge opportunities, discussions and insightful comments, which helped me to broaden my views from numerous perspectives and develop new ideas to face future challenges not only in the risk and uncertainty fields, but also in life. I hope I will have the privilege to continue receiving your guidance and possibly work together again, in future endeavours.

I would like to thank my industrial supervisor, Dr. Franz Knoll, for the massive experience and practical information brought into this research project.

The insights from academics which had the hard task to conduct my periodic assessments were extremely useful and added great value to my work, and I want to show my deepest appreciation to all of them, particularly to Dr. Francisco Alejandro Díaz De la O and Dr. Adam Mannis.

I would also to thank the extraordinary assistance of all Liverpool University staff over the past few years, particularly Ms. Lesia Swain, Ms. Andrea Jones, Ms. Carole Rhodes, Mr. Jack Carter-Hallam and Ms. Lyn Hughes.

I am very thankful to the support given by the Brazilian National Petroleum Agency (ANP), particularly Director Magda Chambriard. Without your valuable support and incentive, it would not be possible to conduct this research.

It is an honour for me to express my deepest appreciation to my wife Mariana, which took the challenge to move 9,500Km from Rio de Janeiro to Liverpool and wholeheartedly shared a student life with me, full of joy and discoveries. Your love and encouragement made this journey an unforgettable experience!

I am eternally indebted to my parents Marlene and Franklin (*in memoriam*). Your example of love, sacrifice, wisdom and determination will guide my life forever and will always motivate me to achieve my objectives with honesty, passion and enthusiasm.

Finally, I would like to thank my fellow colleagues at the Institute for Risk and Uncertainty, from the old Brodie Tower to the brand-new (and windowless!) Chadwick Building! All the research and fun we had in the last four years will never be forgotten, my PhD experience was surely enhanced by the terrific work environment you have always sustained!

www.manaraa.com

Abstract

Learning from accidents: human errors, preventive design and risk mitigation

Raphael N. Moura

Recent technological accidents, which resulted in severe material losses, multiple fatalities and environmental damage, were deeply associated with human errors. Direct human actions or flawed decision-making processes have been increasingly tied to devastating consequences, raising major concerns regarding industry's ability to control risks.

The most common approach to estimate the probability of human errors and weigh their impact to the overall risk is the application of a suitable Human Reliability Analysis (HRA) technique. However, uncertainties associated with behavioural aspects of humans dealing with advanced technology in complex organisational arrangements turn this type of evaluation into a challenging task to perform, an issue that brings difficulties to ensure sound predictions for human actions when interfacing with complex systems.

Consequently, the development of innovative strategies to overcome existing limitations to understand how these sociotechnical systems could fail is of paramount importance, particularly the intricate relationship between humans, technology and organisations. This PhD research project is devoted to approach this multidisciplinary problem in a systematic manner, providing means to recognise and tackle surrounding factors and tendencies that could lead to the manifestation of human errors, improving risk communication and decision making-processes and ultimately increasing confidence in safety studies.

The initial part of this thesis comprises a large-scale analysis of human errors identified during major accidents in high-technology systems. Detailed accident accounts were collected from regulators, independent investigation panels, government bodies, insurance companies and industry experts. The raw data is then scrutinised and classified under a common framework, resulting in a novel and comprehensive major-accident dataset, the Multi-attribute Technological Accidents Dataset (MATA-D).

The second stage applies advanced data analytic techniques to gain further insight into the conditions leading to the genesis and perpetuation of errors, essentially making use of cluster analysis and classification. The application of different clustering methods reveals common patterns among accidents, and the usage of an artificial neural network approach (self-organising maps) algorithm allows the translation of the multidimensional data into visual representations (2-D maps) of accidents' contributing factors. This stage generates appropriate information to increase the understanding of these sociotechnical systems, to overcome barriers to communicate risk and to enable a wide-ranging "learning from accidents" process.

The final part of the research project builds upon the self-organising maps algorithm output, focusing on a deeper interpretation of specific clusters to disclose strategies to minimise human factors weaknesses and reduce major accidents. An important practical implication suggested by the data analysis is that human errors, in most of the cases, constitute reasonable responses to disruptive transactions between the technology and the organisation, which impact human cognitive functions. Accordingly, the recognition that human errors are mistakenly seen as root-causes of major accidents and the examination of these interaction problems from a new perspective provided an effective way to recognise hazards and tackle major risks, delivering realistic proposals to improve design, decision-making processes and to build trust in safety assessments.

المنارة للاستشارات

www.manaraa.com

Table of Contents

www.manaraa.com

www.manaraa.com

www.manaraa.com

I. Introduction

Modern developments in structural analysis, engineering, risk and human reliability approaches are undoubtedly conveying more dependable and consistent systems, progressively reducing the likelihood of failures. Yet, technological accidents resulting in severe material losses, multiple fatalities and/or environmental damage are being increasingly perceived as a product of human errors. The Gulf of Mexico's Macondo well blowout, the Fukushima nuclear accident, the Air France 447 Flight hull loss and the South Korean Sewol Ferry capsize are examples, to name but a few, of disasters in which direct human actions or flawed decision-making processes were intimately related to devastating consequences.

Although the daily debate concerning the safety of industrial systems is normally confined to knowledgeable groups such as designers, engineers, psychologists, sociologists and philosophers, major accidents have the power to amplify the discussion to the general public and even force an outlook shift regarding certain technologies. As a result of the Fukushima disaster, the German government decided to shut-down eight nuclear reactors and reject the construction of new ones (Schneider et al., 2012). Correspondingly, the Taiwanese government postponed the start-up of a new reactor at the Lungmen Power Plant, and halted the construction of a second one, which clearance is conditional to a positive outcome in a nationwide referendum (Ishikawa, 2015).

In modern societies, it is precisely when a disaster strikes that the public is made aware of the technological risks and uncertainties carried by industrial activities, which might provoke a societal distrust climate with wide-ranging consequences. Boosted by staggering media coverage, especially in the face of catastrophes, human error becomes a concern to wider societal groups, and thus a very relevant research topic.

For engineering applications, the expression "human error" is typically defined as a failure to perform a certain task that leads to an adverse consequence (Moura et al., 2017b). In order to estimate the probability of human erroneous actions and evaluate the human factors impact to the overall risk, the most common approach is to apply a suitable Human Reliability Analysis (HRA) technique. However, uncertainties related to the behaviour of individuals dealing with advanced technology in intricate organisational environments turn this kind of evaluation into a challenging task to perform. Therefore, new strategies are

www.manaraa.com

required not only to better understand how human perform in such complex circumstances, but also to validate current approaches to model human performance and evaluate risk.

To tackle the need for appropriate and sufficient performance data to support HRAs, the U.S. Nuclear Regulatory Commission (NRC) developed the Scenario Authoring, Characterization, and Debriefing Application – SACADA dataset (Chang et al., 2014). The dataset is fed by plant staff (mainly training instructors and operators), and its prime aim is to collect operator simulator exercise data executed during nuclear power plants training programmes.

Preischl and Hellmich (2013) extracted human reliability data from the German licensee nuclear power plant events report system, obtaining HEP estimates using Bayesian methods. Their objective was to validate and extend the THERP (Swain & Guttman, 1983) human reliability analysis approach, and new data for twenty-one HEPs for which there were no previous data were presented. Previously, Groth and Mosleh (2012) had proposed a Bayesian belief network using data from nuclear power plant operating events, in order to produce a causal model for performance influencing factors from multiple sources, and calculate HEPs for HRAs. The data was exclusively extracted from nuclear industry sources, i.e. the Human Events Repository Analysis - HERA dataset (US Nuclear Regulatory Commission, 2008) and from worksheets used to analyse the behaviour of operators during abnormal operating conditions.

Forester et al. (2014) presented a large-scale international empirical study, which compared HRA predictions with crew performance outcomes when responding from basic to complex simulated scenarios in nuclear power plant (NPP) control rooms, using the Halden Reactor Project's HAMMLAB (Halden Human-Machine Laboratory) research simulator. The considered scenarios were modelled in a probabilistic risk assessment of the plant. Important strengths and weaknesses of several HRA methods were exposed, revealing a solid improvement path for current and future HRA approaches, particularly in the domain area of the study (crew performance in NPP control rooms). Some of the limitations of this work, such as difficulties to separate analyst and method effects, were later addressed in Forester et al. (2016), which compared HRA approaches with personnel actions when responding to simulated emergency scenarios from a U.S. NPP simulator. This new study not only discussed the analysts influence (e.g. HRA method implementation inconsistencies

www.manaraa.com

from individuals) by using multiple teams to test the consistency of HRA predictions, but also included visits to the reference plant to collect data and interview people. This is particularly important, as HRA methods might require particular data beyond the pure scenario description and simulation results, in order to deliver consistent outputs. Although it is fair to believe that the results might be extrapolated to general scenarios requiring the usage of emergency operating procedures, the scope of both studies (Forester, 2014, 2016) is limited to the evaluation of human reliability analysis approaches for NPP crews in the control room.

Recently, Kim et al. (2017) have suggested a new classification scheme for human error probability (HEP) estimations from simulator data. He conducted an extensive literature review comprising existing methods such as THERP (Swain & Guttman, 1983), HEART (Williams, 1986), CREAM (Hollnagel, 1998) and ATHEANA (Cooper et al., 1996), as well as datasets such as CORE-DATA (Gibson & Megaw, 1999) and SACADA (Chang et al., 2014) in order to quantify the nominal HEP estimates for the newly-developed framework. The selection of the factors is largely based on the analysis of audio-visual records of simulated tasks involving emergency operating procedures.

The development of the MATA-D and the application of an artificial neural network and other clustering/classification approaches to identify interaction among factors differ from current initiatives, in the sense that the objective here is not to quantify human error, to validate current HRA approaches or to develop a new method to do so. The intent is to enhance risk perception through the recognition and representation of multidimensional contributing factors interacting with human factors and thus affecting human performance.

Despite the fact that one of the features of the underlying MATA-D framework (originally used in CREAM HRA method) is the capacity to capture detailed cognitive functions and failure modes (Kim et al., 2017), the focus of the current work is not on the immediate factors shaping human actions, but on higher interactions between organisations, technology and human factors. The contribution to knowledge is a method which allows the identification of comprehensive contributing factors directly and indirectly affecting human actions and cognition, exposing the fact that improving human performance is not a self-contained effort: it will necessarily depends on technological and organisational enhancements. This research is a step forward in this identification process, addressing important needs of the practice and practitioners (e.g. creating synergy between human

www.manaraa.com

factors and system design and engineering communities) through the usage of major-accident investigation information, ultimately adding to current efforts to fulfil these data gaps from a new perspective. Accident analysis can offer factual data about the influencing factors leading to those events, and support a deeper examination of the ongoing dynamics involved in undesirable occurrences.

The dissemination of information about previous events is considered to be a crucial step towards improved operations (Lindberg et. al, 2010) and to reduce the likelihood of future events. Thus, the establishment of a "learning from accidents" process is particularly relevant for high-technology organisations, where major risks make more traditional knowledge expansion approaches such as trial-and-error unacceptable (ESREDA, 2015).

Accordingly, many initiatives aiming at the collection of operational data are being conducted, most of them using web-based incident reporting systems to gather information regarding safety events. Examples are the International Reporting System for Operating Experience, operated by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency of the Organisation for Economic Cooperation and Development (OECD/NEA); the Aviation Safety Reporting System, maintained by the US National Aeronautics and Space Administration; the Licensee Event Report from the US Nuclear Regulatory Commission; the Integrated Operational Safety System maintained by the Brazilian National Agency for Petroleum, Natural Gas and Biofuels; and the World Offshore Accident Database, developed by DNV-GL. Yet, difficulties to use the data to promote an effective learning strategy are acknowledged, and many researchers indicate that organisations have not been as successful as expected to absorb past occurrences' lessons (Kletz, 1997, Leveson, 2011, Le Coze, 2013, ESREDA, 2015).

This thesis largely relies on the data generated by independent investigations of major accidents, in opposition to near-misses or minor events, due to two fundamental reasons. Firstly, high-consequence events provoke wide-ranging data collection processes to support in-depth investigations. The data generated turns out to be very detailed, and valuable cross-industrial lessons can be learned, especially regarding complex interactions among contributors in higher hierarchical levels. Secondly, the dynamics involved in major-accidents are perceived to be extremely rare, requiring unique conditions to develop into the observed high-consequence events. Therefore, it is suggested that the subtleties captured by detailed investigations are hardly prospectively foreseeable, making these

www.manaraa.com

events significantly different from linear deviations and single-point failures, which are expected to occur in the course of regular operations.

Additionally, datasets comprising near-misses or minor operational occurrences usually lack detailed information about the organisational environment in which workers are placed, since scant attention and resources are dedicated to events with very limited (if any) consequences. Frequently, factors immediately identifiable such as equipment failures and operating errors turn out to be recorded as causes of events, without thoughtfully considering the bigger picture. Furthermore, the disproportionate emphasis on operators' errors might override the disclosure of profounder technology or organisational issues. Detailing procedures or retraining personnel are direct (and cheaper) solutions to manage, if compared to the discontinuation of components and equipment, design modifications or profounder changes to the sociotechnical system.

The appreciation of the organisational context is of paramount importance to fully understand the underlying conditions leading to an accident (Reason, 1990; Hollnagel, 1998; Cooper, 1996; Sträter, 2000; Dekker, 2014), and data acquisition and handling shortcomings can be a serious obstacle to achieving this enhanced comprehension. There must be a balance between the search for human, technology and organisational features, and sufficient resources should be allocated to identify all nuances of these complex, multi-faceted interactions. In a more realistic perspective, it is the dynamics of unanticipated interactions among potential contributors that are, in fact, pivotal to the manifestation of major accidents, and not mere isolated factors or causes.

Therefore, an effective data source for learning purposes must be able to deliver detailed information about accidents, being targeted at the search for contributors without biases and preconceptions and, most importantly, expose the intricate interfaces among influencing factors. It should not be limited to the apparent erroneous actions in the sharp-end, but investigate the motivations and understand cognitive processes behind human behaviour.

Mostly because of the societal pressure following catastrophes, major accidents give impetus to comprehensive data collection processes to support in-depth investigations, which are typically executed by very experienced professionals. These experts have diverse academic backgrounds and are independent from the affected company, broadening the

www.manaraa.com

examination prospects and being less subjectable to eventual pressures to direct the investigation or its outcome. Accordingly, Casal (2008) refers to historical analysis as the finest source of experimental data capable of delivering essential information to the validation of accident causation models. Also, the European Safety, Reliability and Data Association - ESREDA (2015) recognised that only large-scale events can make appropriate resources available to allow detailed examinations of systems and safety barriers, in contrast with near-misses (or deviations), which investigations are unlikely to go sufficiently deep to motivate major improvements in the sociotechnical system. An event such as the Macondo well blowout, occurred in the Gulf of Mexico in 2010, was investigated by two regulators (USCG, 2010, BOMRE, 2011) and an independent federal agency (US-CSB, 2016), along with industrial and academic groups. Furthermore, an inquiry on the eleven resulting fatalities and the environmental damage took place, offering plentiful information regarding the conditions leading to the disaster.

Still, incident analysis is not the only method to minimise high-technology risks. Qualitative and quantitative assessments have been widely used in high-technology industries, providing means to increase the reliability of components and systems, control hazards and promote safety. With this intent, a number of well-documented techniques and tools have been developed (and enhanced) since the 70s. Particularly, Probabilistic Safety Assessments (PSAs) have been successfully applied from the design conception to the final disposal of high-technology facilities, decisively contributing to the reduction of risks in high-hazard industries. The general idea is to quantify failures and adverse events, in order to evaluate systems, identify possible safety weaknesses, direct safety improvements and generate information for decision-making processes. PSAs are considered to be fundamental risk reduction tools, and are currently required by virtually all regulators and governments licencing processes involving, for instance, the construction, operation or modification of high-hazard facilities.

Other risk reduction approaches focus on learning from organisations with notable safety history. The principle underlying the High-Reliability Organisations theory is that certain industrial groups dealing with high-hazard technologies are able to deliver outstanding safety records for long periods of time, thus presenting a considerably higher number of success cases than failure cases (or accidents). Therefore, researchers sharing this view (Roberts, 1990, Grabowski & Roberts, 1997, La Porte & Consolini, 1998, Roberts & Bea, 2001) believe that it is possible to mitigate risks by studying the positive characteristics that

www.manaraa.com

make these organisations perform better than others. The overwhelming amount of data is one of the most tempting advantages to embrace this approach, as billions of working hours producing successful outcomes (i.e. the absence of failures) could be made available from a single organisation. However, some accident theorists seem to disagree. The intricacy and unpredictability of organisational behaviour and apparently untreatable features of some modern technologies, such as complexity and high-coupling, are recurrent discussion topics among accident causation theorists (Cohen et al., 1972, Sagan, 1993, Perrow, 1999, Taleb, 2007). They suggest that these characteristics make major accidents unique and, to some extent, unavoidable. Taleb (2007) claims that data collected from standard operations and the information generated (or what can be learned from it) have no relation with the dynamics of disasters, deemed as outliers, or black-swans. He understands that the nature of major accidents is completely different, and the data provided by regular operations cannot give much insight into the genesis of major accidents. Ultimately, he believes that an excessive focus on success cases can even override the sources of extremely rare, low-probability events, in which an unfamiliar combination of contributing factors may be seen as highly improbable, and thus negligible.

Recognising the different perspectives on how to approach major risks, this research project builds on the hypothesis that the examination of major accidents is able to provide a very rich data source through the detailed investigation accounts, enabling the exploration of the whole range of surrounding factors contributing to undesirable occurrences. The unfortunate events leading to catastrophic consequences undoubtedly offer an opportunity which cannot be left unexploited. In fact, it would be even socially unacceptable not to learn from those events, which sometimes leave long-lasting scars in modern societies. Therefore, it is the initial purpose of this research to develop a substantial dataset containing major accidents, in order to capture comprehensive information about disasters.

To ease the impact of the High-Reliability Organisations theory central assertion, specifically the fact that there are fewer failure cases than success ones to be examined, this research project concentrates on the development of a dataset capable of absorbing a wider spectre of major accidents from diverse industrial backgrounds. With this intent, a non-specific dataset classification structure yet robust and adaptable to embrace various accident investigation outputs is being used. As a result, virtually all types of industrial activity, ranging from offshore oil & gas to aviation, are successfully captured by the Multi-attribute

www.manaraa.com

Technological Accidents Dataset (MATA-D), creating an aggregate data volume suitable for the application of data mining approaches.

The complex data have been subjected to different data clustering and classification techniques, in an attempt to disclose tendencies leading to major accidents. Barriers to deal with multidimensional data – the dataset matrix can capture up to fifty-three contributing factors per accident – are overcome through its conversion into two-dimensional graphical representations of the accidents and associated contributors. In special, the 2-D maps generated by the application of the self-organising maps (SOM) algorithm (Kohonen, 2001) provide innovative means to visualise and communicate high-technology risks, while preserving the original data for further interpretation. Common patterns among major accidents are revealed and used in many ways to enhance risk perception and enable a comprehensive "learning from accidents" experience. Implications to build trust on risk management approaches and to improve decision-making processes are then discussed.

i. Aims and Objectives

The aim of this research project is to critically assess the complex interactions between human factors, technological aspects and organisational contexts in high-technology facilities, in order to identify and tackle surrounding factors and tendencies that could lead to the manifestation of human errors and result in major accidents, mitigating risks.

The main objectives of the research project are:

- To execute a large-scale analysis of human errors by collecting and classifying accident data from real projects worldwide, combining major accidents from different industrial backgrounds under a common framework in order to make them comparable;
- To understand the genesis and perpetuation of human errors, by applying advanced data mining techniques to disclose key features and significant trends in major accidents;
- To propose an alternative approach to risk communication, by translating complex interactions among accidents' contributing factors into graphical interfaces visually interpretable;

www.manaraa.com

- To build trust and improve the quality of safety studies, using the in-depth MATA-D information to ensure that human factors, technology and organisational aspects were properly taken into account by risk assessments; and
- To make recommendations to minimise the possibility of human errors, by means of improving the design of high-technology facilities.

ii. Original Contribution

The main outcome of this research is a wide-ranging analysis and interpretation of major accidents, providing conditions to learn from these undesirable events and offering opportunities to enrich the knowledge in the human factors field. A novel industrial accidents dataset, the Multi-attribute Technological Accidents Dataset (MATA-D), was fully developed, merging events occurred in numerous industrial backgrounds and countries. Methods to analyse and visually represent accident data are successfully proposed, and the graphical interfaces generated by the application of proper data mining techniques produced new insights into the conditions leading to accidents. The graphical output also provided unique means to understand and communicate risks. A new risk assessment verification scheme was established, based on the MATA-D common patterns disclosed by the application of the self-organising maps algorithm and on the innovative interpretation of its output.

iii. Structure of the Thesis

This thesis consists of a series of published papers that embodies the results of the PhD research. From the total of eleven published papers, five representative works were carefully selected to describe the study sequence, detail the findings and highlight the conclusions developed throughout the PhD period. These works were predominantly developed by the author of this thesis, with the valuable support of the co-authors and PhD supervisors listed in the corresponding chapters.

The first part of this thesis in Chapter 1 (Moura et al., 2016) introduces the Multi-attribute Technological Accidents Dataset (MATA-D), a proprietary dataset fully developed during the research, which contains 238 major accidents from different high-technology industrial sectors. The structure of the dataset follows the Contextual Control Model used as a basis for Hollnagel's (1998) Cognitive Reliability and Error Analysis Method. Accident reports prepared by regulators, independent investigation panels, government bodies and

www.manaraa.com

insurance companies, among others, were obtained, scrutinised and classified under the dataset's common framework, establishing the grounds for the subsequent application of data mining and clustering techniques.

Chapter 2 (Moura et al., 2017b) and Chapter 3 (Moura et al., 2015c) present the successful application of different data mining approaches to the MATA-D dataset, aiming at the disclosure of relevant features and revealing common patterns among major accidents' contributing factors. The latter chapter recurs to a tailored Hierarchical Agglomerative Clustering method, while the former applies an artificial neural network approach, i.e. self-organising maps (Kohonen, 2001), to the dataset. The application of the SOM approach allows for the translation of the MATA-D multidimensional data into 2-D maps, and graphical interfaces produce further insight into the conditions leading to major accidents. The SOM maps interpretation provides innovative means to understand, visualise and communicate major risks.

The subsequent chapters build upon the results of the SOM algorithm, demonstrating the wide-range applications of the research. This is the third part of the thesis.

Chapter 4 (Moura et al., 2017d) uses the output of the clustering method and thus the most common interactions between human factors, technological issues and organisational aspects, as extracted from the SOM maps, to produce a new framework to verify safety studies. The outcome is a sixty-six-item attribute list, addressing wide-ranging features that should be taken into account by risk analysts, particularly when assessing high-technology industrial facilities.

In Chapter 5 (Moura et al., 2017c), the focus is on MATA-D interactions which are connected with decision-making processes. Tendencies observed from the reinterpretation of the SOM output are compared with decisions made by the first-line management of an offshore facility, in the face of a real emergency scenario. It enables a broader debate of common managerial shortcomings, discussing practical means to improve emergency response decision-making processes in an offshore production platform, supported by the trends extracted from the major-accident dataset.

www.manaraa.com

Part I

The Multi-Attribute Technological Accidents Dataset (MATA-D) construction

www.manaraa.com

Chapter 1: Learning from major accidents to improve system design

Overview

The first part of this research project focus on the development of a novel industrial accidents dataset, i.e. the Multi-attribute Technological Accidents Dataset (MATA-D). The underpinning idea was to collect major-accident data from different industrial backgrounds, and then categorise them under a common framework, in order to make events comparable and to create the basis for the study.

A fifteen-month effort to obtain input data from institutions responsible for investigating major accidents resulted in the current version of the dataset, which contains 238 events. The development of a new dataset, limited to rare events (i.e. major accidents), was an attempt to overcome data collection problems on human performance, a relevant issue later addressed in this chapter.

Therefore, detailed accounts on major accidents were collected from insurance companies, regulatory bodies, commissions of inquiry and investigation boards, such as MARSH Inc., the Australian Department of Industry and Resources (DoIR), the Australian National Petroleum Safety Authority (NOPSA), the Brazilian National Petroleum Agency (ANP), the European Agency for Safety and Health at Work (EU-OSHA), the National Aeronautics and Space Administration (NASA), the Norwegian Foundation for Scientific and Industrial Research (SINTEF), the Petroleum Safety Authority Norway (PSA), the UK Department of Employment, the UK Health and Safety Executive (HSE), the US Bureau of Safety and Environmental Enforcement (BSEE), the US Chemical Safety and Hazard Investigation Board (CSB), the US Department of Energy (DoE), the US Environmental Protection Agency (EPA), the US Fire Administration (USFA), the US Minerals Management Service (MMS), the US National Transportation Safety Board and the US Occupational Safety and Health Agency (OSHA).

The dataset structure follows the Contextual Control Model used as a basis for Hollnagel's (1998) Cognitive Reliability and Error Analysis Method. The chosen framework aims to provide new means to capture the connections (and possible disturbances) between human factors, technological issues and organisational aspects which resulted in catastrophic consequences, as described in several contemporary investigation reports from major accidents occurred in high-technology systems. This chapter presents a detailed

www.manaraa.com

example of how the data was translated from the reports to the dataset categories (Table 2, pp. 21).

The statistical results suggested that a deeper understanding of human behavioural characteristics interlaced with current technology aspects and organisational context might reveal new opportunities to improve safety and mitigate risks. The accidents' collection and the detailed data interpretation provided a rich data source to tackle major risks, and the chapter introduces the usage of integrated accident information to generate input to design improvement schemes. Additionally, after identifying specific correlations involving human factors and design failures, implications to improve the robustness of system design and the identification of some of the surrounding factors and tendencies that could lead to the manifestation of human errors were effectively addressed. The successful creation of the MATA-D paved the way for the next research steps.

www.manaraa.com

Learning from major accidents to improve system design[1]

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
[*] Corresponding author at: Office G79 Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom.

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 emphasized 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, 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.

---

[1] Original publication in Moura, R. et al., 2016. Learning from major accidents to improve system design, *Safety Science Journal 84*: 37–45, DOI 10.1016/j.ssci.2015.11.022.

www.manaraa.com

In the early 60's, the first structured method to be used by industry to quantify human error was presented by Swain (1963), which later evolved to the well-known Technique for Human Error Rate Prediction - THERP (Swain & Guttman, 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 (interrelated errors) to deliver a human reliability analysis event tree. Some researchers (e.g. Reason, 1990; Kirwan, 1997a; Everdij and Blom, 2013) refer to THERP as the most well-known method to assess human reliability and to 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 (Figure 1).

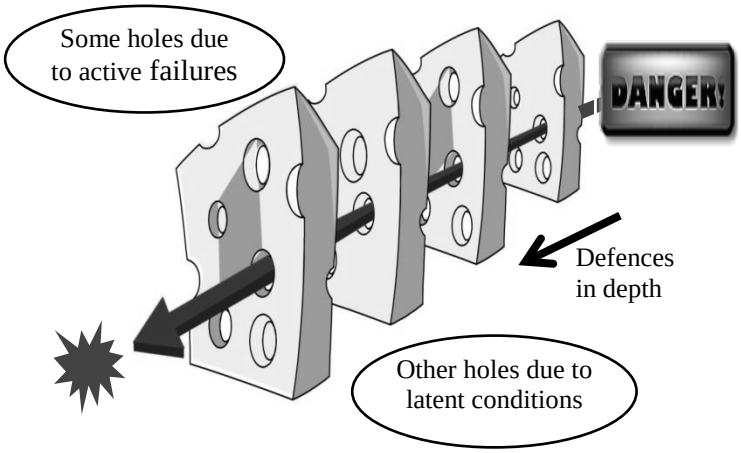

Figure 1. "Swiss Cheese Model" after Reason (1997)

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).

www.manaraa.com

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 60's and early 90's, 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).

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

www.manaraa.com

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 of 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.

www.manaraa.com

Although the classification schemes are usually connected to the industrial domain for which they were originally developed, some of them are nonspecific (e.g. HEART) and thus have been successfully applied in a broader range of industries.

Regardless of the variety of HRA methods available to enable practitioners to assess the risks associated with human error by estimating its probability, the substantially high uncertainties related to the human behavioural characteristics, interlaced with actual technology aspects and organisational context, turn this kind of evaluation into a very complicated matter, thus has been raising reasonable concern about the accuracy and practicality of such probabilities.

Those concerns resulted in significant efforts towards the validation of HRA methods. Kirwan (1997a, 1997b), compared HRA outputs against known data, essentially verifying if the estimations matched the true values. The usage of real data from operational experience (including near misses) is considered of "first order", while the validation based on simulations, experimental literature and expert judgment is referred as approximate or "second order" validation. A third order (or convergent) validation would involve the comparison among HRA techniques. In his view, the usage of real data from operational experience is *clearly* the best solution. Correspondingly, Preischl and Hellmich (2013) relied on human reliability data from the German licensee nuclear power plant events reporting system to obtain HEP estimates, later comparing some of the results with the THERP handbook tables, in order to validate it. They found the results derived from the reporting system to be in fair agreement with THERP, but also identified twenty-one new HEPs, which they suggest that should be added to the THERP dataset.

Using a high-fidelity simulator (the Halden Reactor Project's HAMMLAB), Forester et al. (2014) compared HRA outputs from several approaches with results from personnel responding to simulated emergency scenarios in a nuclear power plant control room. Shirley et al. (2015) assessed the requirements and identified objective needs (such as restricting the data collection to high-fidelity simulators) for the validation of a specific technique (i.e. THERP) using simulator data, presenting a useful guide for future validation works.

www.manaraa.com

1.3 Human performance data limitations

Data collection and the availability of meaningful datasets to feed human reliability analyses, to assess human performance in engineering systems and to understand how human factors interact with systems and organisations are relevant issues constantly addressed by risk and safety management practitioners and researchers. Many studies in the early 90's addressed these issues, and both the unavailability of data on human performance in complex systems (Swain, 1990) and limitations related to the data collection process (International Atomic Energy Agency, 1990) were considered to be problems extremely difficult to overcome. In order to fulfil the need for appropriate data to support HRAs, a number of recent works (Groth & Mosleh, 2012, Preischl & Hellmich, 2013, Kim et al., 2017) were developed, mainly focusing on improving the estimation of human error probabilities.

Other data collection efforts recognised the importance of understanding accident scenarios to mitigate risks, and attempted to use operating experience. The Storybuilder Project (Bellamy et al., 2006), for instance, concentrated on the classification and statistical analysis of occupational accidents to construct a general accident causation model. Still, Grabowski et al. (2009) pointed out the exponential rise of electronic records as an operational data collection problem, claiming that *data validation, compatibility, integration and harmonisation are increasingly significant challenges in maritime data analysis and risk assessments*. Problems related with the integration and harmonisation of data may be intensified by attempts to classify and compare accidents from different industrial backgrounds, if an adequate framework is not selected.

This work aims to generate a new data source, to serve as a suitable input to the understanding of human performance under high-hazard scenarios and to expose how it can be affected by technology and organisational aspects. Moura et al. (2015a) have previously discriminated some of the difficulties that might be preventing the development of a comprehensive, cross-industrial dataset with this intent. Main issues can be summarised by: (i) dissimilar jargons and nomenclatures used by distinct industrial sectors are absorbed by the classification method, making some taxonomies specific to particular industries; (ii) the effort to collect human data from accident reports and real operational experience is time-consuming, and could favour, for instance, the immediate use of expert elicitation or less-than-adequate available data, instead of developing a new dataset; (iii)

www.manaraa.com

the accuracy of the collection method is very difficult to assess, and distinct sources (e.g. field data, expert elicitation, performance indicators or accident investigation reports) can lead to different results; and (iv) the interfaces between human factors, technological aspects and the organisation are context-dependent and can be combined in numerous ways, due to the variability of the operational environment and the randomness of human behaviour.

These significant drawbacks will be minimised by the development of a novel industrial accidents dataset, bringing together major accident reports from different industrial backgrounds and classifying them under a common framework, which is capable of absorbing accident narratives from several sources. In spite of being a time-consuming and a laborious process, 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.

Accident investigations can be considered to be one of the most valuable and reliable sources of information for future use, provided that several man-hours from a commissioned expert team are applied in an in-depth analysis of an undesirable event sequence, providing detailed insight into the genesis of industrial accidents.

2. Classification Method

2.1 The Cognitive Reliability and Error Analysis Method (CREAM) taxonomy as a common framework to classify accidents

In a previous work, some of the most used taxonomies in human reliability analysis were examined as possible inputs to the establishment of a data classification framework for a global accidents dataset. The three nomenclature sets considered by Moura et al. (2015a) were The Human Factors Analysis and Classification System - HFACS (Shappell et al. 2007), the Error Promoting Conditions (EPCs) from the Human Error Assessment and Reduction Technique (HEART) and the CREAM categorisation.

Primarily, CREAM is a HRA approach, thus its taxonomy was not only designed to support the search for causes in retrospective evaluations (or accident analysis), but also to provide human error probabilities estimations. Although some important limitations for the use of CREAM as a HEP estimation method are known, such as the fact that the CREAM failure

www.manaraa.com

types assignment is too subjective and not sufficiently detailed to account for differences observed in crew performance (Forester et al.,2014), the method is still capable of supporting prospective and retrospective evaluation initiatives (Ung, 2015, Zhou et al., 2017).

Some of the limitations appear to be intimately associated with the flexibility of the method, as a trade-off between detailing the factors directly affecting human actions and including higher level organisational ones (to explain past events) had to be reached, in order to enable the method to capture factors serving both purposes.

However, the current work exclusively relies on previously executed analyses of major accidents – within the "retrospective analysis" class – to build a dataset comprising immediate and latent contributing factors, which are mostly exposed in detailed accident investigations. The main objective is to better understand major accidents and ultimately identify significant interactions between organisations, technology and human factors, to improve human performance under complex scenarios and reduce risk. With this intent, the taxonomy is solely used to construct the dataset structure, not following Hollnagel's (1998) procedures to perform accident analyses or prospective analyses.

Several important initiatives (Cooper et al., 1996, Gibson & Megaw, 1999, Chang et al., 2014, Kim et al., 2017) are focused on estimating human failure probabilities to serve HRA data needs and allow further integration with PRAs. Nonetheless, there is a growing need to understand complex decision-making processes in abnormal or accident scenarios, to identify human interactions with latent system failures and to explore organisational factors (Oxstrand, 2010).

Provided that generating HEPs is out of the scope of the current work, the aforementioned taxonomy issues are not supposed to affect the research outcome. Perfectly supporting the envisioned application, the classification method has shown a great potential to capture appropriate information from accident narratives, as previously discussed in Moura et al. (2015a) and further demonstrated in section 3.4 of the current work. Therefore the development of the dataset is intended to support an improved understanding of operator performance, especially under complex major-accident scenarios, meant to provide a key contribution to operational safety.

www.manaraa.com

Additionally, the fact that CREAM uses a nonspecific taxonomy, thus adaptable to most industrial segments, and its natural separation between man, technology and organisation, facilitating the accidents classification, made this terminology to be selected, in order to originate the structure of the new dataset.

Figures 2, 3 and 4 show the dataset classification structure.

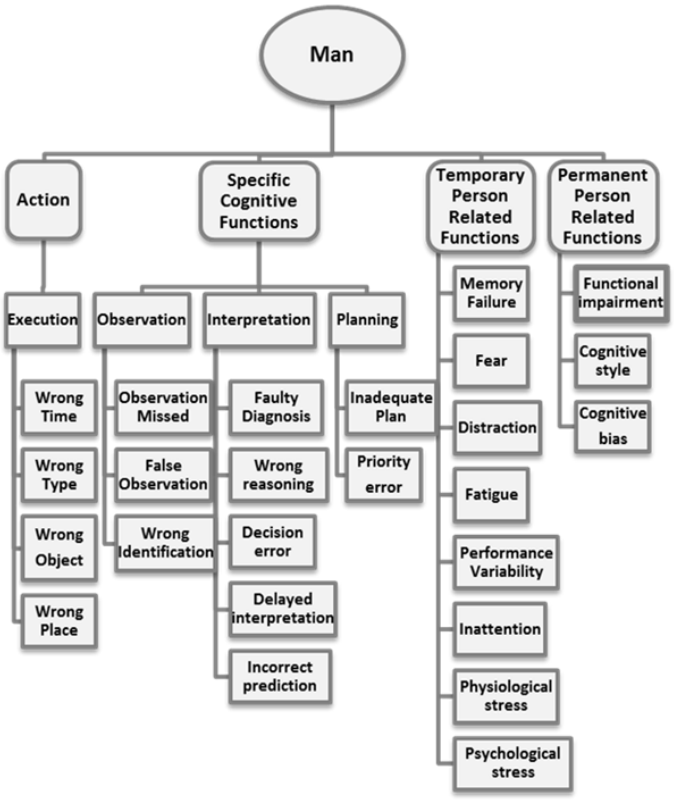

Figure 2. "Man" categorisation, adapted from Hollnagel (1998).

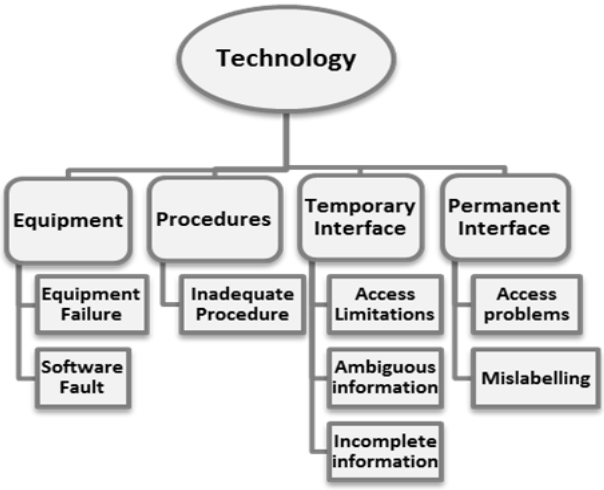

Figure 3. ""Technology" categorisation, adapted from Hollnagel (1998).

www.manaraa.com

Figure 4. "Organisation" categorisation, adapted from Hollnagel (1998).

The 53 factors which could have influenced each of the 238 assessed accidents are organised in the three major groups depicted in Figures 2, 3 and 4. The "man" group concentrates human-related phenotypes in the action sub-group, representing the possible manifestation of human errors through erroneous actions (Wrong Time, Wrong Type, Wrong Object and Wrong Place), usually made by operators in the front-line. These flawed movements cover omitted or wrong actions; early, late, short, long or wrong movements, including in an incorrect direction or with inadequate force, speed or magnitude; skipping one or more actions or inverting the actions order during a sequence.

Possible causes or triggering factors with human roots can be classified as Specific Cognitive Functions, or the general sequence of mental mechanisms (Observe-Interpret-Plan) which leads the human being to respond to a stimulus. Also, temporary (e.g. fatigue, distraction or stress) and permanent disturbances (biases such as a hypothesis fixation or the tendency to search for a confirmation of previous assumptions) can be captured under the sub-groups Temporary and Permanent Person-related Functions. These are the person-related genotypes.

The second major group (Figure 3) represent technological genotypes, associated with procedures, equipment and system failures, as well as shortcomings involving the outputs

www.manaraa.com

(signals and information) provided by interfaces. The last group (Figure 4) encompasses organisational contributing factors, representing the work environment and the social context of the industrial activity. It involves latent conditions (such as a design failure), communication shortcomings and operation, maintenance, training, quality control and management problems. Factors such as adverse ambient conditions and unfavourable working conditions (e.g. irregular working hours) are also included in this category.

3. Review of 238 major accidents: the multi-attribute technological accidents dataset (MATA-D)

3.1 MATA-D conception: data selection

To overcome the problems of the data collection process and the quality variability of different data sources, this work limits the data gathering to detailed accounts of accidents occurred in the industrial segments listed in Table 1. Accident reports and detailed case studies contain comprehensive information about the events, which can be interpreted and modelled into the groups and sub-groups shown in Figures 2, 3 and 4, to serve as input to the newly-created Multi-attribute Technological Accidents Dataset (MATA-D). The original reports were obtained from reliable sources such as regulators, investigation panels, government bodies, insurance companies and industry experts. A detailed account of the contributing institutions can be found in Moura et al. (2015a). The dataset covers major accidents occurred worldwide, from the early fifties to today. Table 1 shows the accidents time-spam per industrial activity.

It is worth mentioning that the data selection criterion brought two significant gains. The use of real-life accounts reduces uncertainties related to the accurateness of the data, and investigation reports supply detailed technical info, evidences and an in-depth analysis of the interfaces between human factors, technology and the organisation in which the event occurred. This seems to be one of the finest sources of information available, from which MATA-D is fully designed.

Table 1. MATA-D events distribution by industry

Industry	Accidents		Period
	#	%	
Refinery	39	16.39	1978 - 2011
Upstream (Oil & Gas)	37	15.55	1975 - 2012
Chemicals Factory	29	12.18	1975 - 2011
Petrochemicals	25	10.50	1974 - 2008

www.manaraa.com

Nuclear Industry	23	9.66	1953 - 2011
Civil Construction	16	6.72	1968 - 2011
Terminals and Distribution	15	6.30	1975 - 2012
Aviation Industry	13	5.46	1996 - 2013
Gas Processing	09	3.78	1977 - 2008
Metallurgical Industry	07	2.94	1975 - 2011
Waste Treatment Plant	05	2.10	2002 - 2009
Food Industry	04	1.68	1998 - 2009
Other	16	6.72	1980 - 2011

3.2 MATA-D usage

This new accident dataset aims to provide researchers and practitioners with a simple and innovative interface for classifying accidents from any industrial sector, reflecting apparently dissimilar events in a comparable fashion. The binary classification for the evaluated factors (presence or absence) allows data interpretation using uncomplicated statistical methods or sophisticated mathematical models, depending on the user's requirements.

Moreover, the detailed descriptions available for each identified factor, as can be seen in the example given in Table 2, allows comprehensive understanding and analysis of single accidents, as well as the disclosure of the precise evidence of failures associated with psychological (cognitive functions), engineering (e.g. design and equipment failures) and organisational (e.g. management problems and training) aspects. These descriptions provide an effective translation of highly technical content reports to a linguistic approach easily understood by practitioners from outside the engineering field, facilitating cross-disciplinary communication among professionals and academics. Many applications can be developed from these unique characteristics.

3.3 Features of the data sample

1,539 fatalities were recorded in 67 of the 238 analysed events. Some of the reports also contained damage recovery information, and 95 events were accountable for more than £20 billion in material losses. Apart from these significant features, it is acknowledged that many additional costs arise from major accidents. It is reported (Fowler, 2013) that British Petroleum (BP) paid around US$ 14 billion in indenisations related to the Gulf of Mexico oil

www.manaraa.com

spill clean-up, and Bell (2012) described a 35.00% stock price drop from the event occurrence in 2010 to 2012.

However, the most significant feature of the dataset events is that all of them involved a major emission, fire, explosion or crash, exposing humans and/or the environment to serious danger. Thus, these events largely fit the definition of "major accident", according to the United Kingdom's Control of Major Accident Hazards Regulations (1999).

3.4 MATA-D Construction: data interpretation and classification demonstration method

The analysis and classification of nearly 250 accident reports (some events were investigated by more than one entity and had multiple records) was a time-consuming process, but enabled the comparison among accidents from different industries. Investigation reports varied from a few to a maximum of 494 pages.

The process involved the interpretation of the accidents reports and their subsequent classification under the common taxonomy to create the dataset.

Table 2 exemplifies how one of the collected accidents was carefully decomposed and recorded in the MATA-D database. This example scrutinises a severe explosion of flammable gasoline constituents released from a refinery's hydrofluoric acid (HF) alkylation unit, examined by the US Chemical Safety and Hazard Investigation Board (2005b). The release, ignition, fire and several explosions occurred during the preparation of a pump repair, which was being removed by maintenance workers. As a consequence, six employees were injured, the production was stopped for approximately 6 months and a damage repair cost of US$ 13 million was reported.

Table 2. Oil Refinery Fire and Explosion classification example

Group	Sub-Group	Factor	Description*
Man	Execution	Wrong Type	Movement in the wrong direction: during a seal repair, the operator attempted to isolate the pump by closing a plug valve. He moved the valve wrench to a perpendicular position in relation to the flow, believing this was the closed position, but the valve was actually open.

www.manaraa.com

Man	Specific Cognitive Functions (Observation)	Observation missed	Overlook cue/signal: The valve stem was equipped with a position indicator, but the operators overlooked it. The indicator was correctly indicating the open status.
Man	Specific Cognitive Functions (Observation)	Wrong Identification	Incorrect identification: the mechanic specialist recognised the valve as closed due to the wrench position and, following a safety procedure, placed locks and tags on the valve, to prevent its inadvertent opening.
Man	Specific Cognitive Functions (Interpretation)	Wrong reasoning	(i) Deduction error: Operator and mechanic specialist firmly believed that the closed valve position was always identified by the wrench being perpendicular to the flow of product. (ii) Induction Error: after unbolting the flare line, a small release of a high flammable component was observed for a few seconds. As the flux stopped, the operator inferred that the pump was de-pressurised and the removal was safe. However, vent line was clogged by scale.
Man	Specific Cognitive Functions (Planning)	Priority error	After the installation of the locks, the operator noticed that the position indicator was showing that the valve was open, but he maintained his plans and left the plant to fetch the necessary tools for the pump removal.
Man	Permanent Person Related Functions	Cognitive bias	Confirmation bias: search for information was restricted to looking at wrench position, which confirmed the operator's assumption that the valve was closed, dismissing a further consideration of the fully functioning position indicator.
Technology	Temporary Interface	Ambiguous Information	Position mismatch: wrench collar was installed in an unusual position. Usually, the perpendicular wrench position indicates the closed state, while the parallel wrench position indicates the open status. Thus, wrench position (open-close) was inverted and thus conflicting with the position indicator.
Organisation	Organisation	Maintenance Failure	(i) There was no effective preventive/predictive maintenance programme to maintain pumps operational, as interventions (repair / parts replacement) took place only when equipment failed. The investigation of possible failure mechanisms (the actual causes of the breakdowns) never occurred. (ii) Flare line was clogged by scale.

www.manaraa.com

Organisation	Organisation	Inadequate Quality Control	(i) Despite the recurring failures of several pump seals in the plant (prior to the accident, 23 work orders for similar defects were issued), quality control procedures failed to ensure the adequacy of the equipment to the transported product and to certify that maintenance procedures were suitable. (ii) Quality control failed to identify the inadequate installation of the wrench collar, which allowed the wrench bar to stay in an unusual position, unfamiliar to operators.
Organisation	Organisation	Design Failure	The valve actuator (wrench) collar had a squared shape and could be installed in any position, thus there was a discrepancy between the design of the valve and its actuator. Design should have prevented the wrench installation in an unusual position. Also, further investigation identified that the original actuator was a gear-operated one, and the design change to a wrench actuator failed to address further safety implications, such as the produced mismatch between the position indicator and the wrench position.

**Adapted from the evidence/accounts from the US Chemical Safety and Hazard Investigation Board (2005b) Case Study.*

The classification method was applied to the above accident and the Table 2 clearly exemplifies how the investigation report from an event occurred in a specific industry (i.e. a refinery) can be decomposed into general categories, enabling the association with most industrial sectors. This classification method allowed the creation of a dataset composed by major accidents from industries with no apparent connection, but sharing common features (groups, sub-groups and factors) which contributed to serious events. In addition, the dataset preserves the main characteristics of the scrutinised events at the description column, facilitating the prompt understanding of complex investigation reports and allowing further analysis of single or grouped events, if required.

A seemingly pure human error (which could be described by the removal of the pump without closing the isolation valve or, more specifically, opening the isolation valve instead of closing it) can be explained by some cognitive mechanisms triggered by technology and organisational issues. The worker tried to isolate a pump for maintenance by putting the valve wrench in a perpendicular position in relation to the piping, which is a widely accepted convention for the closed state of a valve. He disregarded the position indicator at the valve body, assuming the wrench position as a sufficient proof of the pump isolation. A

www.manaraa.com

mechanic specialist who was responsible for double-checking the isolation, for safety reasons, also deduced that the valve was closed just by looking at the wrench position, and locked the valve. This allows the identification of valuable cognitive functions influencing the human erroneous actions, assisted by the terminology of the classification method, such as the observation missed, the wrong identification, wrong reasoning and priority error. A person-related cognitive bias was also categorised, explaining why the operator ignored the position indicator.

Even more important, the link between technology, design and human factors can be clearly established: the ambiguity of the information provided by the interface (unfamiliar wrench position versus position indicator), triggered by the design failure, motivated the operator to reason in a way that the error of opening the isolation valve, instead of closing it, was plausible. Other organisational contributors, such as the quality control faults of the wrench installation and the mechanical integrity programme, were also captured by the classification scheme.

3.5 MATA-D Results & Analysis

Following the same method presented in Table 2, 238 major accidents were scrutinised and computed into the MATA-D. Tables 3, 4, 5 and 6 summarise the results obtained from the interpretations of the accident reports analysed by the authors, as well as the resulting categorisation.

Table 3. Data Classification results (main groups).

Group	Frequency*	
	#	%
Man	136	57.14
Technology	196	82.35
Organisation	227	95.38

**Number of events where groups appeared.*

Table 4. Data Classification results (factors & sub-groups).

Factor	Frequency*		Sub-Group	Freq.*
	#	%		%
Wrong Time	35	14.70	Execution	54.60
Wrong Type	28	11.80		
Wrong Object	06	2.50		
Wrong Place	75	31.50		

www.manaraa.com

Observation Missed	37	15.50	Cognitive Functions**	47.50
False Observation	08	3.40		
Wrong Identification	06	2.50		
Faulty diagnosis	31	13.00		
Wrong reasoning	27	11.30		
Decision error	22	9.20		
Delayed interpretation	11	4.60		
Incorrect prediction	09	3.80		
Inadequate plan	23	9.70		
Priority error	17	7.10		
Memory failure	02	0.90	Temporary Person Related Functions	13.00
Fear	05	2.10		
Distraction	14	5.90		
Fatigue	07	2.90		
Performance Variability	03	1.40		
Inattention	05	2.10		
Physiological stress	02	0.80		
Psychological stress	07	2.90		
Functional impairment	01	0.40	Permanent Person Related Functions	7.60
Cognitive style	00	0.00		
Cognitive bias	17	7.10		
Equipment failure	131	55.00	Equipment	56.30
Software fault	06	2.50		
Inadequate procedure	105	44.10	Procedures	44.10
Access limitations	03	1.30	Temporary Interface	18.90
Ambiguous information	06	2.50		
Incomplete information	42	17.60		
Access problems	04	1.70	Permanent Interface	3.40
Mislabelling	04	1.70		
Communication failure	25	10.50	Communication	29.00
Missing information	49	20.60		
Maintenance failure	83	34.90	Organisation	94.10
Inadequate quality control	144	60.50		
Management problem	22	9.20		
Design failure	157	66.00		
Inadequate task allocation	143	60.10		
Social pressure	17	7.10		

www.manaraa.com

Insufficient skills	86	36.10	Training	54.20
Insufficient knowledge	84	35.30		
Temperature	03	1.30	Ambient Conditions	8.80
Sound	00	0.00		
Humidity	00	0.00		
Illumination	02	0.80		
Other	00	0.00		
Adverse ambient condition	17	7.10		
Excessive demand	13	5.50	Working Conditions	11.30
Poor work place layout	06	2.50		
Inadequate team support	08	3.40		
Irregular working hours	09	3.80		

**Number of events where factors or sub-groups appeared.*
*** Cognitive functions detailed on Table 5.*

Table 5. Data Classification results (cognitive functions).

Cognitive Function	**Frequency***	
	#	**%**
Observation	47	19.70
Interpretation	79	33.20
Planning	38	16.00

**Number of events where cognitive functions appeared.*

Tables 3, 4 and 5 specify the number of appearances of the man-related, technology and organisational phenotypes and genotypes identified in the major accidents examined. Percentages relate to the total of events (238).

At least one human element was identified in 57.14% of the cases, with 54.60% of direct erroneous actions (phenotypes). Cognitive functions accounted for 47.50%, with the interpretation genotype appearing as the most relevant (33.20%). At least one technology genotype was recognised in 82.35% of the accidents, highlighting equipment failure (55.00%) and inadequate procedures (44.10%) as the foremost factors related to this group. Organisational issues appeared in 95.38% of the accidents, emphasising design failures (66.00%), inadequate quality control (60.50%) and inadequate task allocation (60.10%) as the most significant genotypes within the group.

Table 6 presents a macro-analysis of the major groups (man, machine and organisation), indicating that a single group causing a major accident is not common. Merely 0.84% of the examined events showed an erroneous action with a man-related genotype resulting in an

www.manaraa.com

accident. Exclusively technological factors were responsible for the undesirable outcome in only 3.78% of the cases, while 7.56% of the events were solely explained by organisational factors. On the other hand, combinations involving a minimum of two groups featured significantly in the dataset. A Man-Technology arrangement appeared in 47.48% of the cases, while a Man-Organisation combination performed in 56.30%. The Technology-Organisation pair figured together in 78.57% of the events. In 47.48% of the cases, the three groups appeared together. Table 6 summarises these results.

Table 6. Macro-analysis (main groups).

Group / Combination	**Frequency***	
	#	**%**
Only Man	02	0.84
Only Technology	09	3.78
Only Organisation	18	7.56
Man-Technology	113	47.48
Man-Organisation	134	56.30
Technology-Organisation	187	78.57
Man-Technology-Organisation	113	47.48

**Events where a single group or combinations appeared.*

There is a close relationship between the design failure genotype and the man group: 72.80% of the erroneous actions (execution errors) were accompanied by a design failure, such as in the case study presented on Table 2. In addition, 62.50% of temporary and permanent person related functions and 74.34% of cognitive functions were connected to design failures.

Also, it is important to notice that the design failure is the most significant single genotype from all three groups, appearing with an incidence of 66.00%, followed by inadequate quality control (60.50%), inadequate task allocation (60.10%) and equipment failure (55.00%). Despite the significance of these further contributing factors, which can be used in future studies to improve the organisation of work and disclose operational strategies, the following discussion will focus on the design failure genotype features and connections revealed by the statistical analysis.

www.manaraa.com

4. Discussion

4.1 Improving robustness of system design

Design failures were detected in 157 of the 238 major accidents included in the MATA-D, clearly emphasising the need for further developments in design verification schemes. These deficiencies are examples of embedded failures in the system design, which can stay dormant for many years before aligning with human errors, technology issues and other organisational problems to result in a serious occurrence. The failures related with the design of the Fukushima nuclear power plant, such as insufficient tsunami defences combined with the lack of flood protection for batteries, which caused the loss of DC power, remained dormant for decades. Similarly, icing problems of the original speed sensors in the Airbus 330 airplane persisted for approximately 8 years before triggering the catastrophic Rio-Paris flight crash in 2009. Although these design flaw examples could be promptly addressed (before the alignment of the holes in the Figure 1), the lack of a robust dataset containing useful information about the multifaceted interaction between human factors, technology and organisation in complex systems may be preventing standards and regulations from addressing the human performance problem in earlier stages of the lifecycle of engineering systems, such as design, in a structured way. The MATA-D construction intends to break this tendency, being composed by major accidents from high-technology industries to create means of analysing this kind of catastrophic events. Also, major accidents are notably rare events, and the wide-ranging taxonomy used to classify events in the MATA-D allows the accumulation of data from several industrial sectors to perform a deeper analysis and disclose early contributors and significant tendencies leading to human errors.

Other studies were able to identify this relationship between human errors, technology and organisational issues. Bellamy et al. (2013) analysed 118 incidents involving loss of containment in Dutch Seveso plants and identified that 59% of the failures to use/operate a safety barrier were associated with human errors. Despite the application of a different classification system for human errors and the inclusion of events with minor consequences (only 9 out of 118 events were major accidents reportable under Seveso II Directive), these figures might well be related with the present study findings, in which 57.14% of the 238 major industrial accidents were found to have human contributing causes, as reflected in the “man” category statistics.

www.manaraa.com

The comparison of single group accidents with the statistics for at least two simultaneous groups on Table 6 confirms that high-technology systems require a complex interaction of multiple failures in order to produce a major accident. It is important to notice that not only a number of barriers need to be breached, but it also has to interact in a very particular way. This makes the prediction of all design interactions and responses to human, technology and organisational events virtually impossible, highlighting the importance of developing design verification schemes to raise the awareness level of designers relating to major accidents. Therefore, providing some straightforward information based on the most common interactions occurring in complex accidents may be of assistance. The relationship between design failures and human factors indicates that the design damage tolerance criteria must be tested against specific human-related factors disclosed by this research. The direct association of execution errors and cognitive functions with design problems is a valuable finding, demonstrating how design failures can deeply influence human behaviour.

Design failures particularly appear to trigger failures in the human capacity to interpret system status (wrong reasoning and faulty diagnosis), enable potential observation misses and cause some execution errors (sequence, timing and type).

Based on these findings, an effective design review process should carefully address circumstances where some system analysis/diagnosis, interpretation or hypothesis formulations are required before taking an action. The common man, technology and organisation interfaces discussed indicate that it is likely that cues, measurements or information originally intended to lead to a human action have a substantial probability of being missed, an effect explained by some specific cognitive functions (inferences, generalisations or deductions) highlighted by this study.

The aim of the review would be to improve system design by making it responsive to common active failures translated as human erroneous actions, such as omissions; jumping forward a required action; performing a premature, delayed or wrong action; and performing a movement in the wrong direction, with inadequate speed or magnitude. Of course these operators' "action failures" occur in a greater frequency than accidents, and should be considered customary, or part of a non-mechanic behaviour. Consequently, human performance will vary, and it seems that addressing design shortcomings which can affect human behaviour, by learning from major accidents in an informed and structured way, is a reasonable path to reduce major accidents and tackle the genesis of human errors.

www.manaraa.com

4.2 Using the MATA-D for a design review process: an example

One suitable example of effective design improvement approach would be to apply a design review process which considers the connections between human erroneous actions, cognitive functions and design failures highlighted during this study.

The role of the proposed review process is to identify and correct design imperfections that could lead to major accidents. Primarily, due to the complexities of high-technology systems, it is important to bear in mind that one reviewer is unlikely to hold all necessary knowledge to assess all design disciplines and aspects (system functionalities, materials, mechanics, structure, fabrication methods, electrics, chemistry, corrosion protection, risk, compliance etc.). The person in charge should be able to form a team, identifying and engaging with experts in the respective fields (face-to-face meetings), whether or not they are directly involved in the business. Designers, manufacturers, constructors and operators, for instance, are obvious interested parties, but referring to external parties, such as associations, academic institutions and regulatory bodies, will also aggregate significant value to the group task, being "time" the key constraint to be managed during this phase.

In summary, the first step would be to *(i)* identify and rank the safety critical elements (SCE) within the installation. One helpful definition of SCEs is found in the UK Safety Case Regulations (2005), in which the term is defined as any part of an installation whose failure could cause or contribute to a major accident, or elements designed to prevent or limit the effect of a major accident. Considering the wide range of high-technology installations encompassed by the MATA-D (e.g. oil and gas, nuclear plants and aviation), the SCEs list will vary enormously from facility to facility, depending on the industrial segment assessed. Then, *(ii)* the information associated with the critical elements (e.g. material and functionalities description, conceptual and detailed design, fabrication and installation drawings and process and instrumentation diagrams) are used to disclose the relevant human tasks, and *(iii)* the identified operations would be tested against the basic execution errors disclosed by this study (i.e. omissions; jumping forward a required action; performing a premature, delayed or wrong action; and performing a movement in the wrong direction, with inadequate speed or magnitude), to identify undesirable effects affecting the critical elements documented in step *(i)*. Next stage would involve *(iv)* the assessment of indications intended to trigger human actions, such as cues, measurements and displays. The possibility of missing them, as discussed in previous sections, should prompt deep

www.manaraa.com

consideration about the alternative measures in place (e.g. redundancy, double-check, automatic shut-down, supervisor intervention) to provoke human responsiveness. The last review step would comprise the *(v)* analysis of complex tasks, which can be defined as the ones requiring observation of signals, its correct interpretation and system diagnosis.

The mental modelling is inherent to the worker's level of knowledge, the information available and the work environment/situation, among other factors, thus the matter of a human inadequate reasoning while evaluating relevant conditions linked to critical elements must be considered in the review. Although this may seem, at first glance, an excessively challenging task to be undertaken by the design reviewer, the MATA-D results, which indicate specific mechanisms leading to poor interpretations, can be used to build a systematic assessment process. The available inputs to diagnose the undesirable condition should be listed and evaluated, in order to identify where: a) information (e.g. instructions, codes & standards, manuals, signals, communication); b) knowledge (e.g. level of training, education and engineering practice) and c) the work situation (e.g. adverse ambient conditions, irregular working hours, and inadequate work place layout) are likely to induce inferences, generalisations or deductions which can lead to invalid results.

Also, most of the industrial fields allow the designers to choose among a wide range of standards and protocols as an input to design. Thus, compliance verification is similarly a significant method to detect information imperfections, i.e. if the engineering best practices for the existing condition are being applied. The usage of codes and standards which consider human factors as well as the disclosed interactions should be preferred.

Consequently, this design review process should be able to identify possible blind spots and reflect a "design clarity" degree, indicating if the expected functions defined in the conceptual phase are thoroughly satisfied during the earlier stages of the installation lifecycle.

5. Conclusions

5.1 A new method to apply past accidents lessons to design reviews

Learning from past accidents is essential to minimise the possibility of undesirable events recurring, but this is not a trivial task. The particular sequence of events resulting in a serious accident is multidimensional and highly associated with the perfect alignment of

www.manaraa.com

very specific circumstances within a work environment. Consequently, limited learning is likely to arise from the analysis of a single event or even a few accidents, justifying the need for a broad comprehensive understanding of the common features and mechanisms leading to human error, which is the aim of the large major accidents collection.

A new accident dataset, created from detailed investigation reports and using a classification that admits events from different industries, was then introduced.

This work also described some advantageous findings for designers and practitioners who deal with major hazard control, in the sense that it is essential to take human error into account during design. Accordingly, improved insight into erroneous actions and influencing factors was revealed, as the vast collection of real-life accidents (i.e. 238) presented relevant relationships between man, technology and organisation and disclosed common patterns within disasters from different industrial segments.

Specific human factors to be addressed in a design review were then presented in the discussion section guidelines, reducing the burden and the time required to apply extensive human error lists to predicted tasks or complicated methodologies during the development of new projects. This approach, due to its simplicity, can be easily adapted to current design review processes, effectively raising awareness for the development of strategies to minimise human error through design.

The MATA-D includes valuable lessons from several high-technology industries, such as upstream, refining, aviation and nuclear, involving specialists from different fields and providing common input to major hazard control strategies. This new dataset can be used for any application requiring technical input from past major accidents.

6. Acknowledgements

This study was partially funded by CAPES (Proc. nº 5959/13-6).

www.manaraa.com

Part II

Major accidents data classification and analysis, human errors understanding and graphical representations

www.manaraa.com

Chapter 2: Learning from major accidents: graphical representation and analysis of multi-attribute events to enhance risk communication

Overview

Chapter's 2 key feature is the analysis of the MATA-D dataset developed in the previous chapter, with the support of adequate mathematical methods. Recognising that major accidents are complex, multi-attribute events, originated from the interactions between intricate systems, cutting-edge technologies and human factors, the purpose is now to reduce the high-dimensionality of the data captured by the proprietary dataset, in order to overcome barriers to learn from major accidents and enable stakeholders to fully understand and communicate risk.

Perspectives on learning from disasters have been lately discussed, generally suggesting that lessons from undesirable events have not been fully understood or implemented, especially regarding high-technology systems. Schröder-Hinrichs et al. (2012) examined some widely-known maritime accidents, and argued that catastrophic sinking events such as the Titanic and the Costa Concordia seem to encompass the same underlying human and organisational factors, despite the 100-year distance separating them. Likewise, Le Coze (2013) compared a group of major accidents occurred in the first decade of the 21st century with events in the 70s and 80s (e.g. nuclear: Chernobyl vs. Fukushima; offshore production: Piper Alpha vs. Deepwater Horizon; aviation: Tenerife vs. Rio-Paris) arguing that similarities among these accidents produced a *déjà vu* feeling. Biases associated with the attribution of excessive weight to the human error contribution to accidents and public pressure towards blame allocation (Hopkins, 2006, Johnson, 2008) are some of the issues that can also inhibit a favourable learning environment.

The general strategy used in the current research to convey risk information involves the manipulation of integrated data to display similarities (or shared tendencies) in a particular collection of major accidents. With this purpose, an artificial neural network approach, i.e. self-organising maps - SOM (Kohonen, 2001), was applied to the MATA-D dataset, revealing common patterns and disclosing significant features. Due to the intrinsic characteristics of the SOM algorithm, the chosen approach successfully reduced the dataset dimensionality without data loss, fully preserving the input data in a 2-D matrix output. This is particularly useful to enable interpretations of the dataset beyond the mere presence or absence of specific contributing factors.

www.manaraa.com

The chosen method allowed a comprehensive analysis of the interactions among contributors, harmonising complex tendencies leading to major accidents with simple and straightforward visual representations. The contributing factors and their interactions were presented in a convenient graphical alternative, producing further insight into the conditions leading to major accidents and supporting a novel and comprehensive ‘‘learning from accidents” experience. Accident examples illustrate some of the tendencies disclosed by the SOM. The intention is to provide additional means to help stakeholders absorb risk information, thus improving risk communication and enhancing risk perception.

www.manaraa.com

Learning from major accidents: Graphical representation and analysis of multi-attribute events to enhance risk communication[2]

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

[a] Institute for Risk and Uncertainty, University of Liverpool, Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom
[b] Institute for Risk and Reliability, Leibniz Universität Hannover, Callinstr. 34, 30167 Hannover, Germany
[c] National Agency for Petroleum, Natural Gas and Biofuels (ANP), Av. Rio Branco, 65, CEP: 20090-004, Centro, Rio de Janeiro-RJ, Brazil
[*] Corresponding author at: Office G79 Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom.

1. Introduction

1.1 Perspectives on learning from accidents and understanding human errors

Major accidents have a multidimensional nature, arising from a wide range of contributing factors interacting in a seemingly random and sophisticated fashion to result in large-scale technological disasters. Many of these contributing factors are developed since the design conception, comprising of technical and non-technical issues and ultimately including the alluring influence of human errors.

The term "human error" has been coined in several different fields such as engineering, economics, psychology, design, management and sociology, with numerous interpretations and diverse objectives. Although most of the researchers and practitioners would (probably!) agree that human error can be generally understood as a failure to perform a certain task, the indiscriminate usage of the label "human error" to define some sort of human underperformance can be highly controversial. Hollnagel (1993, 1998), Woods et al. (2010) and Dekker (2014) claim that errors are best seen as a judgment in hindsight, or an attribution made about the behaviour of people after an event, being a quite misleading term, of limited practical use and nothing more than a tag. Conversely, Reason (1990, 2013) favoured the usage of the nomenclature, describing three necessary features to define human error: (i) plans; (ii) actions (or omissions); and (iii) consequences, surrounded by two situational factors: intention and absence of chance interference. Therefore, according to Reason, human errors can be acknowledged when an intention is reflected in a planned

[2] Original publication in Moura, R. et al., 2017. Learning from major accidents: Graphical representation and analysis of multi-attribute events to enhance risk communication, *Safety Science 99*: 58-70, DOI 10.1016/j.ssci.2017.03.005.

www.manaraa.com

sequence of actions which fails to accomplish its projected outcome, with observable consequences. The plan can be flawed or the action(s) can be imperfect, and some chance agency (e.g. an act of God or *force majeure*) is not recognisable.

The understanding of human error is typically encapsulated by a wider concept entitled "Human Factors". This applied discipline has grown significantly after World War II, where the consideration of the human aspect was deemed necessary for achieving a realistic reliability assessment (Swain and Guttman, 1983; Dhillon, 1986). Since then, the multi-disciplinary nature of the human factors studies, which focus on the relationship between humans, tasks, technologies, organisations and the surrounding environment, allowed for some variances among the views and needs of engineers, psychologists, sociologists, managers and the general public. Hollnagel (1998) suggested that the original engineering and design approach aimed at analysing humans as components, in order to assign a human failure probability (or human error likelihood) to risk and safety assessments. Adopting a different perspective, psychologists attempted to understand mental processes and awareness mechanisms leading to erroneous actions, while sociologists were looking for flaws in the socio-technical system, usually attributing errors to management and organisational shortcomings.

But how do stakeholders see errors, especially after a major accident? Two common attitudes towards human errors were distinguished by Dekker (2014). The first one is what he called the "old view", which considers errors as causes. On the other hand, the "new view" regards human errors as consequences of accidents, effects or symptoms of some sort of organisational shortcoming. Hollnagel (1998) highlighted that human error has been seen as the cause of events (when accidents are said to be due to the human intervention), the event itself (when an action, e.g. pressing the wrong button, is said to be a human error) or the consequences (the outcome of the action is said to be an error, e.g. the driver made the error of fuelling a petrol-fuelled car with diesel, inferring a car malfunction).

The general approach to human errors and the level of comprehension of human factors will deeply affect the process of learning from accidents. Major events are likely to trigger exacerbated societal reactions and impair communication channels, demanding an immediate and strong response from industry and authorities to ensure accountability. In those cases, acknowledging that humans are pivotal in any engineered system, the temptation to expose a scapegoat may limit the search to individuals who made errors

www.manaraa.com

throughout the lifecycle of the industrial process. If the concept of errors as causes of events prevails, the investigation will aim at the culprits' exposure, the blame allocation and the imposition of penalties, and thus valuable lessons regarding organisational and technological aspects can be lost. Hopkins (2006) and Johnson (2008), discusses the tension between the requirement to learn as much as possible from events and the public pressure, highlighting that fear of litigation can act as an important barrier to learning the lessons from accidents.

That is why Reason's characterisation of human errors turns out to be extremely beneficial, tying up two loose ends: firstly, the need for recognition and common understanding of human error, a deeply rooted concept in both technical and general public reality, serving as a useful bridge between the two worlds; and secondly, a clear and convenient definition, focused on the internal and external characteristics of the analysed subject and on the genesis of error. This approach allows for the search for profounder issues related to accidents and can help to reduce the knowledge gap among authorities, the general public and wider stakeholder groups, in order to accomplish an improved learning environment.

1.2 Recent catastrophes in complex, multi-attribute accidents

The relevance of human factors and the impact of human errors in industrial accidents were extensively emphasised by contemporary studies. Human error was regarded as a major contributor to more than 70% of commercial airplane hull-loss accidents (Graeber, 1999). Correspondingly, according to Leveson (2004), operator errors can be considered the cause for 70–80% of accidents, given recurrent deviations between established practice and normative procedures. Considering the cost issue, a review by the United Kingdom Protection and Indemnity (P&I) Club indicated that US$541 million per year is lost by the marine industry due to human errors (Dhillion, 2007).

Major accidents have the potential to capture the public's attention and demand strong responses from authorities. The Fukushima accident in March 2011 has triggered a considerable shift in the way the nuclear industry was seen by governments and the general public.

Mr. Kiyoshi Kurokawa, the chairman of the independent investigation commission for the Fukushima nuclear accident, stated in the official report that the tsunami and technical

www.manaraa.com

issues were not the sole reasons for the tragedy, declaring that human factors as well as deeper Japanese cultural issues were vital contributors (Kurokawa et al, 2012): *"What must be admitted – very painfully – is that this was a disaster 'Made in Japan'. Its fundamental causes are to be found in the ingrained conventions of Japanese culture (…). Therefore, we conclude that the accident was clearly 'man-made'".*

This wide-reaching accident was drawn into the international media's spotlight. In a global perspective, it has driven the German government to immediately shut-down eight reactors (their restart is highly unlikely) and reject the construction of new units (Schneider et al., 2012). Thus, the phasing-out of nuclear plants and the replacement with renewables or other energy sources in Germany seems to be irreversible. Also, the former Republic of China's president Ma Ying-Jeou decided to limit the operating lifespan of nuclear power plants to 40 years, and declared that the continuation of the ongoing construction of a new nuclear power unit in Taiwan would be decided by a public referendum (Ishikawa, 2015). It appears that the political climate due to the public's perception of risk is highly unfavourable to nuclear power, especially after Fukushima.

Recently, prosecutors called for the death penalty for the captain of the MV Sewol, a South Korean ferry that sank in April 2014 and left 304 fatalities, most of them pupils on a school trip. He was found guilty and sentenced to 36 years in prison, and 14 crewmembers were jailed from 9 to 25 years. Families and protesters affirmed that lessons were not learnt from a series of previous accidents (BBC, 2014).

These are examples, to name but a few, of how the process of learning from accidents can be compromised if risks are not adequately communicated, due to the natural distance between experts' views and the public's perception.

From an engineering perspective, the highly complex interaction between operators, technology and organisations is a recurring subject arising from investigations involving major events. The *Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile* (2011) official report on the AF-447 Rio-Paris Airbus A-330 accident on 1st June 2009 acknowledged an apparently simple equipment defect (icing of the Pitot probes) resulting from a design failure, which led to some inconsistencies of the flight speed indicators. This deficiency triggered several human-related events (wrong system diagnosis and inappropriate control inputs, among others), ultimately resulting in the airplane hull-loss in

www.manaraa.com

the Atlantic Ocean, with 228 victims. The investigation report also highlighted some intricate factors such as the de-structuring of the task-sharing in the cockpit during the response to the anomalous event, training shortcomings in a predictable flight mode (manual handling of the airplane in high altitudes), and the lack of indication of the airspeed inconsistencies in the flight console, exposing a complex combination of several factors leading to the catastrophe.

These major accident examples, mostly involving up-to-date technologies with numerous systems under normal operation (e.g. Airbus (2016) states that around 1,200 A330 airplanes are operated by over 100 companies, meaning that an aircraft takes off or lands somewhere every 20 seconds!), illustrates the complexity behind erroneous actions, mental models, technology, organisational issues, culture and the environment in high-technology industries. This highly interdisciplinary and intricate setting, including the influence of the utmost public and media attention and the fact that human errors are palpable and a compelling argumentation to explain undesirable events, brings a substantial challenge to stakeholders. How to develop means to learn from multi-attribute events and translate these lessons into an approachable scheme for researchers, practitioners, policymakers and society, in order to communicate and tackle risks appropriately?

Consequently, this work aims to overcome barriers to dealing with complex datasets containing incident/accident information, by means of applying an unsupervised learning neural network approach to a proprietary accident dataset. The Multi-Attribute Technological Accidents Dataset (MATA-D) presented by Moura et al. (2016) will be converted into two-dimensional graphical representations of accidents and their corresponding surrounding factors. The 2-D interfaces will provide innovative means to communicate high-technology risks and to disclose tendencies that could lead to the genesis of errors, facilitating and enhancing interactions among internal stakeholders and the general public.

www.manaraa.com

2. Analysis Method

2.1 Capturing the complexity underlying major accidents: fit for the past, adaptable to the future

The underlying dynamics observed during critical events is so great that some renowned accident causation theorists consider the failures in complex, tightly coupled systems as inevitable (Perrow, 1999), or not prospectively foreseeable (Taleb, 2007). This is due to the acknowledged difficulties to capture and understand all facets of socio-technical systems and all circumstances leading to catastrophes, which pose a challenge to researchers and practitioners. As a result, any method to capture lessons from accidents will have inherent limitations. In this work, a data-based approach which starts from the available information (detailed accounts from major accidents) and uses an artificial neural network process to generate useful knowledge is proposed. The dataset structure is flexible and expandable: new accidents can be added, or prospective analyses can be conducted in order to increase the database.

Other dataset frameworks inspired by novel accidents causality models based on systems theory and system thinking, such as the System-Theoretic Accident Model and Processes (Leveson, 2011), could be used for accident analyses, and the artificial neural network approach presented in this work would be equally applicable. However, the data required to construct a reasonable model based on some new approaches would require accident investigators to have previous knowledge of those approaches and carry out a targeted data collected process to suit the framework. Consequently, it is unlikely that the massive amount of data from early major accident accounts currently available would be immediately adaptable. Even considering a broader, virtually ideal holistic approach, potential influencing factors such as the percentage of profit allocated to safety, the influence of political decisions on industrial segments or the impact of the change of controllers and investors on companies, would not be fully available for earlier accidents, implying a new start point for data collection and thus a drawback to embrace past events. Therefore, the choice of the dataset framework took into account the possibility of starting from the available information reflected on past accounts to generate immediate knowledge. On the contrary, to construct a dataset based on a fully new framework, many years of catastrophic events (fortunately major accidents are rare) would be necessary, and even the most comprehensive model would still hold intrinsic limitations.

www.manaraa.com

Additionally, this study presents an expansion of conventional reductionist models. The focus of the analysis method lies on the examination of the interfaces among contributing factors, instead of specifying root-causes in a classical chain of directly related events. Although accident reports are intended to present a logical explanation to accidents, usually comprising a sequence of events through time, non-linear interactions among contributing factors can be also identified during in-depth investigations, allowing a systemic learning process. Irrespective from the accident causation method used to understand events, it was possible to classify all of them under the common framework in which the dataset was based, as seen on Moura *et al.* (2016).

For example, The Piper Alpha Accident Report (Cullen, 1990) revealed design, construction, management, operational and human factors interfacing in an undesirable fashion to result in 167 fatalities and billions of pounds in property losses in July 1988. The recommendations (106 in total) arising from the report addressed changes to oil & gas offshore facilities, industry, the UK government and trade unions. New legislation (The Safety Case Regulations) was developed after a full review of existing legislative arrangements, progressing from the former prescriptive regime to the current performance-based safety management model. Even the responsibility for safety oversight was transferred from the Department of Energy which used to regulate both revenue collection and safety, to the Health & Safety Executive (Paté-Cornell, 1993).

Therefore, accident narratives arising from detailed investigation processes can give impetus to broader safety improvement measures, and the collective understanding of previous occurrences is able to reveal new interfaces, contribute to a holistic safety understanding and improve stakeholders' risk awareness level.

www.manaraa.com

2.2 The Multi-attribute Technological Accidents Dataset (MATA-D)

Many researchers (e.g. Swain, 1990; International Atomic Energy Agency, 1990; Grabowski, 2009) referred to the lack of reliable data on human performance in high-technology systems and the complications associated with the collection, consistency and interpretation of data.

In addition, most of the near-misses datasets contains condensed descriptions of events, generally limiting the information to direct or immediate causes (e.g. operator failure, equipment defect), due to usual constraints (i.e. time, budget, human resources) to conduct in-depth analysis of inconsequential events. The main shortcoming with non-detailed data is that the context in which workers are placed is usually overlooked. However, it is widely accepted (Reason, 1990; Hollnagel, 1998; Cooper, 1996; Strater, 2000; Dekker, 2014) that the context is actually the central element to be studied, in order to provide a full picture and a better understanding of undesirable events.

The European Safety, Reliability and Data Association (2015) stated that major accident investigations allow for a detailed analysis of preventive and protective systems, as well as the exploration of events and surroundings conditions leading to accidents. In addition, high-impact events usually provide impetus for the application of lessons learned to minimise reoccurrence, as observed in the wake of disasters such as the Texas City Refinery, the offshore production platform Piper Alpha and the Nuclear Power Plant in Fukushima (Fukasawa, 2012; Dahle, 2012). Society's risk perception, the regulatory approach and industry's behaviour towards safety were affected in a global scale by these events.

Although major accidents seem to be one of the finest sources of information available, they are considered to be rare events (Reason, 1997; Taleb, 2007), and the currently available data might not be enough for the application of traditional statistical approaches. Thus, a method to allow the seamless learning process between different industrial sectors is necessary, in order to generate sufficient data for a suitable analysis. Nevertheless, transversal learning is not trivial, due to differences among technologies, industrial jargon and contexts in complex systems. To overcome these issues, the authors developed a major-accident dataset, using a common framework, the Contextual Control Model used as a basis for the Cognitive Reliability and Error Analysis Method (Hollnagel, 1998), to classify

www.manaraa.com

data captured from investigation reports prepared by regulators, investigation commissions, government bodies, insurance companies and industry experts to explain the contributing factors and causes behind major accidents. The framework is comprehensive, containing 53 contributing factors distributed in groups (man, technology and organisation) and subgroups (erroneous actions, specific cognitive functions, temporary and permanent person-related functions; equipment, procedures, temporary and permanent interface; communication, organisation, training, ambient and working conditions). The data structure is represented in Figures 1, 2 and 3. Further information about the decision to develop a new dataset and all the details regarding the creation and content of the Multi-attribute Technological Accidents Dataset (MATA-D) can be found in Moura et al. (2016).

The use of high-consequence accident reports to feed the MATA-D proved to have many benefits. Deep investigations involve internal and external experts in the search for evidence and to disclose contributing factors and relevant interactions between humans, technology and organisations. Therefore, uncertainties associated with the consistency of the input data were reduced, and the selected framework permitted the classification of events from diverse industrial backgrounds under a common taxonomy, making them comparable. Consequently, the MATA-D structure allows for the application of mathematical methods, aiming at the disclosure of common patterns and at the recognition of significant features. This way, the genesis of multi-attribute events can be better understood and communicated.

www.manaraa.com

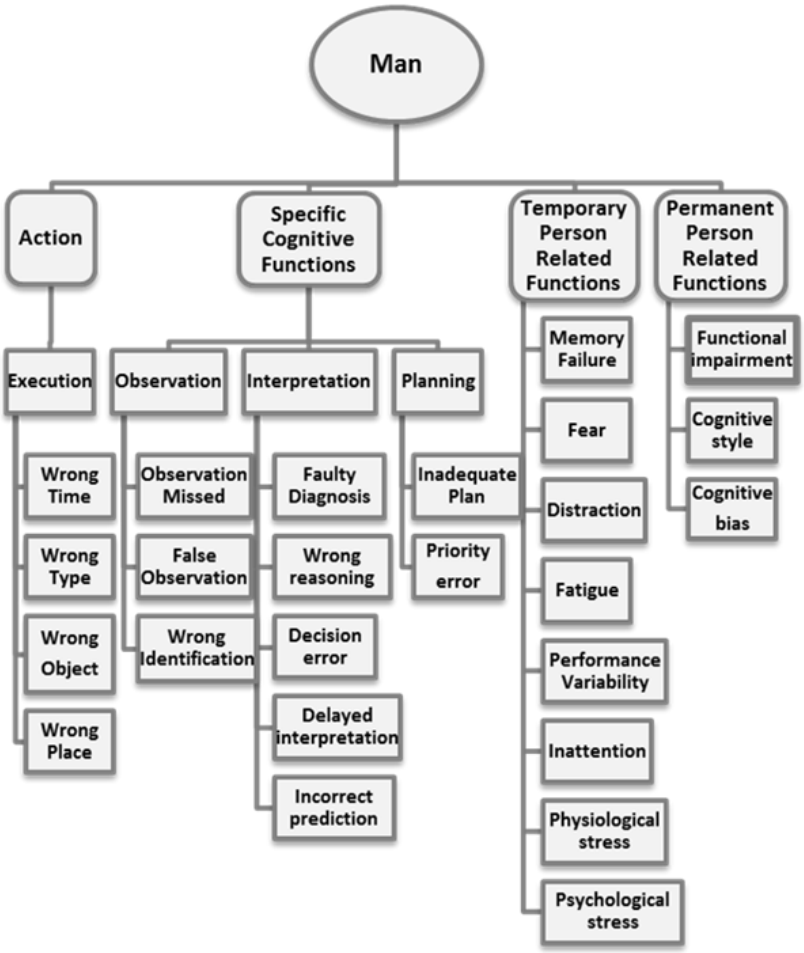

Figure 1. "Man" categorisation, adapted from Hollnagel (1998)

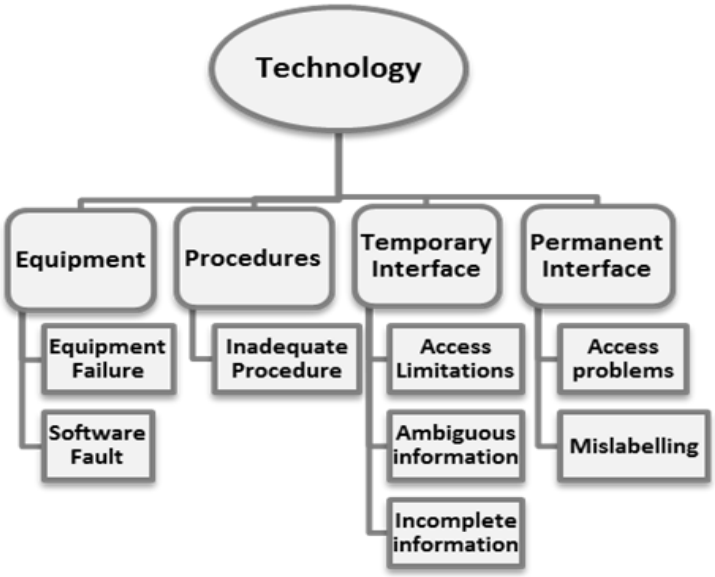

Figure 2. ""Technology" categorisation, adapted from Hollnagel (1998)

www.manaraa.com

Figure 3. "Organisation" categorisation, adapted from Hollnagel (1998)

The dataset includes 238 major accidents from several industrial segments, as detailed in Table 1.

Table 1. MATA-D Accidents distribution by industrial sector, after Moura et al. (2016)

Industrial sector	Accidents	
	#	%
Refinery	39	16.39
Upstream (oil & gas)	37	15.55
Chemicals	29	12.18
Petrochemicals	25	10.50
Nuclear Power Plants	23	09.66
Civil Construction	16	06.72
Terminals & Distribution	15	06.30
Aviation	13	05.46
Gas Processing	09	03.78
Metallurgical industry	07	02.94
Waste Treatment Plant	05	02.10
Food Industry	04	01.68
Others	16	06.72

www.manaraa.com

2.3 The data mining process

The aim of the data mining process is to disclose common structures among accidents and significant features within the major-accident dataset. In this work, making an attempt to go beyond the general statistical analysis presented by Moura et al. (2016), a well-known clustering approach named Self-Organising (or Kohonen) Maps (SOM), developed by Kohonen (1998), is applied to the MATA-D. The objective is to convert the 53-dimensional dataset (a matrix of 238 accidents holding 53 possible contributing factors each) into a low-dimensional (i.e. 2-D) array, enabling the data visualisation and interpretation.

Essentially, the SOM algorithm consists of an initialisation followed by three processes: (i) competition; (ii) cooperation; and (iii) adaptation. The network learning begins with the attribution of arbitrary values for the initial weight vectors. Then, the training starts with the competition process, where the winning output neuron (best matching node) is the one which minimises the Euclidean Distance $\|\vec{x} - \overrightarrow{m_i}\|$ for each input pattern (Eq. (1)). After defining the output winner, the cooperation process consists of the application of a neighbourhood function (usually the Gaussian function Eq. (2)) to define the spatial influence of the best matching unit upon the neighbour neurons. The last process is the adaptation one, where the weights of all neighbour neurons are sequentially updated while both the learning rate and the neighbourhood function decrease with time, following the Eq. (3). This sequence is repeated (through iterations) until the map converges (Kohonen,2001; Andreev and Argyrou, 2011).

$$v(t) = \arg\min_{i\epsilon\Omega}\|x(t) - m_i(t)\| \quad (1)$$

$$h_{ci}(t) = \propto(t) \cdot \exp\left(\frac{\|r_c - r_i\|^2}{2\sigma^2(t)}\right) \quad (2)$$

$$m(t+1) = m_i(t) + \propto(t) h_{ci}(t)[x(t) - m_i(t)] \quad (3)$$

Kohonen (2013) has shown that a variation of the updating rule (Eq. 3) would be useful to eliminate convergence complications and generate steadier asymptotic m_i values. Therefore, a batch-learning version of SOM (Batch-SOM) was revealed for practical applications, in order to generate more consistent outcomes. Eq. (4) shows the Batch-SOM updating rule developed by Kohonen.

$$m_i^* = \frac{\sum_j n_j h_{ji} \overline{x_j}}{\sum_j n_j h_{ji}} \quad (4)$$

www.manaraa.com

With the new update rule (Eq. 4), the definition of a learning parameter $\propto$ is no longer necessary, as the batch-learning implies that the codevectors are being updated once, rather than in a recursive fashion. Each best matching node m_i^* represents the centroid of an influence region defined by $\overline{x_j}$ (the mean value of a group of input vectors *x(t)*), the neighbourhood function h_{ji} and the number n_j of samples.

The representation of the dataset (a 53-dimension input space, Figure 4) in a 2-D topographic map shows the MATA-D events organised by similarity, i.e. accidents with analogous contributing factors will be close to each other (e.g. Figure 5). This enables the generation of clusters which can be analysed in an integrated way, revealing tendencies within a group of major accidents.

One of the most important features of the SOM's learning process is that it comprises an unsupervised learning process, dismissing the need for any pre-classification, pre-selection of the number of clusters or the definition of main/leading factors (Kohonen et al, 1996). Consequently, the data mining process is not affected by external parameters, avoiding potentially biased concepts regarding the main factors influencing accidents and potentially leading to human errors.

3. Results

3.1 Clustering Results

The application of the SOM algorithm brought together accidents by resemblance – the more similar the accidents are, the closer they are positioned in the output space. Figures 4 and 5 show the input space (a matrix 238 x 53) and the output space (a 2-D representation of the events).

$$\begin{matrix} A_{1.1} & \cdots & A_{1.53} \\ \vdots & \ddots & \vdots \\ A_{238.1} & \cdots & A_{238.53} \end{matrix}$$

Figure 4. Input Space: A dataset containing 238 samples x 53 features

www.manaraa.com

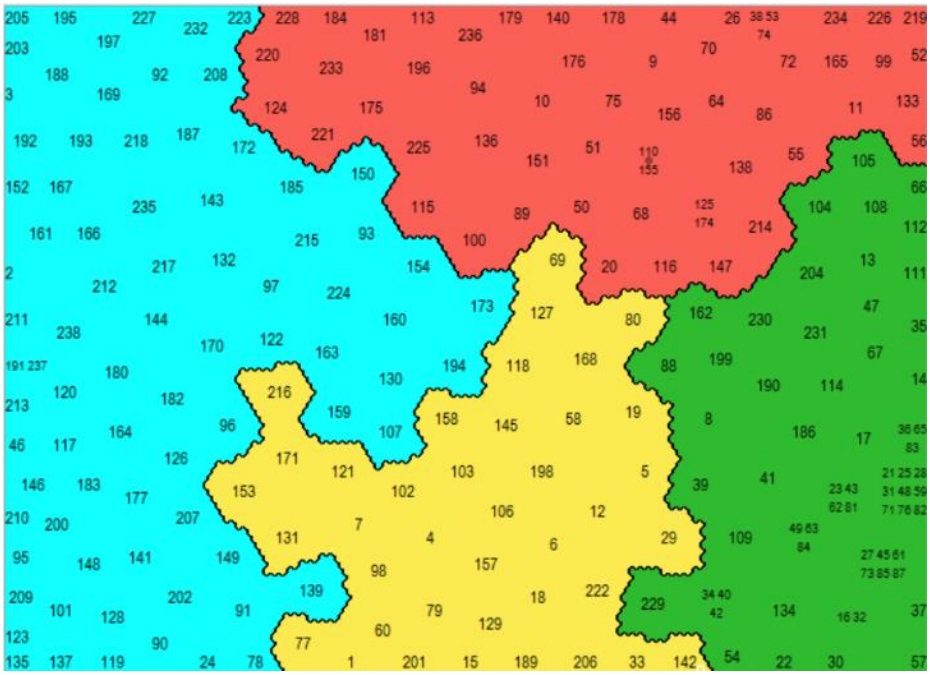

Figure 5. Output Space: A reorganised 2-D grid

Maps were generated from the 238 records with 53 possible attributes each. The output space was trained with 111 batches, and the width of the kernel (the radius of the Gaussian neighbourhood - Eq. (2)) was 0.41. This value is set to be the smallest to form meaningful clusters while maintaining the best possible representation of data differences, with attribute values being averaged less. Maps were produced by the expert version of Viscovery SOMine® software, in order to enhance graphical visualisation.

The Viscovery® SOMine software has a clustering quality indicator, a histogram which classifies conceivable groupings by attributing an index for each possible clustering arrangement. The 4-cluster final map attained the highest quality measure (Figure 6) and thus was adopted as a useful arrangement for further interpretation.

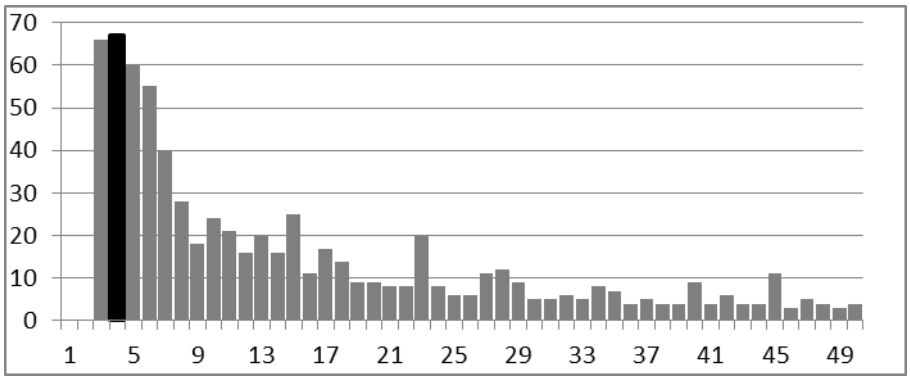

Figure 6. Cluster Quality Indicator (Viscovery SOMine®)

www.manaraa.com

Other analysis methods can be used to evaluate the quality of the map, such as the error quantisation and frequency computation. For the current application, quantisation errors were very small, and both the data frequency and the error quantisation were evenly distributed throughout the map, indicating that the network was well-trained and the mapping quality is good.

Tables 2 and 3 present the clusters' statistical results. The application of the SOM strengths the contribution of many factors and provide stimulus to further interpretation. Example are Wrong Place and Inadequate Task Allocation in Cluster 1; Decision Error and Adverse Ambient Conditions in Cluster 2; Wrong Time and Design Failure in Cluster 3; and Equipment Failure in Cluster 4. Factors which original contributions were scattered in the overall dataset are now visible, case of Social Pressure in Cluster 1 (from 7.1% to 17.5%), Adverse Ambient Conditions in Cluster 2 (from 7.1% to 14%) and Priority Error in Cluster 3 (from 7.1% to 15.4%). Other factors (e.g. Wrong Object) did not show a decisive alteration between the overall and the clustering frequency and should not be taken into account when interpreting the clustering, as they did not have an important role in the formation of the groupings. These are not statistically significant to the clustering.

Table 2. Clusters' Features

Cluster	Events #	Contributing Factors #				
		Min	Max	Mean	Median	Mode
C1	80	04	24	9.62	09	09
C2	57	01	10	4.56	04	02
C3	39	05	22	8.92	08	08
C4	62	01	06	3.10	03	02

Table 3. Overall dataset statistics (After Moura et al., 2016) and new clustering statistics

		Overall	C 1	C 2	C 3	C 4
	Accidents #	238	80	57	39	62
Erroneous Actions	Wrong Time	14.7%	13.8%	10.5%	41.0%	3.2%
	Wrong Type	11.8%	11.3%	7.0%	30.8%	4.8%
	Wrong Object	2.5%	3.7%	3.5%	2.6%	0.0%
	Wrong Place	31.5%	52.5%	36.8%	12.8%	11.3%
Observation	Observation Missed	15.5%	20.0%	12.3%	23.1%	8.1%
	False Observation	3.4%	6.3%	3.5%	0.0%	1.6%
	Wrong Identification	2.5%	5.0%	0.0%	5.1%	0.0%

www.manaraa.com

Interpretation	Faulty diagnosis	13.0%	26.3%	8.8%	12.8%	0.0%
	Wrong reasoning	11.3%	20.0%	1.8%	25.6%	0.0%
	Decision error	9.2%	5.0%	17.5%	17.9%	1.6%
	Delayed interpretation	4.6%	8.7%	1.8%	7.7%	0.0%
	Incorrect prediction	3.8%	7.5%	1.8%	2.6%	1.6%
Planning	Inadequate plan	23.0%	10.0%	7.0%	25.6%	1.6%
	Priority error	7.1%	6.3%	8.8%	15.4%	1.6%
Temporary Person-related Functions	Memory failure	0.9%	1.3%	1.8%	0.0%	0.0%
	Fear	2.1%	1.3%	0.0%	5.1%	3.2%
	Distraction	5.9%	11.3%	3.5%	7.7%	0.0%
	Fatigue	2.9%	7.5%	0.0%	2.6%	0.0%
	Performance Variability	1.4%	5.0%	1.8%	0.0%	0.0%
	Inattention	2.1%	2.5%	0.0%	5.1%	1.6%
	Physiological stress	0.8%	1.3%	1.8%	0.0%	0.0%
	Psychological stress	2.9%	5.0%	1.8%	2.6%	1.6%
Permanent Person-related Functions	Functional impairment	0.4%	0.0%	0.0%	2.6%	0.0%
	Cognitive Style	0.0%	0.0%	0.0%	0.0%	0.0%
	Cognitive bias	7.1%	15.0%	1.8%	10.3%	0.0%
Equipment Failure	Equipment failure	55.0%	33.8%	22.8%	94.9%	87.1%
	Software fault	2.5%	6.3%	0.0%	2.6%	0.0%
Procedures	Inadequate procedure	44.1%	78.7%	42.1%	38.5%	4.8%
Temporary Interface Problems	Access limitations	1.3%	3.7%	0.0%	0.0%	0.0%
	Ambiguous information	2.5%	5.0%	0.0%	5.1%	0.0%
	Incomplete information	17.6%	36.2%	7.0%	20.5%	1.6%
Permanent Interface Problems	Access problems	1.7%	3.7%	0.0%	2.6%	0.0%
	Mislabelling	1.7%	2.5%	1.8%	0.0%	1.6%
Communication	Communication failure	10.5%	16.3%	5.3%	20.5%	1.6%
	Missing information	20.6%	37.5%	14.0%	15.4%	8.1%
Organisation	Maintenance failure	34.9%	56.3%	14.0%	33.3%	27.4%
	Inadeq. quality control	60.5%	81.3%	24.6%	79.5%	56.5%
	Management problem	9.2%	12.5%	5.3%	23.1%	0.0%
	Design failure	66.0%	85.0%	50.9%	87.2%	41.9%
	Inadeq. task allocation	60.1%	95.0%	68.4%	48.7%	14.5%
	Social pressure	7.1%	17.5%	3.5%	0.0%	1.6%
Training	Insufficient skills	36.1%	56.3%	12.3%	76.9%	6.5%
	Insufficient knowledge	35.3%	60.0%	17.5%	56.4%	6.5%
Ambient Conditions	Temperature	1.3%	1.3%	0.0%	2.6%	1.6%
	Sound	0.0%	0.0%	0.0%	0.0%	0.0%
	Humidity	0.0%	0.0%	0.0%	0.0%	0.0%
	Illumination	0.8%	1.3%	1.8%	0.0%	0.0%
	Other	0.0%	0.0%	0.0%	0.0%	0.0%
	Adverse amb. condition	7.1%	2.5%	14.0%	10.3%	4.8%
Working Conditions	Excessive demand	5.5%	6.3%	8.8%	5.1%	1.6%
	Poor workplace layout	2.5%	1.3%	7.0%	2.6%	0.0%
	Inadeq. team support	3.4%	6.3%	0.0%	7.7%	0.0%
	Irregular working hours	3.8%	10.0%	1.8%	0.0%	0.0%

www.manaraa.com

3.2 Clusters Description

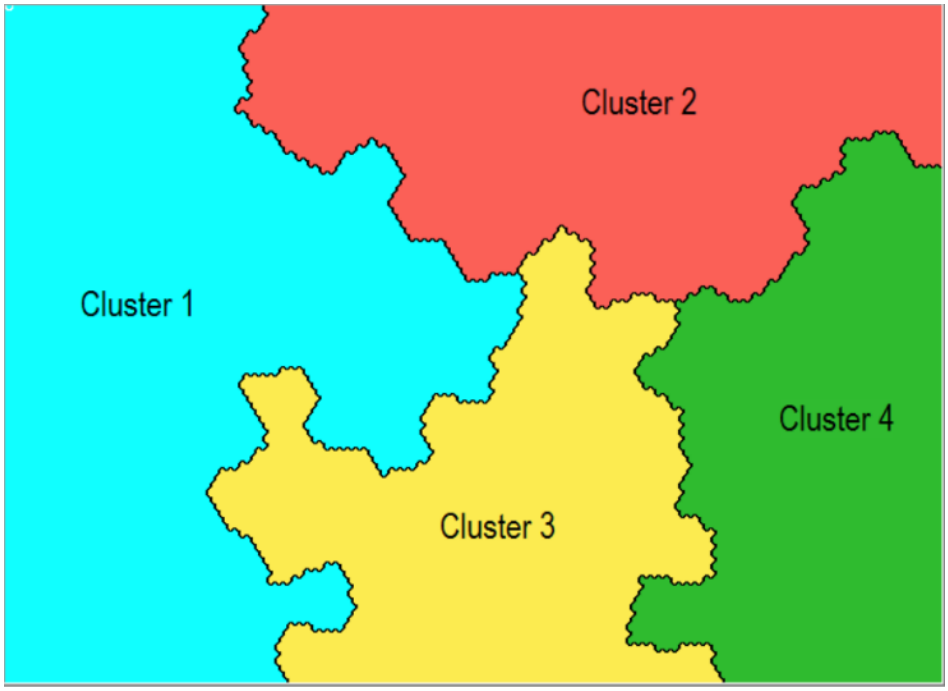

Figure 7. Clusters Identification

Figure 7 presents the accidents positioned by similarity in the grid, separated in 4 (four) clusters with different dominating characteristics.

Cluster 1 is the largest single group, covering 80 accidents which encloses between 4 and 24 contributing factors. It is largely dominated by Inadequate Task Allocation (95.0%), when the organisation of work is lacking due to deficient scheduling, task planning or poor rules and principles. Additionally, accidents within this cluster were deeply influenced by Design Failure (85.0%) and Inadequate Quality Control (81.3%). From an organisational perspective, factors such as Insufficient Knowledge (60.0%), Maintenance Failure (56.6%) and Missing Information (37.5%) were also significant. The most important technological contributor was the Inadequate Procedure factor with 78.7% of incidence, followed by Incomplete Information (36.2%). From a human factors perspective, erroneous actions labelled as Wrong Place (when actions in a planned sequence are omitted/skipped, repeated, reversed or when an unnecessary action is taken) were in 52.5% of the cluster, mainly accompanied by interpretation issues, specially Faulty Diagnosis, with 26.3% of incidence. Observation Missed and Wrong Reasoning were also noteworthy human-related factors, both appearing in 20% of the cluster.

www.manaraa.com

Cluster 2 grouped 57 accidents, all varying from 1 to 10 contributing factors and with low mean, median and mode figures (Table 2). Organisational factors such as Inadequate Task Allocation (68.4%) and Design Failure (50.9%), as well as the technological factor Inadequate Procedure (42.1%) were the most frequent in this grouping. Some hostile ambient and working conditions were highlighted, with Adverse Ambient Conditions (14.0%) and Inadequate Workplace Layout (7.0%) standing above the overall data distribution. Decision Error (17.5%) was a noticeable human contributor, highlighting cases where workers were unable to make a decision or have made the wrong choice among possible alternatives.

The leading factor for Cluster 3, which contains 39 major accidents, is a technological aspect labelled Equipment Failure, populating 94.9% of the grouping area. This cluster also presented very strong organisational factors, as Design Failure (87.2%), Insufficient Skills (76.9%), Management Problem (23.10%) and Communication Failure (20.5%) attained their maximum values in this cluster, being also the Inadequate Quality Control factor very relevant, with 79.5% of incidence. The human factors incidence is quite substantial, with actions occurring at the wrong time (41.0%) or being of the wrong type (30.8%). These cases include omitted, premature or delayed actions, as well as using disproportionate force, magnitude, speed or moving in the wrong direction. These human erroneous actions were accompanied by all three levels of cognitive functions, i.e. observation, represented by Observation Missed (23.1%), interpretation, with Wrong Reasoning (25.6%) and Decision Error (17.9%); and planning, with both Inadequate Plan (25.6%) and Priority Error (15.4%) attaining their maximum incidence. It is worth to notice that the number of contributing factors for each event in this cluster fluctuated from 5 to 22, with a mean of approximately 9 and median and mode of 8.

Cluster 4 contains 62 events, each one encompassing 1 to 6 contributing factors, recording a mean of approximately 3, median of 3 and a mode of 2 features. For most of the accidents in this cluster (i.e. 87.1%), an Equipment Failure was the most frequent contributor to accidents, followed by Inadequate Quality Control (56.5%), Design Failure (41.9%) and Maintenance Failure (41.9%).

Figures 8 to 21 show the self-organising maps for individual features. These figures detail how individual characteristics were distributed in the map after the application of the SOM algorithm. Colder colours (tending to blue) mean the absence of a feature, while warmer

www.manaraa.com

colours (tending to red) mean the presence of a contributing factor. Multiple intersections of warm colours in different individual SOM maps can be interpreted as an interface/relationship.

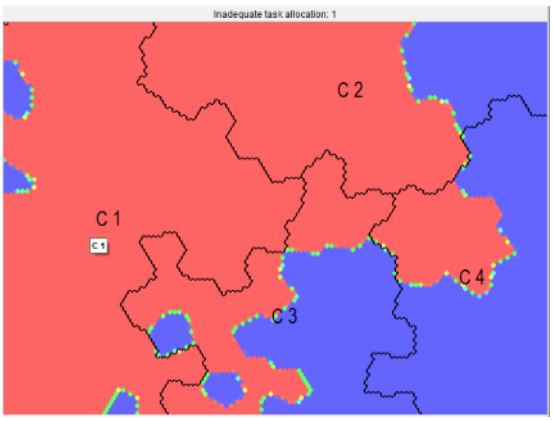

Figure 8. Inadequate Task Allocation SOM

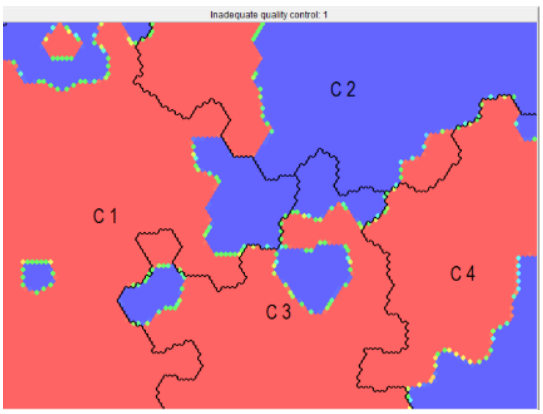

Figure 9. Inadequate Quality Control SOM

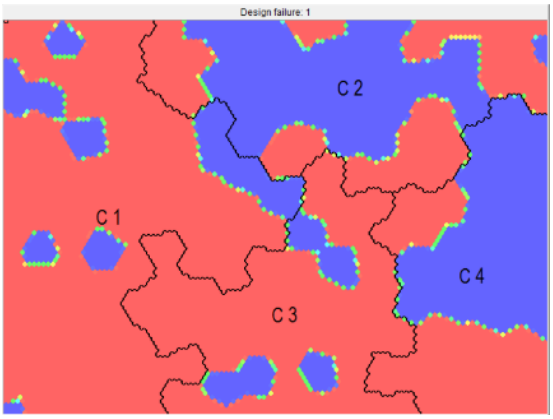

Figure 10. Design Failure SOM

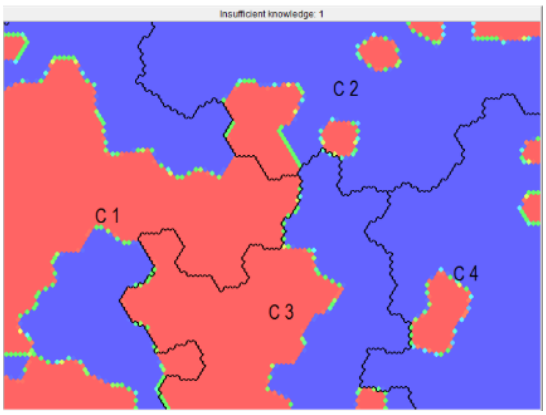

Figure 11. Insufficient Knowledge SOM

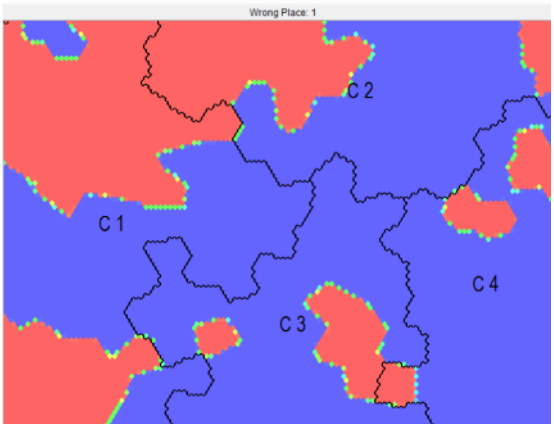

Figure 12. Wrong Place SOM

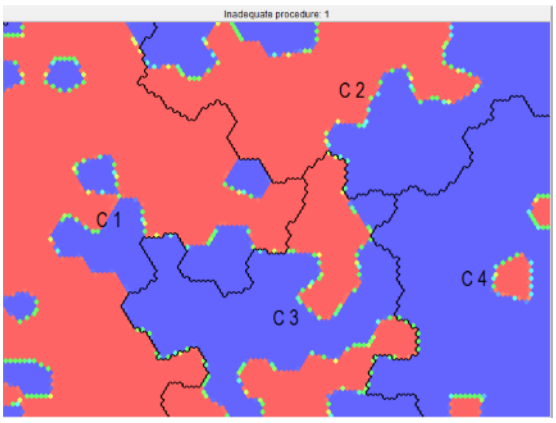

Figure 13. Inadequate Procedure SOM

www.manaraa.com

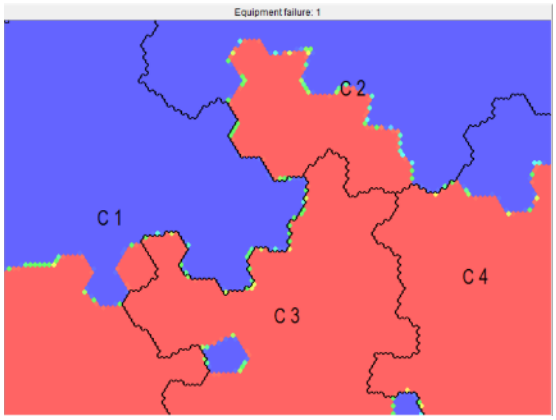

Figure 14. Equipment Failure SOM

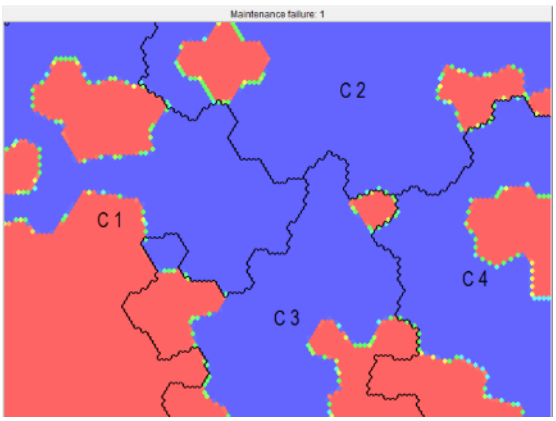

Figure 15. Maintenance Failure SOM

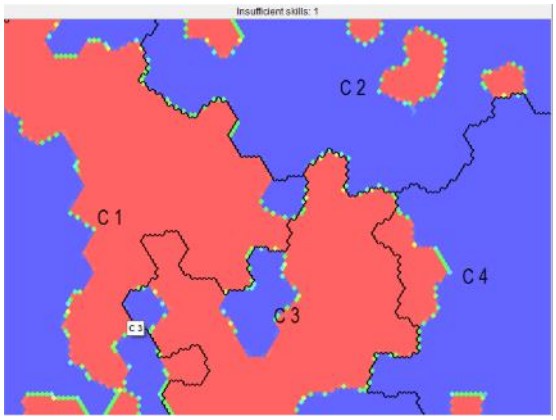

Figure 16. Insufficient Skills SOM

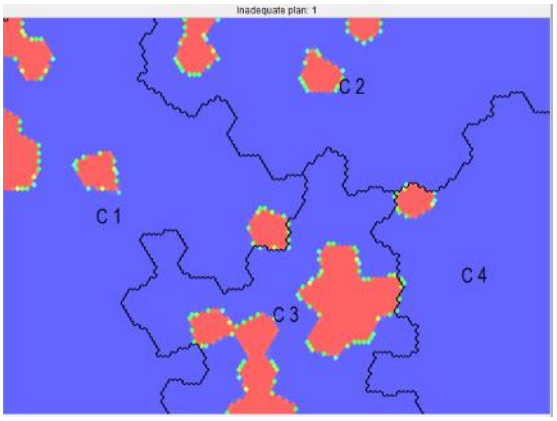

Figure 17. Inadequate Plan SOM

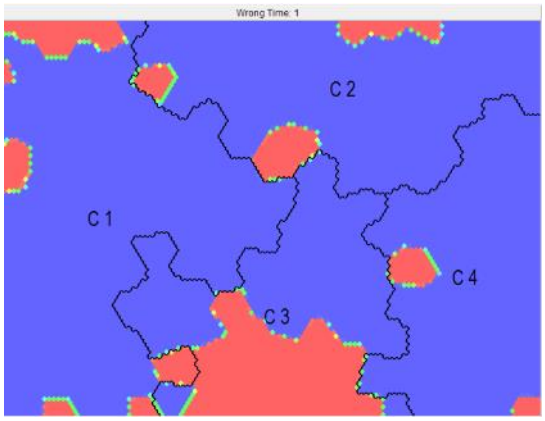

Figure 18. Wrong Time SOM

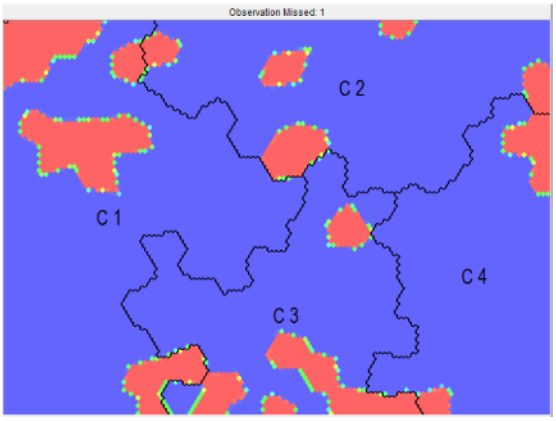

Figure 19. Observation Missed SOM

www.manaraa.com

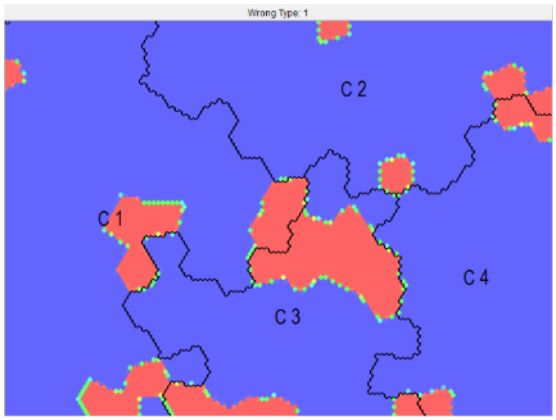

Figure 20. Wrong Type SOM

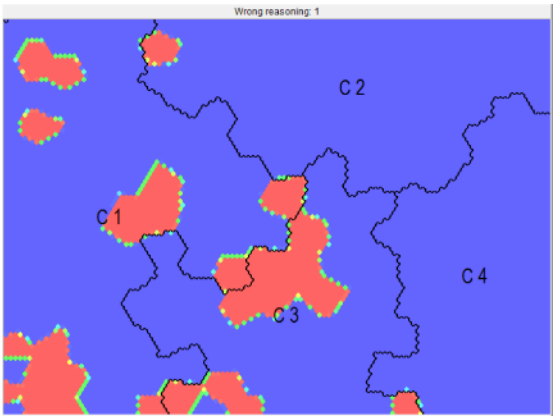

Figure 21. Wrong Reasoning SOM

4. Discussion

4.1 Clustering Interpretation

The application of the SOM algorithm resulted in the reorganisation of accidents originally arranged in a 238 x 53 matrix (Figure 4) into topographic maps (Figures 5 and 7-21). Having the accidents grouped by similarity (considering the contributing factors), it is now possible to identify common patterns and highlight key relationships within the dataset. Moreover, the results are presented through a graphical interface, allowing analysts to effectively *see* the most frequent features or have further insight into contributing factors which might be of interest (such as Design Failures, Human Erroneous Actions, Quality Control and Task Allocation).

The combination of three organisational factors (Inadequate Task Allocation, Inadequate Quality Control and Design Failure - Figures 8, 9 and 10) occupied most of the Cluster 1 area, meaning that these aspects are leading contributors to the grouping. Human erroneous actions contribute to 70% of the cluster, being the Wrong Place (Figure 12) the most relevant one, covering more than a half of the grouping. The analysis of the individual maps clearly shows that Inadequate Procedures (Figure 13) are highly associated with this specific type of human erroneous action, meaning that incorrect, incomplete, ambiguous or instructions open to interpretation provoked specific problems to implement a sequence of operational movements. A deep relationship between Inadequate Procedures (Figure 13) and Insufficient Knowledge (Figure 11) can be perceived in Cluster 1, denoting that written instructions presumed some level of specific knowledge to recognise the situation and complete the operation, which was not the case in many events.

www.manaraa.com

An example of this type of accident was described in a US Chemical Safety and Hazard Investigation Board (2004) safety bulletin, when operators were assigned to a cleaning process in a petrochemicals plant. They executed a nitrogen gas purging exactly as required by the written procedures, in order to remove a hazardous mixture from the pipe. Afterwards, they started a steam purge to finish the service. However, the procedural steps were not sufficiently detailed to ensure the removal of the mixture from the pipe, especially in the low points, and failed to describe the consequences of having flushing liquid in the system. The operators were unaware of the possibility of having residues in the line, as well as the chemical reactions that could occur. The steam purge heated the peroxide/alcohol mix above its thermal decomposition temperature, resulting in an explosion and fire. The SOM map exploration shows that this combination of contributing factors is not an isolated episode, but a recognisable pattern (or tendency) in Cluster 1, which should prompt the attention of risk analysts.

The correlation of further factors, such as the design failure which allowed an unnecessary low-point section in the pipe route and the failure of the quality control to identify the low-point trap as well as the deficient procedure are also persistent in this grouping.

As in Cluster 1, Cluster's 2 most common features were Design Failure accompanied by Inadequate Task Allocation and Inadequate Procedures. However, the results for these factors are close to the overall dataset figures (65.97%, 60.07% and 44.09%, respectively) and thus cannot be considered to be major influencing factors to generate this clustering. A noticeable feature in this cluster was Adverse Ambient Conditions, which attained 14% in this grouping. The exploration of these events demonstrates that not only major natural events such as hurricanes, typhoons or earthquakes should be considered from a risk and safety management perspective, but also more common adverse situations like torrential rain, electrical storms and even the presence of airborne particles. A straightforward example of the latter is the case where haze from forest fires carried atmospheric particles to the intake of an air separation unit of a gas processing facility, causing an explosion and a large fire.

Equipment Failure (as shown in Figure 14) dominates almost the whole area of Cluster 3, but, in sharp contrast with Cluster 1, the association with Maintenance Failure (Figure 15) is not relevant any longer. In fact, the analysis of the maps indicates that the equipment failure events tend to be associated with Design Failure and/or Insufficient Skills (Figure 16)

www.manaraa.com

for this grouping. Therefore, it can be learned that enhancing maintenance cannot be considered the only solution to minimise the possibility of equipment failures. The lack of skills (training / experience) to operate a system or equipment may well be combined with equipment faults, as well as with design shortcomings. 71.8% of the Cluster 3 area was covered by human erroneous actions, mostly Wrong Time and Wrong Type (Figures 18 and 20). A profounder analysis of specific cognitive functions influencing human actions can be also attained. Observation Missed, Wrong Reasoning and Inadequate Plan maps represented many cases where events or signals that were supposed to trigger an action were missed; the operator misinterpreted a given signal or cue – a deduction or induction error; or the mental plan/solution to solve an issue was incomplete or wrong. The airplane accident report mentioned in the introduction (*Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile,* 2011) perfectly illustrates circumstances where an equipment failure due to a design shortcoming can trigger cognitive disturbances, leading to errors and ultimately major accidents. The lack of skills of the co-pilot to handle some problems (i.e. the approach to stall) at high altitudes made him build an erroneous mental plan to react to the undesirable situation. He adopted a tactic applicable to low altitudes, destabilising the flight path with inappropriate control inputs. Therefore, these tendencies reveal that specific training, aimed at dealing with critical conditions and major hazards, is very complex and must be carefully selected. Instead of reassuring written procedures or transmitting instructions, an effective training strategy must embrace the systemic development of a problem-solving mindset. Although most of the simulation and training strategies are focused on *conditioning* the human to expected or predictable scenarios, critical situations will demand advanced decision-making skills and should focus on processes and techniques aimed at the identification and development of adequate operation alternatives.

Equipment Failure is also the main contributor to Cluster 4, but the accidents within this grouping presented different characteristics from the former cluster. The map's analysis for this cluster (i.e. Figures 9, 10 and 14) unmistakably shows that equipment problems were accompanied by quality control issues and design shortcomings. Although these relationships are quite clear, the low mode of 2 contributing factors prevents further tendencies from being accurately inferred in this grouping.

Previous studies such as Groth and Mosleh (2012) successfully applied an analogous approach, in an attempt to develop causal insights from an incident dataset. Their objective

www.manaraa.com

was to quantitatively incorporate those insights into a Human Reliability Analysis method, constructing a Bayesian Network mostly with data from the Human Events Repository Analysis (HERA) dataset. The HERA dataset contains risk-significant Nuclear Power Plant operating events, thus restricted to the nuclear industry but incorporating data points such as minor events, near-misses and inspection results. Only events containing human errors (at least one) are recorded. In summary, the results indicated four error contexts: (i) Training, Team and Complexity; (ii) Knowledge, Attitude and Organisational Culture; (iii) Attitude, Loads and Complexity; and (iv) Resources and Complexity.

Although the first (i) and most significant error promoting context had been also acknowledged in the Cluster 3 interpretation above, significantly different taxonomies (and with different objectives) will necessarily lead to different results. While the taxonomy applied by Groth and Mosleh (2012) is detailed, in order to capture factors influencing single human errors in a specific and delimited scenarios, the classification system used to construct the MATA-D dataset generally contains higher hierarchical levels, intended to capture contributing factors affecting all human performance before and during the development of complex, rare events, i.e. major accidents.

A more detailed set of performance influencing factors facilitates the quantification of contributing factors and the attribution of probabilities to human errors, fulfilling a vital requirement of HRA models, which is a major element of current probabilistic risk assessments. On the other hand, the recognition of complex patterns leading to human performance shortcomings and the understanding of the whole range of interactions involved in a major-accident event would require a far-reaching and comprehensive taxonomy, capable of conveying risk reduction information to interested parties in the blunt-end, such designers, as well as to communicate risks to diverse stakeholder groups.

www.manaraa.com

5. Conclusions

The successful conversion of multi-attribute, complex data from a major-accident dataset into a 2-D array revealed numerous possibilities of data clustering and interpretation, in order to disclose features, facilitate risk communication and enhance the learning process. The usage of graphical visualisation techniques such as topographic maps, which were generated by the SOM algorithm (Kohonen, 2001) in this research, provided additional means to help stakeholders absorb risk information and synchronise the textual explanation with meaningful visual representations.

The application of an artificial neural network approach permitted the identification of common patterns and comparable contributing factors within four major accidents groups, revealing interfaces and conveying information to operators, designers, risk managers and the general public.

Beyond the visual aid provided by the maps' construction, it was possible to directly correlate real accidents with images, creating and enhancing a full learning experience that can be further expanded, depending on the objectives and the targeted public. This is due to the data mining approach, which fully preserved the input data (the MATA-D 238 x 53 Matrix) in the output space (the 2-D Maps) and allowed the retrieval of the dataset records. Also, the interpretation of the graphs can help to understand and communicate the relationship between contributing causes for major accidents. Figures 14 and 15, for instance, can be used to show to a sceptical operations manager that very advanced maintenance procedures do not guarantee that equipment will not fail, and further measures might be necessary.

The strategy of representing accident data in maps allows the fast transmission of relevant information and increases the possibility that stakeholders will fix and remember the lessons learned from accidents, minimising the dominance of biased concepts such as the oversimplification of addressing human errors as the main cause of major disasters.

6. Acknowledgements

The authors gratefully acknowledge the insights from Dr. Franz Knoll (NCK Inc.). This study was partially funded by CAPES [Grant nº 5959/13-6].

www.manaraa.com

Chapter 3: A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors

Overview

This paper was presented in the 2015 IEEE Symposium Series on Computational Intelligence. Essentially, it scrutinises an earlier version of the MATA-D dataset presented in Chapter 1 from another perspective, in order to disclose relevant features and indicate paths to the recognition of the genesis of human errors. This is a good example of the flexibility of the proprietary dataset, demonstrating that it is adaptable and can be used and integrated with other data mining and classification approaches.

In order to understand the accident data and identify key similarities among events, a tailored Hierarchical Agglomerative Clustering method, using the Bray-Curtis dissimilarity and two different linkage functions – complete and average – are now applied to the dataset. Basically, the dissimilarity measurement, which was specifically chosen to fit the MATA-D data, aims to aggregate accidents with proximate contributing factors, while the linkage function extends the concept to align comparable clusters. In order to display more cohesive clusters and facilitate the interpretation of the output, the intermediate hierarchical level of the dataset was used for the groupings, meaning that the dimensions were reduced from fifty-three to fifteen before the application of the algorithm. These intermediate dimensions are: erroneous actions, observation, interpretation, planning, temporary person-related functions and permanent person-related functions; equipment, procedures, temporary interface and permanent interface; and organisation, training, ambient conditions and working conditions.

Although the methodology presented a significant simplification in relation to the previous chapter, i.e. the hierarchical level of the contributing factors being considered, it successfully described common interactions between human factors, the organisational environment and technology. New attributes (e.g. fatality rate per cluster) were also taken into account, revealing which combinations appeared to lead to an increased loss of life, such as accidents featuring communication issues and interface problems.

The hierarchical arrangement of the clusters in a familiar dendrogram structure also enabled a bird's eye view of the dataset. Organisational environment dominated the clustering, and two large groups – Organisation-Technology and Organisation-Human

www.manaraa.com

Factors – were instantly noticeable. Then, the lower branches (i.e. the nine clusters) were analysed, disclosing relevant features. A relationship between the complexity of the accidents (the ones containing more contributing factors) and advanced cognitive functions (the need to observe, interpret signals and create a strategy before acting) was established. Other interesting combinations were also highlighted by the cluster analysis. Conclusions to improve human performance based on these clustering results, such as the need to improve communication (make sure operators receive and understand messages) and the interface (warning and error messages) for the most complex cases, were successfully addressed.

www.manaraa.com

A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors[3]

Raphael Moura[a,*], Christoph Doell[b], Michael Beer[a], Rudolf Kruse[b]

[a] Institute for Risk and Uncertainty, University of Liverpool, Brodie Tower, Brownlow Street, Liverpool L69 3GQ, UK

[b] Institute of Knowledge and Language Engineering, Otto von Guericke University Magdeburg, Universitatsplatz 2, 39106 Magdeburg, Germany

[*] Corresponding author at: Office 614 Brodie Tower, Brownlow Street, Liverpool L69 3GQ, UK

1. Introduction

Major accidents appear to be a collateral effect of the development of human activities, and the added complexity of high-technology systems seems to challenge the improvement of industrial safety records. Only in the last 5 years, a perplex society faced worldwide tragedies such as the Macondo Blowout in the Gulf of Mexico, the Fukushima Nuclear Plant disaster in Japan, the missing Malaysian airplane MH370 and the Korean Ferry which has capsized and killed 304 people. Similarly, Reason (2013) listed several analogous events in past decades (e.g. Seveso, Three Mile Island, Bhopal, Chernobyl and Piper Alpha) referring to them as *man-made* organisational disasters.

Technical investigations arising from these events have generated a considerable amount of data, revealing an extremely intricate chain of contributing factors leading to disastrous consequences and highlighting the decisive part humans have played (Cullen, 1990; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011; Kurokawa et al., 2012). Factors such as management problems, lack of information, communication failures, fear, poor working conditions and reasoning shortcomings were combined with human erroneous actions during the operational stage, to result in the catastrophic failure of cutting-edge technologies and systems, which are perceived as highly reliable.

One of the methods used to minimise human errors is to apply a suitable Human Reliability Analysis (HRA) technique to predict the probability of human error while executing the

[3] Original publication in Moura, R. et al., 2015. A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors, *2015 IEEE Symposium Series on Computational Intelligence*, Cape Town, pp. 1838-1843. DOI 10.1109/SSCI.2015.256.

www.manaraa.com

tasks required during the operation of systems. Previous work (Bell & Holroyd, 2009) identified 72 different methods to assess human reliability, and some of these techniques are widely used by industry, such as the Human Error Assessment and Reduction Technique HEART (Williams, 1986), the Technique for Human Error Rate Prediction THERP (Swain & Guttmann, 1983), and A Technique for Human Error Analysis ATHEANA Barriere et al., 2000). These techniques usually comprise a list of internal and external features called performance shaping factors, used to quantify the likelihood of human failure given the task and the existing contributing factors. In spite of the adequateness of HRA techniques to estimate human error probabilities, it is clear that uncertainties related to human behaviour, which are highly associated with cultural issues, the organisational context, the work environment, work pressures and relationships, training and technological aspects, among others, turn the outcomes of this kind of study largely imprecise.

Therefore, in face of the decisive impact of human actions and decisions on the performance of engineering systems, associated with the uncertainties of current estimation methods, it is necessary to improve the understanding of the relationships among contributing factors. For that reason, the Multi-attribute Technological Dataset (Moura et al., 2015a) will be scrutinised by a suitable data mining technique, in order to overcome barriers to dealing with complex data and to reveal improvement opportunities. The dataset contains 216 major accidents from different industries, all classified under the same framework. The dataset structure was built upon the taxonomy developed by Hollnagel (1998) in the Cognitive Reliability and Error Analysis Method (CREAM).

In the following sections, a short description of the data is given and the data pre-processing steps are disclosed. Then, the review of the hierarchical agglomeration clustering is followed by the definition of the distance similarity criterion for the particular case. Finally, conclusions are built upon the relationships among contributing factors, revealing opportunities for the development of accident prevention schemes.

2. Data Description

A dataset containing information regarding major accidents was analysed. The documentation generated from more than 200 major accidents was scrutinised and comparable information was made available, such as the number of casualties, the year, the location and the industry in which the accident occurred. Along with this general

www.manaraa.com

information, the disclosed contributing factors are of special interest. Previous research (Moura et al., 2015a) suggests that fifty-three hierarchically ordered attributes are capable of describing the contributing factors for accidents, allowing an adequate representation of the accident causation model. On the first hierarchical level, there are three entries: Man, Technology and Organisational Environment. The group Man generalises human errors, where a human action or cognitive aspect were directly involved. Man can be split into the following four subgroups: Erroneous Actions, Specific Cognitive Functions, Temporary Person-related Functions and Permanent Person-related Functions. The technology part can be divided in the following four categories: Equipment, Procedures, Temporary Interface and Permanent Interface. Organisational Environment is fragmented into Organisation, Training, Ambient Conditions and Working Conditions. Deeper levels of the hierarchy and more detailed information were described earlier by Moura et al. (2015a).

The overall dataset contains 216 major accidents. To maintain the focus on the contributing factors analysis, these will be the data points considered by the data mining technique. Accidents are given as vectors in the fifty-three dimensional Boolean space, describing which conditions were present or absent when the accident occurred, thus the dataset can be represented by a 216x53 Boolean matrix. For these overall 11448 values, the dataset contains 1416 ones and 10032 zeros. Given the data, the goal is to find groups with common features, the so-called data clusters. Table 1 presents the factors' list ordered by frequency in the MATA-D dataset. Design Failures was the most frequent factor and appeared in 64.35% of the accidents, while four factors (Cognitive Style, Sound, Humidity and Other) were not identified.

Table 1. Features and corresponding frequencies

Features	**Frequency (%)**
Design failure	64.35
Inadequate quality control	59.26
Equipment failure	58.33
Inadequate task allocation	58.33
Inadequate procedure	43.98
Insufficient skills	37.50
Maintenance failure	35.19
Insufficient knowledge	34.26
Wrong Place	26.85
Missing information	19.91
Observation Missed	15.28
Wrong Time	14.81

www.manaraa.com

Incomplete information	13.89
Faulty diagnosis	12.96
Wrong Type	12.96
Wrong reasoning	12.04
Communication failure	11.11
Management problem	10.19
Inadequate plan	9.72
Decision error	8.80
Adverse ambient condition	7.87
Cognitive bias	7.87
Priority error	6.94
Social pressure	6.94
Distraction	6.48
Excessive demand	5.56
Delayed interpretation	5.09
Irregular working hours	4.17
Inadequate team support	3.70
Incorrect prediction	3.70
Fatigue	3.24
Physiological stress	3.24
Ambiguous information	2.78
Inadequate workplace layout	2.78
Software fault	2.78
Wrong Identification	2.78
False Observation	2.31
Fear	2.31
Inattention	2.31
Wrong Object	2.31
Access problems	1.85
Access limitations	1.39
Mislabelling	1.39
Performance Variability	1.39
Temperature	1.39
Illumination	0.93
Memory failure	0.93
Psychological stress	0.93
Functional impairment	0.46
Cognitive style	0.00
Humidity	0.00
Other	0.00
Sound	0.00

3. Data understanding and pre-processing

In the earlier stages of the data analysis, a relevant aspect is data understanding (Berthold et al., 2010) through the application of simple statistics to get a general idea. Having the

www.manaraa.com

knowledge that the presence of factors (i.e. ones) is especially important, rows and columns with few ones were initially challenged. There are fourteen monocausal accidents (lines in the matrix), representing accidents which showed a single contributing factor or cause, all arising from reports commissioned by insurance companies. This might imply that some insurance companies will not invest further time on lengthy investigations when a strong and sufficient reason, such as an equipment failure, has been found. For the current analysis, these monocausal accidents were all removed, as the applied clustering method would consider these data points as outliers.

An examination of the raw data revealed that four out of fifty-three dimensions did not appear, i.e. Cognitive Style (part of the group of Permanent Person Related Functions), Sound, Humidity and Other (from the group of Ambient Conditions). Seventeen dimensions appeared less than seven times each (less than 3%). Although this could be useful information for the accidents causation understanding, for statistical analysis these dimensions hardly contain information.

In order to verify the amount of information contained, a Principal Component Analysis (PCA) was performed. The result, showing the explained variance of the dimensions, revealed that no further dimensions could be found, allowing its legitimate removal.

Given that the dimensions are hierarchically ordered, data was aggregated considering whether or not an attribute was present in at least one of the groups within the categories. This aggregated dataset (in contrast to the original unaggregated dataset) contained fifteen dimensions. After filtering monocausal accidents and applying the aggregation, the Boolean matrix had a size of 202 x 15. The PCA performed on these new data did not show any duplicate dimensions.

4. Methodology

Having a Boolean representation of the accidents, the next step would be to define an adequate similarity measure to group datapoints. Accidents were considered to be similar if they have similar contributing factors. For two given Boolean vectors i and j, we counted the number of Ones for each event $S(i)$, $S(j)$ and further counted the dimensions in which both vectors show Ones simultaneously $C(i, j)$.

$$d(i,j) = 1 - 2C(i,j)/(S(i) + S(j)) \qquad (1)$$

www.manaraa.com

Equation 1 shows the Bray-Curtis dissimilarity of two accidents (Bray & Curtis, 1957), which is not a formal distance measure as the triangle inequality does not hold. Nevertheless, this dissimilarity measurement ensures that accidents are closer if they have common causes, meaning common Ones in the Boolean space. Dimensions with common Zeros do not increase the accidents' similarity. The measure is normalised by the division of the number of ones contained in both vectors so that high similarities occur if two vectors have many common factors and only a few different dimensions.

As the prime objective is to find groups of similar accidents, the Hierarchical Agglomerative Clustering described in Kruse et al. (2013) was applied. Every data point is considered as a cluster in the beginning, and then successively merged by similarity. The similarity criterion for two given accidents was already exposed, and the concept can be extended to clusters by using an appropriate Linkage Method. For two clusters *A* and *B* with their enclosed points *a* and *b*, respectively, their distances can be defined for complete and average linkage according to equations (2) and (3).

$$\mathrm{d}_{\mathrm{complete}}(\mathrm{A},\mathrm{B}) = \max_{\mathrm{a}\in\mathrm{A},\mathrm{b}\in\mathrm{B}}(\mathrm{d}(\mathrm{a},\mathrm{b})) \qquad (2)$$

$$\mathrm{d}_{\mathrm{average}}(\mathrm{A},\mathrm{B}) = \frac{1}{|\mathrm{A}||\mathrm{B}|}\sum_{(\mathrm{a},\mathrm{b})\in\mathrm{AxB}}(\mathrm{d}(\mathrm{a},\mathrm{b})) \qquad (3)$$

Clusters can be evaluated with silhouette score (Rousseeuw, 1987), which is an effective internal clustering evaluation measure returning values in [−1, 1]. Values are close to one when the resulting clustering returns relatively compact clusters, also having fairly high inter-cluster dissimilarities.

5. Results

The following analysis details the dendrogram of the complete-linkage distances. Reading from bottom to top, it shows the data points, which are iteratively merged into bigger clusters. This process ends when the cut value is reached. Above that value, the connecting edges are blue, and below it they are differently coloured, depending on the cluster. The cutting was performed at the 0.65 distance, where a reasonable jump in the clustering levels can be observed, as shown in Fig. 1. The resulting clustering shows a moderate silhouette score of 0.228, which is slightly better than the score for average linkage 0.221.

www.manaraa.com

The clusters are enumerated from left to right. First single cluster comprises the only two events which contained just human factors as significant contributors to the accidents. This chunk is substantially different from the distribution in the remaining groupings, as the vast majority of the technological accidents of the MATA-D encompass at least one organisational or technological issue. Therefore, these two events can be considered outliers.

All the remaining events involved organisational aspects (organisation, training, ambient conditions or working conditions) to generate the undesirable outcome. Clusters 2 to 5 were highly associated with technological issues (equipment, procedures or interface), while clusters 6 to 9 showed the manifestation of humans factors (execution errors, specific cognitive functions and person-related functions). It is important to notice that the latter groupings (from 6 to 9) form a single cluster containing almost the same number of elements (102 of 106 events) when a different clustering criterion, i.e. the average-linkage method, is applied to quantify dissimilarities between clusters (Fig. 2). Additionally, the same points build the leftmost cluster of outliers.

The main results of the individual analysis of the complete linkage clusters are summarised in Table 2, and will be detailed as follows.

Cluster 2 (twenty elements) was dominated by wrong procedures (100%) and organisational issues (95%). Training was also significant (70%). No erroneous actions were observed.

The third Cluster (twenty-nine elements) contained organisational issues (100%) with training problems (100%), also with a high incidence of equipment failures (75.9%). A marginal incidence (a single case) of erroneous actions was shown.

Cluster 4 (six elements) main feature is the combination of organisational issues with communication problems (100% of the cases). No erroneous actions were observed, and a marginal incidence of temporary person-related functions, i.e. psychological stress, was shown.

Cluster 5 (thirty-nine elements) contained organisational issues (100%) with equipment failure (82%). No human issues were observed.

www.manaraa.com

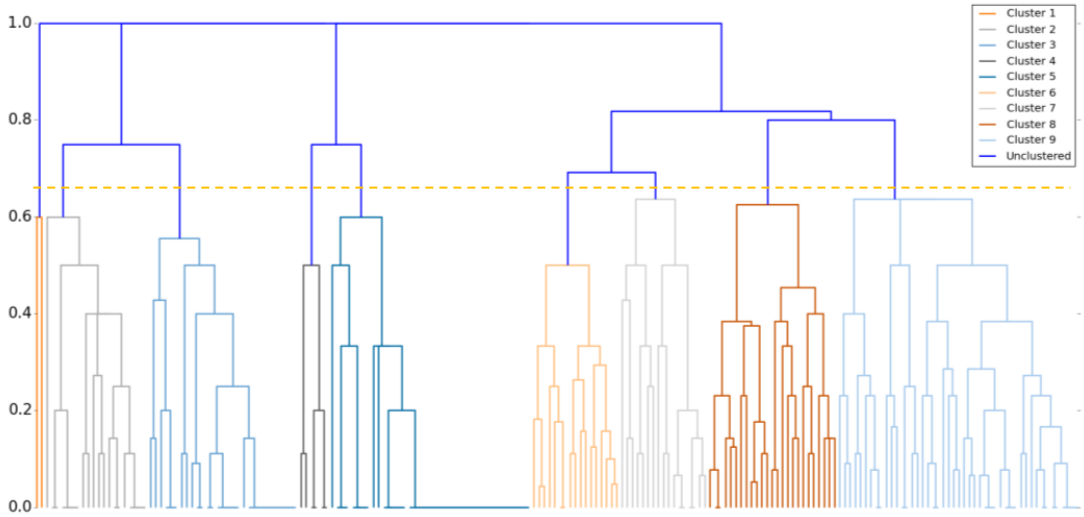

Figure 1: Dendrogram for complete linkage clustering

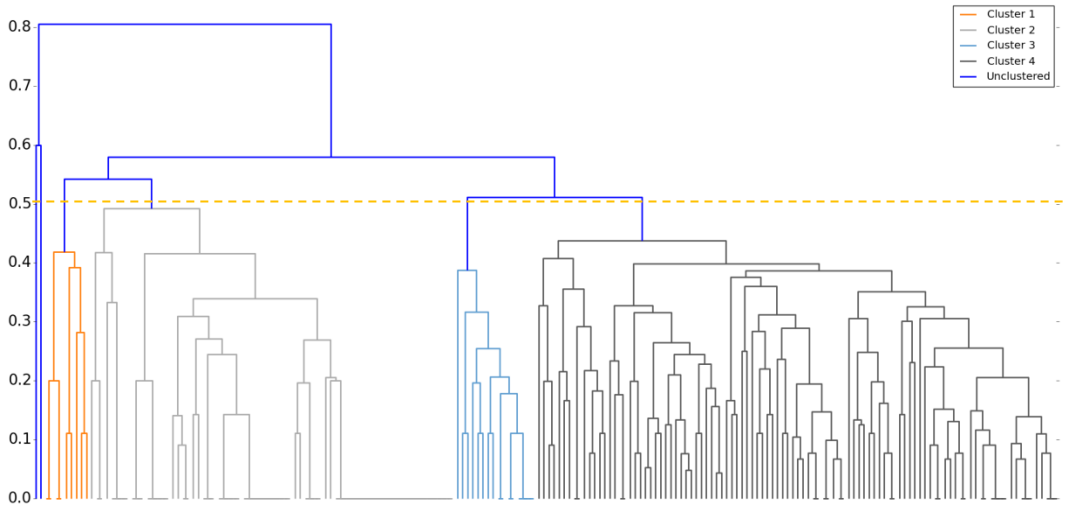

Figure 2: Dendrogram for average linkage clustering

Table 2. Aggregated Data, Complete Linkage

Cluster	C1	C2	C3	C4	C5	C6	C7	C8	C9
Accident #	2	20	29	6	39	17	17	25	47
Median	2.50	6.00	6.00	4.00	2.00	13.00	5.00	10.00	8.00
Average	2.50	5.20	5.66	4.33	2.77	13.65	7.24	10.00	8.30
Mode	n/a	7	5	4	2	13	5	6	9
Fatalities #	5	159	67	2	248	471	6	132	388
Death Rate	2.50	7.95	2.31	0.33	6.36	27.71	0.35	5.28	8.26

The following 4 clusters contained direct human errors joining organisational issues to generate accidents. It is worth mentioning that Cluster 6 was the deadliest combination of factors, reflecting 471 fatalities and a death rate of 27.71 per event, followed by Cluster 9,

www.manaraa.com

which encompassed 388 fatalities and attained a death rate of 8.26, as can be seen in Table 2.

All accidents in the sixth cluster (seventeen elements) contained organisational issues plus erroneous actions. These actions were explained by all three levels of specific cognitive functions, i.e. interpretation (94.1%), Observation (88.6%) and Planning (70.6%). Temporary person related functions were also significant (88.6%). An important feature of cluster 6 is that an interface problem (information provided by the systems, a technology problem) or communication issues (exchange of messages/information within the organisation) were shown in 100% of the cases. Training problems (82.4%) and poor working conditions (58.8%) as contributing factors were also above the overall average.

The accidents in Cluster 7 (seventeen elements) showed organisational issues with erroneous actions (100%) again, but mainly combined with one specific cognitive function level (observation, with 70.6%). Equipment failures and communication issues also showed 70.6% of incidence.

Cluster 8 (twenty-five elements) contained the combination of organisational issues (100%) with erroneous actions (96%), but with an intermediate level of cognitive error (interpretation, with 84% of incidence). Wrong procedures (92%) were very significant, and equipment problems were also shown (72%).

Cluster 9 grouped forty-seven cases (100%) containing erroneous actions with organisational (97.9%) and training (91.5%) issues. 95.7% of the erroneous actions were accompanied by intermediate to advanced specific cognitive functions, i.e. interpretation (61.7%) and inadequate mental planning (44.7%).

6. Discussion

A suitable cluster analysis algorithm was applied to a collection of 202 major accidents from the MATA-D dataset, in order to disclose relevant relationships among contributing factors. All clusters were largely dominated by the Organisational Environment group, confirming that design failures, poor quality control and inadequate task allocation are key contributing factors to major accidents.

www.manaraa.com

The first cluster, which contained only two elements (less than 1% of the sampling), confirmed previous studies (Moura et al., 2015a) indicating that the possibility of having a single failure point leading to a major accident is very low. The two cases represented human erroneous actions following a serious violation of work procedures, such as smoking during a fuel tanker offloading or deviating from the recommended navigating route without any apparent reason. Although violations are not uncommon, it appears to occur in specific cases, such as under an uncertain environment (e.g. system is in an unrecognised, non-routine status), associated with unclear rules or procedures, or when operators distinguish some kind of tangible benefit (e.g. save money, time or effort through an easier way of performing a task) from non-compliance. However, these associations usually require further contributing factors (e.g. inadequate procedure, poor communication or training), which were not the case in the two analysed accidents.

The algorithm application set apart a very significant group, i.e. 106 accidents (From cluster 6 to cluster 9) in which organisational factors were accompanied by human erroneous actions. The exposed differences between these four clusters lie on the mental functions or disturbances, which triggered the action error.

In spite of having only seventeen events, cluster 6 might represent a very important chunk, as it highlights the deadliest grouping, with a fatality rate of 27.71 deaths per event. In addition, accidents within this cluster have shown the largest amount of simultaneous contributing factors to generate an accident, with an average of 13.65 and mode of 13 significant features. The justification is that a very complex chain of events or simultaneous failures took place in sophisticated systems (e.g. oil & gas, chemical or aviation industry), which would have required the whole range of specific cognitive functions (observation, interpretation and planning) to recover the system to a regular state and minimise the effects of the accident sequence.

Although the path to recover the system to a normal state was generally clear in most of the cluster 6 cases, the operator was unable to make progress, due to two main reasons. First, a technology problem related to the man-machine interface failed to provide an accurate information (an indistinct or incomplete error message, for instance), and the communication channels of the organisation failed to deliver a complete information or feedback. Secondly, inadequate working conditions (e.g. excessive demand and irregular working hours) resulted in temporary person-related functions (e.g. distraction, fatigue or

www.manaraa.com

psychological stress) to disturb the mental processing. Deprived from an accurate input from the system and from the organisation (information and training) to support the decision-making process, as well as undermined by inadequate working conditions, the operator was unable to respond appropriately.

Cluster 7 erroneous actions can be explained by a simpler mental modelling, where a wrong observation was the triggering mechanism. Examples are failures to observe an indication/warning, a mistaken or partial identification of a status or an incorrect recognition of a signal. This cognitive failure to observe something can be directly associated with the substantial rate of concurrent equipment failures and communication issues, which prevented the operator from entering in a deeper state of cognition to build a more complex problem-solving mental plan.

The twenty-five major accidents contained in cluster 8 shared similar characteristics with the previous grouping, but with erroneous actions largely commanded by a faulty reasoning (induction or deduction error) or an imperfect diagnosis of the system state. The additional contributors interacting with these human-related issues suggest a reasonable explanation for this: inadequate procedures, which can be specified by incorrect, obsolete or incomplete written instructions, directly affected the operator's capacity to construct a mental plan and to understand the situation or system state, as the written information and the training, typically assumed to be precise, were not representative of the reality.

Cluster 9 grouped the largest number of major accidents, with forty-seven events, and contained a very consistent amount of contributing factors per accident (average of 8.3). Accordingly, the causes for these accidents are quite well dissected, meaning that a reliable understanding of the grouping behaviour can be reached. The human erroneous actions were strongly influenced by advanced cognitive functions, supposing that a complex mental modelling was required to maintain the system under a regular operational state, i.e. a seamless interpretation and the construction of an accurate mental planning was necessary. However, the high incidence of training flaws, including not only the lack of suitable working instructions to improve the human performance and manoeuvring capacity, but also the dispossession of the necessary knowledge to fully understand the system behaviour, seem to have undermined the human capacity to act properly.

www.manaraa.com

7. Conclusions

7.1 Insights to improve human performance and minimise accidents

The examination of complex accidents under an analytical method, i.e. a Hierarchical Agglomerative Clustering using distance measures tailored to the dataset characteristics, can offer wide-ranging insights into the data, which could be advantageous for the development of accident prevention schemes. It is now clear that different mechanisms are able to trigger specific cognitive failures, leading to human erroneous actions and subsequently disastrous consequences, and the decision-making process at any stage of high-technology facilities' lifecycle can take advantage of the findings discussed earlier in this work. From the analysis of the technological accidents in cluster 6, which resulted in 471 fatalities (27.71 per event), it can be concluded that efforts towards the improvement of the communication within the organisation (to make sure operators receive and understood messages) and from the interface (clear warnings and error messages from the system) would have enhanced the operator's ability to recognise the system status. An evaluation of the whole range of information reaching the operators is indispensable to ensure a proper understanding of the operator's cognitive model.

The study has also revealed that the largest cluster (C9, with forty-seven accidents) was intensely associated with training aspects. Current industry's response to training problems is usually short-duration courses and on-the-job evaluations. In spite of being valuable to some extent (primarily to improve practical skills and develop work experience), this approach is unlikely to improve the awareness level when operating complex systems. This is a robust indication that the knowledge level required to operate in high-technology environments is not well aligned with the system demands.

As a result, the application of a multidisciplinary and more advanced recruiting and knowledge development programme might be a good way to minimise this gap. This should be fully tailored to the system and industry in which the operator will be allocated, in order to ensure that capabilities required to understand systems and operate them properly, including the recovery from complex and abnormal situations, are in place.

www.manaraa.com

7.2 Future Developments

The pronounced incidence of organisational problems in all clusters is an issue which deserves further investigation. This category includes failures in maintenance, quality control, management, design and task allocation. Some of them (such as a design problem) can be embedded in the system for many years. The analysed accidents have shown that there was enough time to spot symptoms of some future flaws before they were effectively exposed by an accidental sequence. In addition, a deeper examination of specific flaws (e.g. training) may provide cues to improve organisations and technologies.

Testing distinct data mining methods, such as Frequent Itemset or Association Rule, might help revealing some extra factors in future works.

8. Acknowledgements

This work has been partially funded by CAPES (Proc. no. 5959/13-6).

www.manaraa.com

Part III

Applications

www.manaraa.com

Chapter 4: Learning from accidents: interactions between human factors, technology and organisations as a central element to verify risk studies

Overview

Building on Chapter 2's technique to cluster, classify and represent major-accident data, the following paper is the first application example presented in the current research. Many high-technology industries are subjected to major hazards, which are of great concern to different stakeholders groups. Accordingly, efforts to control such hazards and manage risks are increasingly made, supported by improved computational capabilities and the application of sophisticated safety and reliability models. Recent events, however, have shown that apparently rare or seemingly unforeseen scenarios, involving complex interactions between human factors, technologies and organisations, are capable of triggering major catastrophes.

Recognising that major accidents might generate a disbelief climate and stimulate decision-makers and wider stakeholder groups to treat risk assessments with scepticism, this application idea originated from the need to verify, validate and to build trust in the output of safety studies. The main objective is to provide practical means for regulators and reviewers to check if lessons from past accidents were taken into account by these studies, a common requirement from risk-based regulations which is not only difficult to implement, but also to verify. Consequently, a relevant contribution to verification schemes is proposed, through the conversion of the interactions among contributing factors occurring in distinct industrial environments into a useful, ready-to-use checklist. This way, stakeholders' confidence in risk management will be naturally enhanced, by the assurance that tendencies and patterns observed in past major accidents are appropriately contemplated by safety studies.

This paper first discusses some of the main accident theories underpinning major catastrophes, highlighting the complexity and the dynamics behind socio-technical systems. The accidents dataset presented in Chapter 1 (MATA-D), which contains major events occurred in high-technology industrial domains, serves as a basis for the data analysis. The clustering and data classification results disclosed by the application of the self-organising maps (SOM) technique in Chapter 2 enables further exploration of accidents' information gathered from in-depth investigations. Graphical representations of the contributing factors

www.manaraa.com

interacting in each cluster are also developed (e.g. in Figures 1 and 3), revealing novel means to represent accident data and disclose accident causation information.

The interpretation of the SOM maps and the recognition of the complex interactions among contributors exposed common patterns in major accidents, which are then used in the development of a comprehensive attribute list to verify risk assessment studies. The questions presented in the checklist require a simple “yes” or “no” reply, and negative answers indicate possible shortcomings in safety studies, raising the awareness of safety assessors for complex risks involving interactions between human factors, technological issues and organisational aspects.

The commitment to challenge risk assessments assumptions and results, in order to demonstrate that real complex accident scenarios were fully understood and used to improve the quality of high-technology engineering systems, is key to enhance societal and stakeholders’ trust on safety studies.

www.manaraa.com

Learning from accidents: interactions between human factors, technology and organisations as a central element to verify risk studies [4]

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

[a] Institute for Risk and Uncertainty, University of Liverpool, Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom
[b] Institute for Risk and Reliability, Leibniz Universität Hannover, Callinstr. 34, 30167 Hannover, Germany
[c] National Agency for Petroleum, Natural Gas and Biofuels (ANP), Av. Rio Branco, 65, CEP: 20090-004, Centro, Rio de Janeiro-RJ, Brazil
[d] NCK Inc., 1200 Avenue McGill College, Montreal (Quebec) H3B 4G7, Canada
[*] Corresponding author at: Office G79 Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom.

1. Introduction

1.1 Accident causation models and implications to verify risk assessments

Accident causation models lie beneath all efforts related with safety engineering, as they serve as a basis for accident investigation and analysis, to prevent future accidents in new designs and for the development of risk assessment techniques (Leveson, 2012). The rising interest in understanding the genesis of major accidents and the growing importance of technological issues to societies directed many schools of thought to approach the accident causation problem from different perspectives, leading, to a certain extent, to conflicting ideas on how (and if) hazards can be appropriately addressed and controlled.

According to Perrow (1999), failures in complex, tightly coupled systems are inevitable, and thus the occurrence of accidents with catastrophic potential in some high-technology facilities (e.g. nuclear power and nuclear weapons) is unavoidable, constituting an expected or *normal accident*. His theory was developed after the Three Mile Island accident, a partial core meltdown that occurred in a USA nuclear power plant in 1979 which was his base case. To cut a long story short, he simply suggests the discontinuation of technologies such as nuclear plants and weapons (which he deems hopeless) as he understands that the inevitable risks outweigh the perceived benefits. Operator errors are frequent elements of the scrutinised case studies, highlighting how complex interactions of a series of failures can lead to flawed mental models. Perrow alludes to a sole possible managerial style to

[4] Original publication in Moura, R. et al., 2017. Learning from accidents: interactions between human factors, technology and organisations as a central element to validate risk studies, *Safety Science 99:196-214*, DOI 10.1016/j.ssci.2017.05.001.

www.manaraa.com

safely run these facilities: a military-shaped organisation, authoritarian and rigidly disciplined. However, he claimed that this administration structure would be socially intolerable and unsustainable during peacetime, for industrial civil activities.

The Normal Accidents Theory was preceded by Cohen's Garbage-Can Model (Cohen et al., 1972, Davis et al., 1988), which presented an earlier recognition that organisations have high degrees of uncertainty, leading to ill-defined or competing preferences, ambiguous goals, unclear technology and fluid patterns of stakeholders' involvement in the decision-making process. While the Garbage Can theory indicates that major accidents will happen because organisational behaviour is extremely complex and unpredictable, the Normal Accidents Theory limits the inevitability of disasters to systems where complexity and tight coupling are observed. Though both theories share an unenthusiastic view of the human capacity to predict and control hazards, some distinct (and useful) elements can be extracted from them: the former clearly points towards organisational matters as the root-cause of catastrophes, while the latter blames technological aspects, albeit assuming that it could be somehow mitigated by a particular type of military organisation.

Taleb's book *The Black Swan – The Impact of the Highly Improbable* (2007) coined a popular and wide-reaching concept (Aven, 2015, Aven 2013, Paté-Cornell, 2012) to explain the occurrence of major accidents. He refers to events with extreme impacts as *Black Swans*, considering them as highly improbable events (or outliers) which are not prospectively foreseeable. His celebrated analogy was based on the fact that people in the "old world" only knew white-feathered swans before the English arrival in Australia, where the sight of a black swan came as a surprise. He concludes that predictions based on historical data cannot anticipate outliers, claiming that the usual focus on standard operations disregards the extreme or uncertain. According to his views, the dynamics in high-technology domains are far more complicated than can be anticipated, and conducting laborious pre-analysis and validation based on probabilistic modelling should be ruled out, as it has little effect in terms of major hazards control (or black swans prevention!).

It is worth noticing that many widespread accident causation theories appear to consider the understanding of all complex interactions leading to major accidents during the operation of high-risk industrial facilities as a significant challenge still to overcome. According to this approach, objectives and preferences are being randomly defined, technologies are not fully understood by managers and workers, complex interactions

www.manaraa.com

leading to major accidents are not predictable and stakeholders' groups are fluctuating during the facility's lifecycle.

Conversely, researchers on High Reliability Organisations (Roberts, 1990, Grabowski & Roberts, 1997, La Porte & Consolini, 1998) address cases where organisations managing operations with high potential for disasters achieved excellent levels of reliability for long periods of time, appearing to function better than others. Based on the observation of success cases, they believe that it is possible to recognise scientific methods to sustain a nearly error-free operation, even in very hazardous environments. It is worth noticing that the examples used to ratify the High Reliability Organisations principles include nuclear power stations, putting it in sharp contrast with the Normal Accidents Theory. According to Perrow (1999), these are precisely the sort of facility susceptible to unavoidable failures, and thus society should consider abandoning it at once.

Sagan (1993) conducted an in-depth analysis of the Normal Accidents and the High Reliability Organisations theories, presenting some of the competing viewpoints below.

Table 1. Competing Perspectives on Safety with Hazardous Technologies (Sagan, 1993)

High Reliability Theory	Normal Accidents Theory
Accidents can be prevented through good organisational design and management.	Accidents are inevitable in complex and tightly coupled systems.
Safety is the priority organizational objective.	Safety is one of a number competing objectives.
Redundancy enhances safety: duplication and overlap can make "a reliable system out of unreliable parts".	Redundancy often causes accidents: it increases interactive complexity and opaqueness, and encourages risk-taking.
Decentralized decision-making is needed to permit prompt and flexible field-level responses to surprises.	Organisational contradiction: decentralisation is needed for complexity, but centralisation is needed for tight-coupled systems.
A "culture of reliability" will enhance safety by encouraging uniform and appropriate responses by field-level operators.	A military model of intense discipline, socialisation and isolation is incompatible with democratic values.
Continuous operations, training and simulations can create and maintain high-reliability operations	Organisations cannot train for unimagined, highly dangerous or politically unpalatable operations.
Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.	Denial of responsibility, faulty reporting and reconstruction of history cripples learning efforts.

Despite the evident disparity between these schools of thoughts, especially regarding the possibility of preventing a major accident, Sagan perceived some common ground regarding the frequencies of these events. While the normal accidents theory states that

www.manaraa.com

major accidents are inevitable, but *extremely rare*, high-reliability organisations theory postulates a *nearly* error-free operation by an enhanced safety management. Implicitly, there is a mutual recognition of the low probabilities of catastrophic events. After assessing several study cases on safety events involving U.S. nuclear weapon systems, Sagan (1993) concluded that the collected evidences provided stronger support to the Normal Accidents Theory. His observations indicated that factors such as excessive discipline (he identified evidences of extreme loyalty, secrecy, cover-ups, distain for external expertise and other self-protecting mechanisms), conflicting interests and constraints on learning have limited nuclear facilities' organisational safety and could have resulted in major catastrophes if circumstances were slightly different.

Therefore, Sagan's resulting analysis of the theories can be considered even more pessimistic than the Normal Accidents Theory. Despite the claim that accidents are inevitable, Perrow left the door open for a social incompatible but safety-efficient managerial style: a military-shaped organisation with rigid discipline. However, his allegations were challenged by Sagan's nuclear weapons handling sample, which included an alarming number of close calls.

Other researchers recognise the difficulties in preventing major accidents, but focus on the development of strategies to reduce their likelihood. Following this principle, James Reason developed an acclaimed and widely-known accident causation approach, which evolved from Heinrich's et al. (1980) Domino Theory. Reason (1990) firstly developed the idea of having a combination of active failures and latent conditions to explain how complex systems can fail, later expanding it to a multi-barrier concept known as the Swiss Cheese Accident Model (Reason, 1997), which is widely used by academics and practitioners to describe the dynamics of accident causation. Successive cheese slices represent layers of defences, barriers and safeguards, all containing holes symbolising breaches caused by active failures and latent conditions. In the rare occasions when holes are perfectly aligned and all protective layers are overcome, an organisational accident will occur, usually having devastating consequences. A vital distinction between individual accidents and organisational accidents was highlighted by the theory, especially the risk that organisations will be tempted to rely on LTI (lost-time injury) or Bird's pyramid-type methodologies to demonstrate safety performance, overlooking latent conditions that degrade barriers and lead to major accidents. Many risk management approaches derive from the multi-barrier concept developed by Reason, believing that the underlying

www.manaraa.com

mechanisms causing organisational accidents can be correctly identified and properly managed. Human reliability approaches such as Human Factors Analysis and Classification System – HFACS (Shappell et al., 2007), Systematic Occurrence Analysis Methodology – SOAM (Licu et al., 2007) and the Sequentially Outlining and Follow-up Integrated Analysis – SOFIA (Blajev, 2002), and accident causation analysis methods such as Bow-Tie (Zuijderduijn, 2000) and Cause-Consequence Diagrams (Nielsen, 1971) are examples, to name but a few, of risk assessment techniques deeply aligned with Reason's approach.

Contemporary approaches on accidents causality models try to apply systems theory and system thinking (e.g. Leveson, 2011) to disclose deeper factors contributing to accidents, by adding higher hierarchical levels beyond immediate events and analysing the interactions among factors and broader circumstances. Examples are how public opinion and governments' movements influence the safety culture of an industrial sector. If the interaction among some of the constituent elements violates a set of constraints that guarantees the system safety integrity, an accident may occur. The focus of this systemic approach to accident causation is on understanding why the enforcement of constraints was unsuccessful.

A comparable perspective was previously conceived by Rasmussen's (1997) thoughts on system performance control. Instead of continually constraining individual elements to fit a pre-defined operational standard or limit, he focused on two features of system control theory: firstly, the need for adaptation of the system operation boundaries, i.e. increasing the margin from normal operation to loss-of-control; and secondly, increasing the awareness level of operational limits by making these boundaries visible to stakeholders. Rasmussen also noted that the pace of technology change is much faster than the modification time for management structures, and an even longer change lag is observed in higher hierarchical levels such as governments, regulations and society. This asynchrony defies risk modelling and challenges the rationale of using detailed methods and tools for analysing individual components or sub-systems, as satisfactory results in parts of a system might not reflect the safety status of the overall system.

Current research (Hopkins, 2002; Hollnagel et al., 2011; Arstad and Aven, 2017) highlights the need for taking into account the complexity and the dynamic nature of high-technology systems to prevent major accidents. In summary, these works discusses how it is crucial to

www.manaraa.com

challenge existing risk management assumptions, in order to identify oversimplifications and cope with the intricate interactions leading to the genesis of major events.

When the utmost objective is the verification and validation of risk assessments for hazardous industrial process plants in a dynamic and fast-changing environment, the complexity of the interactions among system elements must be recognised, along with the unpredictability of organisational behaviour and the inherent difficulties to foresee extremely rare, low-probability events, as highlighted by accident causation theorists. Additionally, designed safety barriers are not static and tend to degenerate through time. Factors such as ageing, maintenance shortcomings, budget constraints, personnel fluctuation and pressure towards cost-effectiveness, to name but a few, can contribute to defeat barriers and thus defence-in-depth concepts, which largely serve as a basis for risk assessment studies. Hence, how the confidence of wider stakeholder groups, such as the general public, investors and governments, which are particularly concerned with major accidents and might lack knowledge, interest or appropriate time to go into too much technicalities of risk assessment methods, can be enhanced?

The hypothesis underpinning the current work is that mapping patterns and common tendencies in major accidents, and demonstrating that these accident lessons can be fully understood and applied to new assessments in a logical and structured way, might reveal a realistic path to develop stakeholders' trust and to contribute to verification schemes.

1.2 Identifying common patterns and developing a risk assessment verification framework based on major accidents

The fact that accidents causation theories disagree whether a truthful representation of the multidimensional interactions in major events is achievable or not turns risk assessment verification and trust in risk management into a challenging research topic. Although any model will imply the reduction of the complexity of operational reality, some attributes can be extracted from accident causation models in order to establish an acceptable framework to verify the applicability and accurateness of risk management strategies.

It is disputed if the study of successful cases, as argued by high-reliability organisations theorists, will give some insight into the unusual, rare interfaces observed in major accidents. In contrast, the identification of common patterns arising from interactions

www.manaraa.com

between human factors, technological aspects and organisations during catastrophic events seems to be a reasonable approach to support a verification strategy for risk analysis, at least to certify that lessons learned from previous accidents were contemplated in current studies. This novel approach might help in reducing the gap pointed out by Skogdalen and Vinnem (2012) when analysing a number of quantitative risk analysis from the Norwegian Oil & Gas industry. They identified that human and organisational factors (HOFs) were not taken into account during the estimation of the probabilities of a blowout. In contrast, the Deepwater Horizon blowout was deeply associated with HOFs such as work practice, training, communication, procedures, quality control and management. Previous analysis of 238 major accidents (Moura et al., 2016) also indicated that 95% of these events presented some sort of organisational contribution to the undesired outcome, and 57% were directly associated with human factors, highlighting the importance of considering these significant features to develop realistic safety studies.

Barrier and defences-in-depth concepts will rely on the integrity and availability of the designed barriers to hold hazards or to minimise their consequences. Addressing common organisational and technological shortcomings contributing to the degradation of critical safety barriers can reveal tendencies which make them fail upon demand. The pattern identification process would also support the application of a safety check against recurrent damage mechanisms, reducing latent failures and providing useful data to endorse the expected positive effect of the barrier during a real event.

The disclosure of common patterns leading to major accidents will make operational boundaries visible to stakeholders, improving confidence in the decisions made and justifying the application of additional safety measures. The fact that the output will be directly associated with real events will facilitate the learning process and highlight the significance of addressing the identified concerns.

Therefore, this research will focus on the development of a risk assessment verification scheme, based on the interactions between human factors, technological aspects and organisations during major accidents. The collection of events constitutes the Multi-Attribute Technological Accidents Dataset (MATA-D) introduced by Moura et al. (2016), which captured major accidents occurred in high-technology industrial domains (e.g. aviation, oil & gas upstream, refineries and nuclear plants) and classified them under a common framework, the Contextual Control Model used as a basis for Hollnagel's (1998)

www.manaraa.com

Cognitive Reliability and Error Analysis Method. This previous work presented one of the most complete statistical analyses of major accidents from different industrial sectors in the open literature.

The application of an artificial neural network approach, specifically Kohonen's (2001) Self-organising Maps (SOM), will result in the conversion of complex accident data into 2-D risk maps. Events will be clustered by similarity, allowing the combined treatment of accidents with similar interactions but from distinct industrial segments. The development of the data visualisation provided by the SOM application will give rise to the development of a set of properties, attributes and recommendations for the verification of systems, safety barriers, human-machine interfaces and risk studies, enhancing risk perception and stakeholders' trust.

2. Analysis Method

2.1 Using a major-accident dataset as a reliable data source

Previous works have applied past accidents data to produce insight into the genesis of adverse events, in order to support researchers and practitioners by offering valuable contributions to the development of risk management strategies and to disclose contributing causes to accidents. Most of the existing datasets arise from accident/incident data reporting systems, and were voluntarily developed by companies/associations (e.g. DNV-GL World Offshore Accident Database, International Association of Gas Producers Process Safety Events Data), are enforced by states (e.g. UN International Civil Aviation Organization Accident Indent Data Reporting system – ADREP, UK HSE's Reporting of Injuries, Diseases and Dangerous Occurrences Regulations - RIDDOR) or are maintained by research centres (e.g. Paul Sherrer Institut's Energy-related Severe Accident Database – ENSAD). These efforts to collect data are extremely valuable, but commonly refer to a single industrial sector (Baysari et al., 2008, Evans, 2011) or attempt to embrace from occupational accidents to process safety events (Bellamy, 2007, 2013). Generally, reporting systems also include a category called near-misses, which are hazardous occurrences that did not result in a loss/injury but had the potential to do so.

The events' scrutiny level during the data acquisition stage will involve some expected variations, as it will mostly depend on the consequences of the event and secondly on the societal interest in the subject. Consequently, near-misses will be directly reported by

www.manaraa.com

companies, with the regulating body using this summarised data to develop performance indicators or to trigger further actions such as inspections. Regulators can investigate occupational accidents directly, or validate/rely on companies' internal investigation procedures. Major accidents usually capture the media's and societal attention, pushing governments and regulators to react accordingly. Due to the wide-ranging consequences observed, this type of event requires consistent investigation processes, usually undertaken by one or more regulators, independent investigation commissions or both. The European Safety, Reliability and Data Association (2015) has recently recognised that these events trigger comprehensive examinations concerning preventive and protective systems, along with a careful consideration of factors and surrounding conditions leading to accidents. An illustrative example would be the Transocean's drilling rig Deepwater Horizon blowout and explosion occurred in the Gulf of Mexico in April 2010, which was investigated by the licensee (BP, 2010), regulators (USCG, 2010, BOMRE, 2011), an independent agency (US-CSB, 2016) and academic study groups (CCRM, 2011). Beyond doubt, catastrophic events lead to meticulous examinations and produce very detailed data about the conditions in which operations were inserted. Attributable to this extraordinary level of scrutiny, the data produced is indisputably more reliable and complete than any alternative source of information regarding accident causation.

2.2 The SOM data mining applied to the MATA-D

The current version of the MATA-D, containing 238 major accidents from different high-technology industries (e.g. aviation, hydrocarbons exploration and production, refining, chemical industry, nuclear) will be used as a data source for this research. The dataset was fed from detailed major accident investigation reports, obtained from reliable sources such as regulators, independent investigation commissions and insurance companies (Moura et al., 2016). The dataset framework comprises 53 factors distributed in three main categories: man, technology and organisation. The structured but comprehensive nature of the MATA-D framework allowed for the effective application of several data mining approaches in previous research (e.g. Doell et al., 2015, Moura et al., 2015b, 2015c), such as agglomerative clustering methods, association rule mining techniques and neural networks. Cross-industrial common patterns in major events as well as significant relationships among contributing factors were successfully disclosed.

www.manaraa.com

In this work, key interfaces between human factors, technological aspects and organisations will be identified through the application of a suitable artificial neural network technique, namely self-organising maps - SOM (Kohonen, 2001). This data mining approach is especially effective when an unsupervised method (i.e. the number of clusters or final categories in the output space are unknown) and the classification and visualisation of high-dimensional data are needed (Kohonen, 2013; Ultsch, 1993). Data mining efforts will result in the reduction from 53 dimensions (or contributing factors per accident) to two-dimensional maps. The 2-D SOM maps will be generated with the support of specialised software (Viscovery® SOMine expert version), to enhance the features' visualisation and facilitate the interpretation of the SOM output.

2.3 The SOM construction rationale and further data mining settings

The self-organising maps (SOM) is a widely used clustering and data classification approach developed by Kohonen (2001). It holds important properties to group data by similarity and regarding the preservation of the input data, enabling visual representation possibilities for multidimensional datasets. Proportionally to the amount of data, the computational complexity of the SOM can be considered low and it is an easy-to-implement algorithm (Cottrell et al., 2016), allowing its straightforward usage on practical applications, with minor adjustments.

In the current study, the objective of the data mining process is to provide an improved but simplified organisation and visualisation of the input data, which consists of a 238 x 53 matrix (i.e. 238 major accidents containing up to 53 contributing factors). The SOM output is a topographic two-dimensional map, where accidents with analogous interactions among contributing factors are mutually attracted and contiguously positioned in a general grid. In order to highlight some specific interactions, individual heat maps containing the presence or absence of single properties are also plotted. The clustering process by similarity, in conjunction with the examination of the individual properties' maps, enables the observation and interpretation of common tendencies associated with the major accidents contained in the MATA-D.

Basically, the neural network is trained according to Eq. 1 (Kohonen, 2001), which indicates that the position at the grid will be occupied by the model *m* that minimises the distance between the input vector *x(t)* and an output node m_i.

www.manaraa.com

$$v(t) = \arg\min_{i\epsilon\Omega}\|x(t) - m_i(t)\| \qquad (1)$$

In the output space, a neighbourhood function h_{ji} will define the influence zone around the winning output node (the one which is the closest to the input vector), which will be updated through the batch-learning rule (Eq. (2)) developed by Kohonen (2013) to eliminate possible convergence problems. The best matching node m_i^* will be located at the centroid of the influence region defined by the neighbourhood function h_{ij}; the $\overline{x_j}$, which represents the mean value of a group of input vectors *x(t)* previously defined by *v(t); and* the number n_j of input space samples *x(t)*.

$$m_i^* = \frac{\sum_j n_j h_{ji} \overline{x_j}}{\sum_j n_j h_{ji}} \qquad (2)$$

The sequence will be repeated until the map converges, i.e. until the models for the input vectors are accurately represented in the output space. Due to the neighbouring properties, the more contributing factors in common they have, the closer the vectors will be located in the output. If more than one model in the output space contained exactly the same contributing factors, they would be positioned in the same grid node.

In the current study, the tension of the neighbourhood function (or the radius of the neighbourhood Gaussian function) was defined as the smallest value to produce meaningful clusters and maintain a close resemblance among adjacent neurons, and the map converged after 111 batches. Further details on the SOM algorithm, the network settings, the choice of the neighbourhood function and the clusters' quality criterion for the specific application can be found in Moura et al. (2017b).

After the application of the SOM algorithm, the clusters where the highest incidence of interfaces was identified during major accidents will become apparent. Further examination of the intricate relationship among contributing factors within the clusters of interest will reveal common patterns and accident tendencies, highlighting principles that must be taken into account when developing risk assessment studies.

The conversion of relevant interfaces in a set of principles will support the verification of risk analysis and risk management documents, by applying the lessons learned from major accidents. Accordingly, a straightforward requirement list to be crosschecked against risk

www.manaraa.com

studies will be developed, and further implications to enhance stakeholders' trust will be then discussed.

3. Results

The application of the SOM algorithm to the MATA-D dataset resulted in four different accident clusters containing dissimilar influencing factors, as shown in Figure 1. The contributing factors label sizes are proportional to their effect within the grouping. For example, the Inadequate Task Allocation factor in Cluster 1 (blue) occupies 95% of the total cluster area, while Wrong Place occupies 52.5%, and the Incomplete Information frequency is 36.2%. This is one example of the usage of the visualisation power of the clustering method to interpret accident data. Figure 1 synthesizes information from a 238 x 53 Matrix (number of major accidents x possible contributing factor per event) in a single 2-D image.

Figure 1. MATA-D SOM Clustering output labelled by most relevant contributing factors

The first cluster (blue) covered 35% of the SOM map area, containing the highest number of data points, with 34% of the accidents. Cluster 2 (red) has 25% of the total area and 24% of the dataset. The third grouping (yellow) occupies 20% of the total area and has the lowest event's frequency, with 16%. Cluster 4 (green) also holds 20% of the map area, but

www.manaraa.com

embraces 26% of the dataset events. Figure 2 depicts the rate of contributing factors per event, discriminated by clusters.

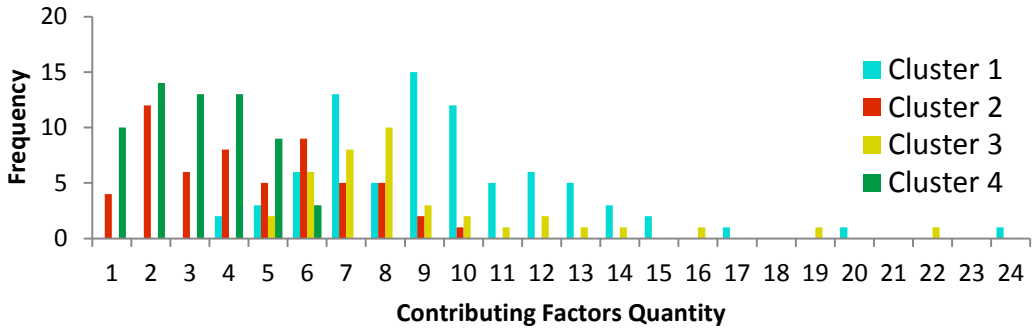

Figure 2. Number of Contributing Factors Histogram

Figure 2 shows Cluster 1's events with four to twenty-four contributing factors per accident and mode of nine, as it appeared in fifteen events. 86.2% of the accidents within this cluster have seven or more contributing factors, constituting a very rich grouping for further interpretation. Cluster 2 events were influenced by one to ten features with 72.2% of the grouping having six or less contributing factors, while the totality of the events in Cluster 4 have six or less features. Both groupings show the same low mode of two factors, indicating a lower prospect for the identification of multiple interactions among contributing factors. For Cluster 3, the total number of contributing factors per accidents varied from five to twenty-two. 79.5% of the events contained seven or more contributing factors, with eight factors the mode value. This grouping also tends to provide good opportunities for enhanced interpretations of the genesis of major accidents.

Results show that the application of the SOM algorithm largely improved the visualisation of interfaces, by confining events with lower frequency of contributors in Clusters 2 and 4, as well as elevating the features' mode for Clusters 1 and 3, highlighting special structures within the dataset.

Table 2 details the results of the SOM clustering, indicating the outcome of the data mining process for selected contributing factors, in relation to the overall dataset. The variation columns compare the overall dataset statistics with the individual factors' influence in each cluster. Negative or very low variations are not indicated, as the preservation or reduction of the frequency of a contributing factor in a grouping (in relation to its overall incidence) means that the factor was not significant to the formation of the cluster. Twenty-seven

www.manaraa.com

features contributed to less than 10% of the individual clusters and will not be represented, due to their low significance to the groupings formation. Contributing factors with strong dominance (more than 50% of the individual cluster areas) are highlighted, as well as frequencies higher than 10% and with positive cluster effect in relation to the overall dataset.

Table 2. Dataset overall statistics vs. clustering distribution for significant features

Contributing Factor	Overall	C1	Effect	C2	Effect	C 3	Effect	C 4	Effect
Wrong Time	14.7%	13.8%	-	10.5%	-	**41.0%**	+178.8%	3.2%	-
Wrong Type	11.8%	11.3%	-	7.0%	-	**30.8%**	+161.8%	4.8%	-
Wrong Place	31.5%	**52.5%**	+66.6%	**36.8%**	+16.8%	12.8%	-	11.3%	-
Observation Missed	15.5%	**20.0%**	+28.6%	12.3%	-	**23.1%**	+48.6%	8.1%	-
Faulty diagnosis	13.0%	**26.3%**	+101.9%	8.8%	-	12.8%	-	0.0%	-
Wrong reasoning	11.3%	**20.0%**	+76.3%	1.8%	-	**25.6%**	+125.7%	0.0%	-
Decision error	9.2%	5.0%	-	**17.5%**	+89.3%	**17.9%**	+93.6%	1.6%	-
Inadequate plan	9.7%	10.0%	-	7.0%	-	**25.6%**	+164.9%	1.6%	-
Priority error	7.1%	6.3%	-	8.8%	+23.2%	**15.4%**	+115.6%	1.6%	-
Distraction	5.9%	**11.3%**	+92.1%	3.5%	-	7.7%	+30.9%	0.0%	-
Cognitive bias	7.1%	**15.0%**	+110.0%	1.8%	-	**10.3%**	+44.2%	0.0%	-
Equipment failure	55.0%	33.8%	-	22.8%	-	**94.9%**	+72.4%	**87.1%**	+58.2%
Inadequate procedure	44.1%	**78.7%**	+78.4%	42.1%	-	38.5%	-	4.8%	-
Incomplete information	17.6%	**36.2%**	+105.1%	7.0%	-	**20.5%**	+16.2%	1.6%	-
Communication failure	10.5%	**16.3%**	+55.2%	5.3%	-	**20.5%**	+95.2%	1.6%	-
Missing information	20.6%	**37.5%**	+82.1%	14.0%	-	15.4%	-	8.1%	-
Maintenance failure	34.9%	**56.3%**	+61.4%	14.0%	-	33.3%	-	27.4%	-
Inadequate quality control	60.9%	**81.3%**	+33.4%	24.6%	-	**79.5%**	+30.5%	56.5%	-
Management problem	9.2%	**12.5%**	+35.2%	5.3%	-	**23.1%**	+149.9%	0.0%	-
Design failure	66.0%	**85.0%**	+28.9%	50.9%	-	**87.2%**	+32.2%	41.9%	-
Inadequate task allocation	60.1%	**95.0%**	+58.1%	**68.4%**	+13.8%	48.7%	-	14.5%	-
Social pressure	7.1%	**17.5%**	+145.0%	3.5%	-	0.0%	-	1.6%	-

www.manaraa.com

Insufficient skills	36.1%	**56.3%**	+55.8%	12.3%	-	**76.9%**	+112.8%	6.5%	-
Insufficient knowledge	35.3%	**60.0%**	+70.0%	17.5%	-	**56.4%**	+59.8%	6.5%	-
Adverse ambient conditions	7.1%	2.5%	-	**14.0%**	+96.0%	**10.3%**	+44.2%	4.8%	-
Irregular working hours	3.8%	**10.0%**	+164.4%	1.8%	-	0.0%	-	0.0%	-

Figure 3 summarises the most relevant contributing factors to the formation of the clusters, rearranged by categories according to the dataset framework.

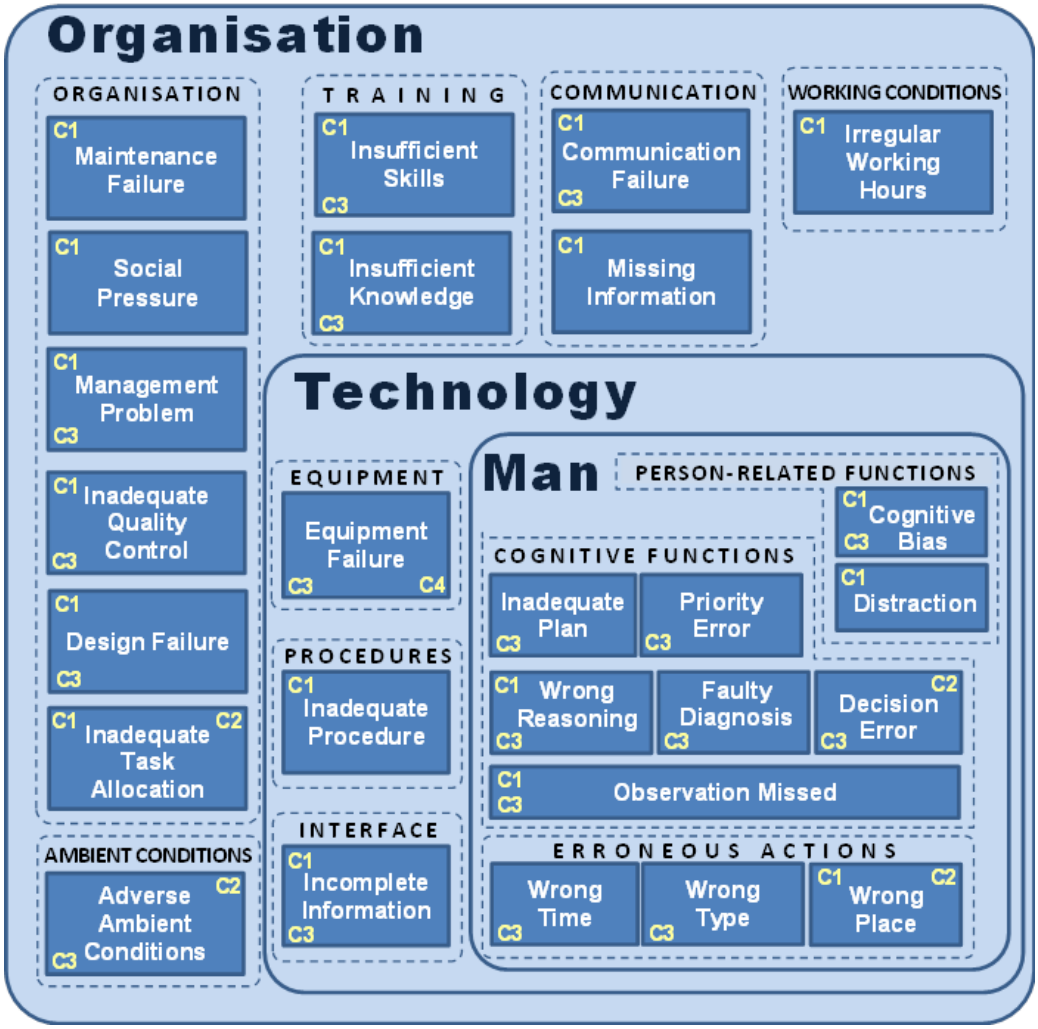

Figure 3. Categories of the most significant contributing factors per cluster

From a human factors perspective, Cluster 1 accidents were dominated by the Wrong Place phenotype, when an action from an expected sequence is skipped, carried out in the incorrect order or substituted by an unrelated movement. Action errors interfaced with intermediate levels of human cognition, as operators were required to observe a signal or

www.manaraa.com

event (observation missed) and diagnose a situation or system state (faulty diagnosis). Inference or deduction errors (wrong reasoning) were also observed. This was the grouping where person-related features were more significant, as shifts in attention (distraction) or constraining the information search to confirm a pre-defined hypothesis, attributing events to specific factors or believing that actions have controlled the system state developments (cognitive bias) contributed to 11.3% and 15% of the cluster, respectively. Technology issues included procedure shortcomings (78.7% of the cluster) and situations where the information provided by the system interface was poor (incomplete information). Many organisational issues interacted within the cluster. Inadequate Task Allocation (95%), Design Failure (85%) and Inadequate Quality Control (81.3%) were the most significant ones, but training (Insufficient Skills and Insufficient knowledge) and communication issues (Communication Failure and Missing information) were considerable as well. Maintenance issues were visible in 56.3% of the cluster, and the effects of other organisational aspects such as social pressure (17.5%), management problem (12.5%) and irregular working hours (10%) were also majored by the application of the clustering technique.

Cluster 2 has Inadequate Task Allocation as the most relevant factor, covering 68.4% of the grouping, followed by an erroneous action (Wrong Place) associated with an inability to decide, a partial/incomplete decision or making the wrong decision among alternatives (decision error). Accidents where Adverse Ambient Conditions were significant are mostly grouped within this cluster.

As indicated by Figure 2 histogram, Cluster 3 shows several important interactions among contributing factors, being a rich grouping for further interpretation. Many action errors were captured during the investigation of these events, where movements were performed earlier or later then required (Wrong Time), or with insufficient force, wrong speed, direction or magnitude (Wrong Type). Erroneous actions were accompanied by all three levels of cognition (observation, interpretation and planning). The fact that complex cognitive functions such as Inadequate Plan (25.6%) and Priority Error (15.4%) contributed to the formation of the cluster, together with observation missed (23.1%), wrong reasoning (25.6%) and decision errors (17.9%), gives us an opportunity to understand how cognitive functions leading to erroneous actions interact with organisational and technological aspects. Equipment failures contributed to almost the totality of the grouping. As in Cluster 1, Design Failure, Inadequate Quality Control and training (Insufficient Skills and Insufficient Knowledge) records were very high, and other aspects such as incomplete information and

www.manaraa.com

communication failure were also significant for both groupings. Management problems were observable in 23.1% of Cluster 3.

Cluster 4 is largely dominated by Equipment Failures (87.1%), the only noteworthy factor to influence the formation of grouping.

Figures 4 to 22 represent the cluster results for individual features. They give further insight into the general map (Figure 1), in the sense that the interactions among individual contributing factors can be visualised. Figures are read as topographical or heat maps, where one can directly observe the regions of the general map affected by individual properties or dimensions. In the current work, blue tones indicate the absence of the contributing factor, while red tones represent its manifestation. Shadowed regions highlight and exemplify special interactions among contributing factors.

Two graphical methods will be used to present individual maps and highlight the main results for further discussion:

(i) disclosing multiple intersections (superposition of images) of the most frequent contributing factors, which represent strong interaction patterns between human factors, technology and organisations (e.g. Figures 4 to 10 and 18 to 22); and

(ii) analysis of special features (e.g. communication issues in Figures 11 to 14, human-related factors in Figures 15 to 17).

In Cluster 1, three map regions (1A, 1B and 1C) represent the intersection between Inadequate Task Allocation, Design Failure, Inadequate Quality Control and Inadequate Procedure (Figures 4 to 7). Region 1A is deeply related to Insufficient Knowledge (Figure 8), while 1B is mostly associated with Insufficient Skills (Figure 9). Accidents represented in 1C tend to combine with Maintenance Failures (Figure 10).

www.manaraa.com

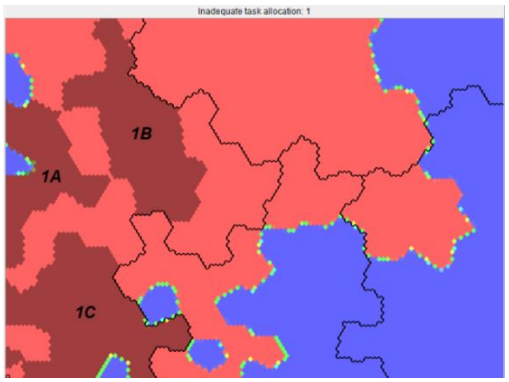

Figure 4. Inadequate Task Allocation Map

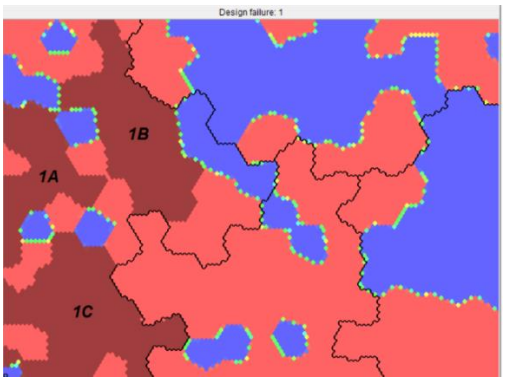

Figure 5. Design Failure Map

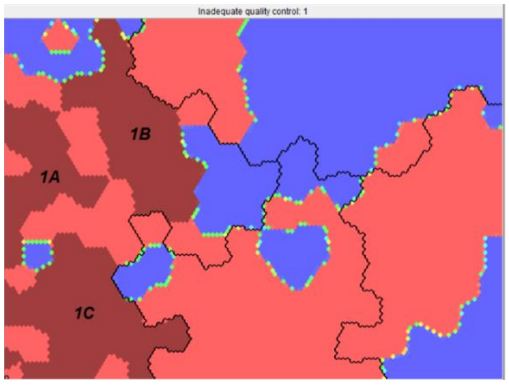

Figure 6. Inadequate Quality Control Map

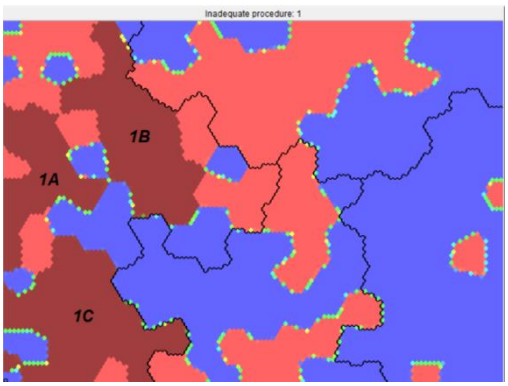

Figure 7. Inadequate Procedure Map

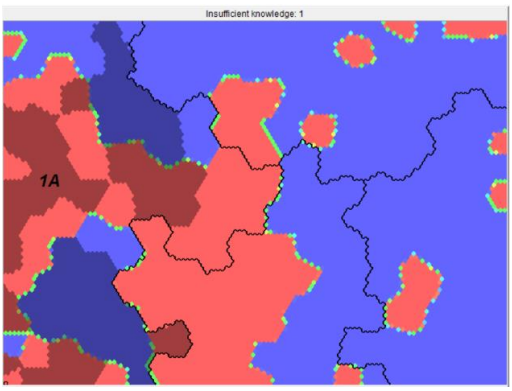

Figure 8. Insufficient Knowledge Map

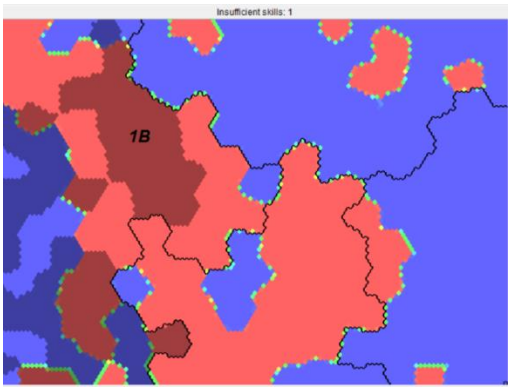

Figure 9. Insufficient Skills Map

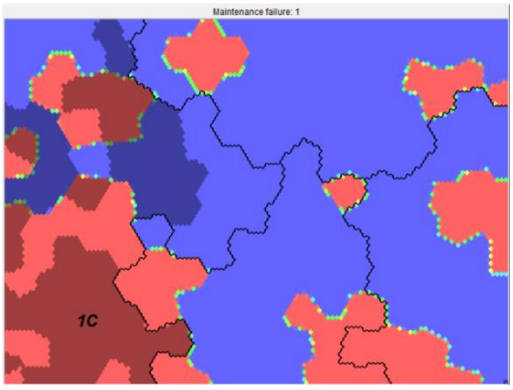

Figure 10. Maintenance Failure Map

www.manaraa.com

Figures 11 and 12 present the SOM maps for communication issues. These issues largely overlapped Inadequate Task Allocation in Cluster 1, as can be seen in the shadowed region in Figure 13. Exceptions are the two small-circled areas, where task allocation issues were substituted by the person-related feature named Cognitive Bias (Figure 14).

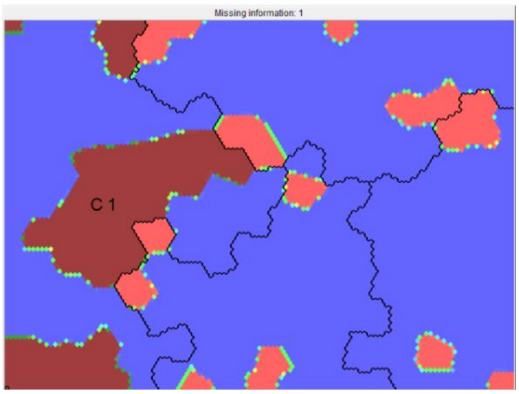

Figure 11. Missing Information Map

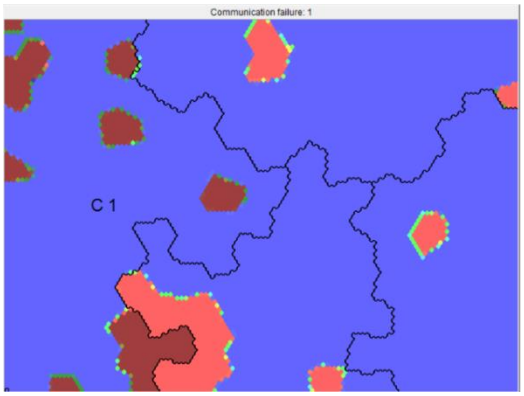

Figure 12. Communication Failure Map

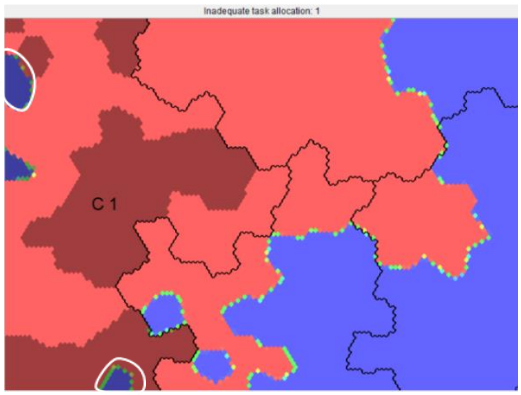

Figure 13. Inadeq. Task Allocation Map

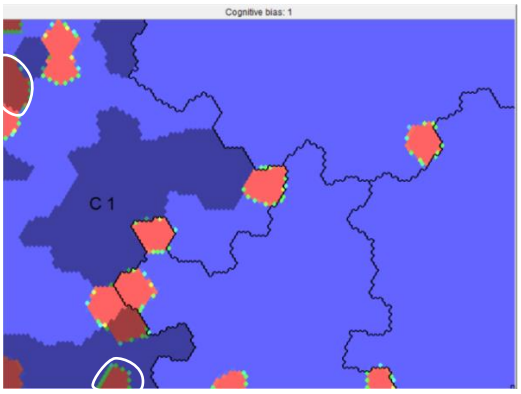

Figure 14. Cognitive Bias Map

64.1% of Cluster 3's area contained two erroneous actions: Wrong Time (Figure 15) and Wrong Type (Figure 16). The faded region depicts the incidence of the three levels of specific cognitive factors within this grouping, showing the human-related contributing factors' representation. Consequently, a combination of observation (Observation Missed), interpretation (Wrong reasoning and Decision Error) and mental planning (Inadequate Plan and Priority Error) was expected to take place, suggesting that a profounder judgement of the confronted situation was necessary to solve system deviations. It can be observed that a technological issue (Incomplete Information – Figure 17) interacted with erroneous actions related to timing in the regions where specific cognitive functions are not identified,

www.manaraa.com

suggesting that supervisory control system and data display limitations led to some of the Wrong Time occurrences. These areas are circled in Figure 15.

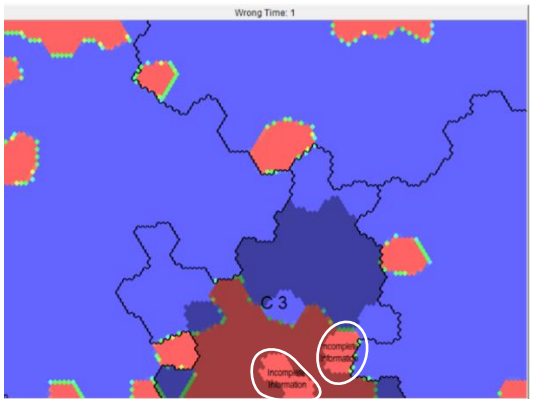

Figure 15. Wrong Time Map

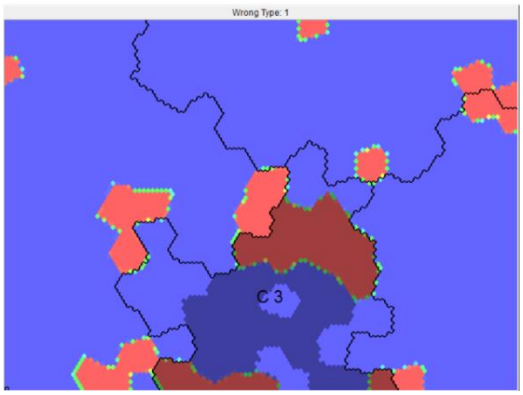

Figure 16. Wrong Type Map

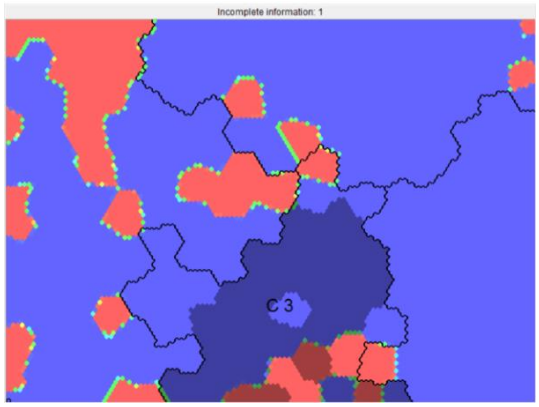

Figure 17. Incomplete Information Map

Figures 18 to 22 show how the main technological (Equipment Failure) and organisational aspects (Quality Control, Design Failure and training) interacted among them and with human-related issues (shadowed region) to result in system control problems within Cluster 3. The shaded region is 79.5% of the grouping area, representing the incidence of human erroneous actions, specific cognitive functions and person-related functions.

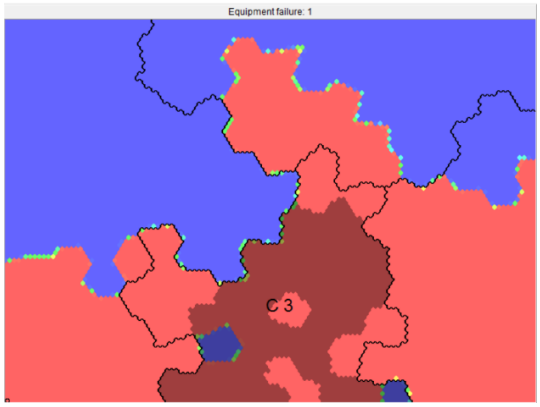

Figure 18. Equipment Failure Map

www.manaraa.com

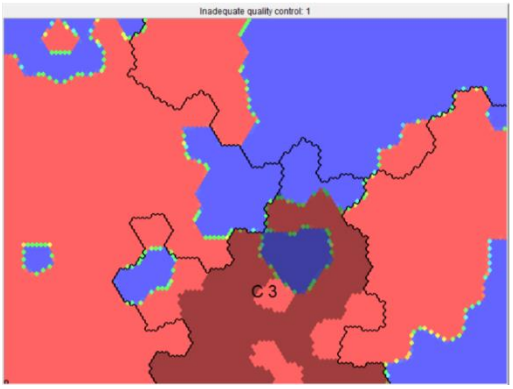

Figure 19. Inadeq. Quality Control Map

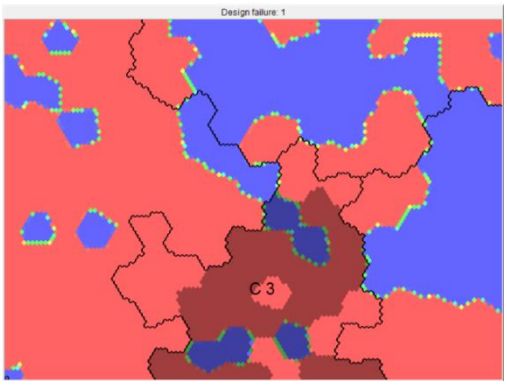

Figure 20. Design Failure Map

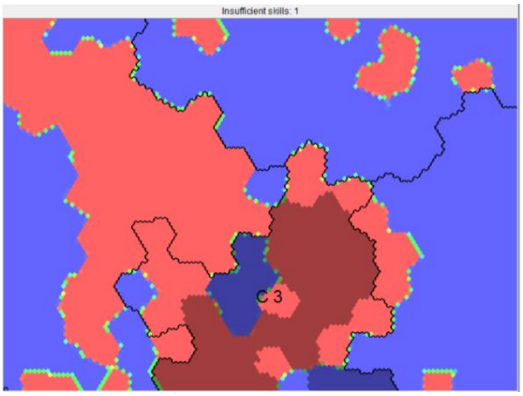

Figure 21. Insufficient Skills Map

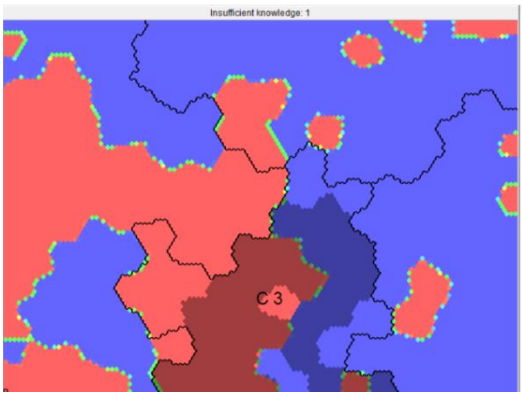

Figure 22. Insufficient Knowledge Map

4. Discussion

4.1 Main Clusters Interpretation

The analysis of the maps indicate an intricate combination of factors contributing to the major accidents contained in the MATA-D database, including the significance of the human factors to the undesirable outcome. Previous studies (Graeber, 1999, McLaughlin et al., 2000, Leveson, 2004) using different industrial sectors as a data source also emphasised the importance of considering human issues when assessing risk, relating between 70% to 80% of accidents to some kind of operator error. Therefore, it seems to be clear that a satisfactory risk assessment study must take into account the relationship between humans, technology and organisations to convey realistic scenarios. Otherwise, the safety analysis will not offer a trustworthy and sufficiently broad view of the major hazards that industrial facilities are exposed to throughout their lifecycle.

www.manaraa.com

So why has limited attention, especially if compared with traditional risk assessment approaches focused on engineering technical systems, been paid to the consideration of human factors in risk studies (Hollywell, 1996; Skogdalen & Vinnem, 2011, 2012)? When analysing occupational risk assessments, Cuny and Lejeune (2003) pointed out some problems to the consideration of the human influence, particularly the preparation of data for processing and the estimation of probabilities to feed deterministic approaches. The complexity of organisational interfaces and the variability of human behaviour also make a socio-technical system modelling a challenging task, maybe explaining the reason behind the disproportionate focus on purely technical aspects and discrete components in risk evaluation.

The interpretation of the maps enables the possibility of considering the whole range of contributors without previous assumptions of their conjectural importance, focusing on their interactions and on the disclosure of tendencies, instead of concentrating on individual factors. The application of the SOM algorithm and the joint analysis of maps highlighted topographical areas containing similar interfaces, allowing a targeted examination of the genesis of the MATA-D accidents and the development of an attribute checklist with the most frequent observations. Some of these interfaces will be illustrated with the accident narratives as positioned in the map, all accessible through the MATA-D database. Examples of specific items developed to raise the awareness for the discussed interactions will be given, and the complete list will be presented in Table 3.

An analysis of Cluster 1 accidents from area 1A (Figure 8) indicates that these events are related to situations where components were designed and implemented on an individual fashion, rather than as a holistic system. A deeper examination of the contributing factors description for the major accidents contained within this region, according to the MATA-D stored data, indicates that safety studies failed to adequately address risks related to the system interaction with the environment as well as possible interferences among individual components. The shortcomings in design, procedures, quality and task allocation joined the loss of situational awareness during operation, and insufficient theoretical knowledge led to the misperception of risks. A practical example of this tendency was the widely-known Varanus Island incident in June 2008 (Bills & Agostini, 2009), when a pipeline rupture and explosion caused a shortage in the gas supply for Western Australia, resulting in three billion Australian dollars in economic losses. In summary, the lack of an integrated approach to design and risk management led to problems in the cathodic protection system, most

www.manaraa.com

likely due to electrical interferences from adjacent pipes and other structures, causing alternating current corrosion. The assumption that safeguards are always active and the sense that their failures are unconceivable are also patterns observed within the grouping. In order to ensure that these common major accident tendencies are addressed by risk studies, it is suggested that holistic verification questions (e.g. items 10, 11, 15 and 59 of the checklist in Table 3) should be developed to raise reviewers and designers' risk awareness level.

Accidents within area 1B (Figure 9) presented situations where process changes undermined the original recommendations from risk assessment studies. Equipment or system replacements, product modifications and procedures updates lacking a proper hazard evaluation (or management of change) enabled the deterioration of the system. The necessary training to operate under the new conditions was also insufficient, causing a human performance failure. The verification checklist items 4, 5, 23 and 33 are examples of checkpoints aimed at neutralising these accident patterns highlighted by the MATA-D data mining using the SOM.

The shadowed region 1C (Figure 10) contained many events where seemingly minor maintenance issues, i.e. keeping vessels and pipes free of deposits, consumable parts (e.g. filters) replacements, lubrication and calibration, drains obstruction and dust/particles accumulation, were combined with quality problems, task allocation issues, design shortcomings and inadequate procedures to generate a major failure. These common accident causation trends gave rise, for instance, to the items 26, 27, 28, 29 and 39 of the verification checklist.

Figures 11 and 12 highlighted the map regions where communication problems attained their highest incidence, mostly combined with task allocation issues (Figure 13). These events were prone to poor communication between workers, which was made worse by background noise (mainly alarms and usual process sounds) or by the low quality of the transmission. Deficiencies in reporting to supervisors some unusual situations observed in the process plant and to convey important information from hazard studies to the personnel were frequent within this grouping. In addition, data transfer from paper to computer-based systems, incorrect coding and poor communication between shifts were risk-increasing factors commonly observed.

www.manaraa.com

Through the results shown in Figures 13 and 14, it is possible to scrutinise a few regions where inadequate task allocation was not as relevant as in the rest of the cluster. Nonetheless, communication issues tended to interact with person-related issues such as a Cognitive Bias, particularly when critical information was not communicated, supporting an illusion that actions taken were sufficient to control the situation, or when actions were constrained by a strong (and wrong) assumption of the current system status. An example extracted from these regions would be the 2011 helicopter crash in Missouri (NTSB, 2013) during a patient transfer from one hospital to another, which resulted in 4 fatalities. The Pilot knew that he has misinterpreted the fuel level to some extent (he reported 26% or forty-five minutes of fuel in the pre-flight check, but post-accident investigation indicated only 18%, or a thirty-minute supply), but his alternative refuelling plans were constrained by the hypothesis that he was able to reach a station 34 minutes away from the departure point. Having visual contact with the refuelling point (three-minute distance) when the gauge indication approached to zero, the pilot sustained his course (instead of landing immediately) until fuel exhaustion. A communication with qualified land-based staff (available at the Operational Control Centre) would have exposed his plans as inadequate. Other interesting tendencies were also identified in the cluster region, such as having the attention caught by phone calls or texting using portable devices.

Examples on how to check if the tendencies identified by the interpretation of Figures 11 to 14 SOM maps were adequately tackled by safety studies are presented on items 19, 21, 34, 35, 36 and 65 of the verification list in Table 3.

Cluster's 3 erroneous actions and cognitive functions' frequencies are generally higher than in any other grouping, especially the most complex ones, involving the need for mental planning. These human-related factors merged with design shortcomings, equipment failures and quality control issues. A tendency to underperform under non-standard operations (e.g. start-up or partial plant operation) was also observed, repeatedly combined with training issues (Figures 21 and 22). Cases where an equipment failure caused a shutdown, and operators focused on fixing the equipment and restarting it without further consideration are recurrent in this grouping. Some of the common failure modes observed are: (i) catastrophic failures due to the hot flow of products into cold pipes and vessels (brittle fractures); (ii) valves and seals which were damaged or partially closed/opened during a pause in operations and were not inspected (a quality control problem) before the restart; and (iii) omitting to realign valves and restart

www.manaraa.com

control/signalling/alarm systems. After the identification of specific patterns in Cluster 3, some suggestions on how to check if safety studies considered these interactions are given by items 30, 32 and 33 of the risk verification checklist.

The grouping also contained some regions where insufficient information from supervisory control and data acquisition systems shaped human erroneous actions (Figures 15, 16 and 17). The growing dependence on information systems is a pattern to be considered when assessing hazards, thus verification schemes must verify if the risk growth due to inadequate/unsatisfactory human-machine interfaces is carefully addressed. The lack of direct indications of problems; panels not providing accurate process overviews; information that is not displayed in relevant places (e.g. in the control room and/or locally); general/critical alarms not taking precedence in relation to local, less important alarms; delays in the information presented, undermining operators' efforts to diagnose system status; and incorrect information display are some of the human-machine interface problems extracted from Cluster 3. These accident causation tendencies resulted in the development of the items 37, 38, 62, 63 and 64 of the proposed example of a safety study verification checklist.

4.2 An Application Example for Safety Studies Verification

A safety study generally comprises a planning process (describing the context, regulatory requirements, scope of the study, risk acceptance criteria etc), a hazard identification phase, a risk assessment (e.g. events frequencies, reliability, event modelling, consequences, level of risk estimation) and a final report (e.g. presentation of results, uncertainties appraisal, recommendations, study quality assurance), to generate input to the decision-making process.

Those stages involve different techniques, combining quantitative (e.g. probabilistic analysis), semi-quantitative (e.g. fault-trees) and qualitative (e.g. Failure Modes, Effects and Criticality Analysis – FMECA; Hazards and Operability Studies – HAZOPs) approaches. The wide range of techniques and possibilities to assess risk turn the verification and validation of safety studies into a challenging task, especially if it is recognised that a non-integrated approach to validation may result in relevant gaps in the overall consideration of risks, leaving outside the scope important interactions that might contribute to major accidents.

www.manaraa.com

The international standard for quality management systems (ISO 9001, 2015) defines verification as the process to ensure that input requirements are met by design and development outputs. It includes activities which aim to certify that the results of the safety study are aligned with the chosen assessment approach and accurately reflect the conceptual description of the system/facility. Correspondingly, validation (ISO 9001, 2015) includes a set of activities performed with the intent to ensure that the output meet the requirements for the projected usage. This process aims to confirm that the safety study contains a sound representation of risks, considering the intended application of the model. Therefore, the current study contributes to verification activities by providing practical means to confirm if lessons from past major accidents have been contemplated by safety assessments. The ultimate objective is to ensure that patterns and tendencies leading to disasters are anticipated and mitigated, thus assisting the development of societal and stakeholders' trust on safety studies.

Once the application of the SOM algorithm successfully supported the disclosure of common patterns in major accidents, the interpretation of the most important interactions can be further used to check if safety studies present a consistent representation of risks, by testing its robustness against the complex and realistic scenarios extracted from the MATA-D.

An example of how to use the accident patterns to contribute to verification schemes is given in Table 3. Accident tendencies disclosed by the application of the SOM approach and the consequent analysis of the maps, as illustrated in section 4.1, are being used to construct a checklist comprising common hazards, major risks and shortcomings involving the interactions between humans, technology and organisations. The checklist aims to give some insight into how these lessons learned from past accidents in different industrial environments can be used as part of a verification scheme, to ensure that recurring accident causation patterns will not escape from scrutiny in new safety studies. A general, comprehensive language is being used, in order to facilitate the direct application of the list or the integration with existing verification and validation approaches.

www.manaraa.com

Table 3. Checklist for risk studies verification

No.	*Item*	*Yes*	*No*	*n/a**
01	Were the premises, hypothesis and justifications for the chosen design concept clearly stated? Was a safer known alternative/approach to achieve the same objective discussed?			
02	Are the underlying basis and limitations of the method, the origin of the input data and further assumptions (e.g. duration of an event, flammable vapour clouds expected drifts, maximum spill size, release composition) that support probabilities, scenarios and results clearly stated? Are they consistent?			
03	Are events' frequencies used in probabilistic risk analysis reliable? Are they used exclusively when historical data is comparable (e.g. same operation type, facility or equipment)? Would alternative approaches (e.g. non-frequentist) be more suitable to estimate the events' likelihood in the study case (e.g. no sufficient past experience or previous operation data)?			
04	Although some regulations prescribe periodic reviews to risk studies, there is a tendency that assessments may fall into disuse due to people, process or environmental changes in between revision deadlines. Modifications usually lead to a management of change and some sort of risk analysis, but more complex, previous deeper safety studies are not revisited at this point. Are design verifications, as-built drawings, production checks, field data collection or other approaches required to confirm/maintain trust on the major/approved risk study throughout the facilities' lifecycle, instead of using a rigid deadline for review? Have the facility's critical factors / performance indicators that could indicate an up-to-date and trustworthy risk assessment been identified/listed?			
05	Were possible critical changes affecting the original studies (e.g. in the operational philosophy, control logic and process modernisations) acknowledged? Are the conditions with the potential to invalidate the current safety study clearly stated?			
06	The safety studies must contemplate a list of recommendations and safeguards, which can be rejected on a technical basis. Is the value of the implementation of risk reduction measures clearly stated? Are the justifications for favoured alternatives or rejections consistent with the best available knowledge? Do the underlying principles for rejections contemplate safety benefits over cost matters?			
07	Is the data extracted from databases and standards (as well as calculations made) logical, traceable and consistent with the operational reality?			
08	Were previous assessments in analogous installations used to give some insight into the hazard identification process?			
09	Were the recommendations and risk control measures previously applied to analogous facilities? Is there any feedback about their suitability from previous designers and operators?			

www.manaraa.com

10	Safety studies have shown a tendency to fail to adequately address risks related to the system interaction with the environment as well as possible interferences among individual components and systems. Was a comprehensive and integrated approach to design and risk management achieved? Were components and systems designed and implemented in a holistic way rather than on an individual and secluded fashion? Are human factors analysis integrated with engineering studies?			
11	Some high-technology facilities are likely to start their operations before the whole system and all safeguards are in place. Offshore platforms may have to adapt their process while a pipeline is not operating or a pump/compressor is not commissioned. Refineries may be designed (or obliged) to operate without some processing modules, due to technical or economic reasons. Does the risk assessment contemplate all modes of operation (e.g. commissioning, start-up, partial operation, maintenance breaks) for the facility examined? Are transitory states (e.g. warm-up and cooling down times) also considered?			
12	Have the studies taken into consideration thermal properties, hydraulics and electrical/electronic parts of components, equipment and systems, not being overly focused on mechanical/structural aspects?			
13	Equipment and structural failures tended to arise from problems during the material selection stage and due to poor understanding and monitoring of well-known damage mechanisms. Has the material selected for construction, equipment fixation, pipelines and support structures identified and analysed by safety studies? Was a compatibility assessment (with loads, system and environment) conducted, including thermal, chemical and electrical properties?			
14	Are the specificities of the assessed facility or process clearly identified, in a way that specific risks will be identified and addressed? Where expert advice is required to assess risk, are the correspondent technical reports included in the safety studies (e.g. to assess the possibility of catastrophic failures due to stress corrosion cracking in stainless steels, or corrosion mechanisms emerging from the saturation of wet hydrocarbons with dissolved carbon dioxide and sour environments)?			
15	Are risks associated with the interaction of different materials addressed (e.g. with different temperature gradients leading to deformations and ruptures or with distinct electric potential resulting in galvanic corrosion)?			
16	Are major hazards, complex areas and critical operations clearly identified? Are the level of detail, the methodology to assess these problematic cases and the safeguards proposed by studies compatible with the magnitude of the risks identified?			
17	Are the steps taken to construct the risk scenarios developed in a logical way? Does the study sequence lead to a clear and rational understanding of the process and its possible outcomes?			
18	Does the criterion for setting accident scenarios, especially the worst-case one(s), consider common-cause, domino or cascading effects and simultaneous/multiple scenarios?			

www.manaraa.com

19	Are the risks associated with third-party operations (material delivering, fuelling, electrical power, water supply) addressed by the safety studies? Are these risks considered in a holistic approach, occurring simultaneously and integrated with the facility's risks?			
20	Are risks associated with auxiliary systems (e.g. cooling and heating) contemplated?			
21	Is technology evolution naturally considered by safety studies? Is the increasing usage of operational and non-operational portable devices (e.g. mobile phones, tablets, cameras, smartwatches and fitness wristbands) considered, for instance, as potential ignition sources in explosive/flammable atmospheres? Does human reliability analysis and task allocation processes consider the new technologies potential to impact the performance of workers (e.g. attention shifters)?			
22	Have the studies evaluated the process plant safety when experiencing the effects of partial or total failures in critical elements (e.g. emergency shutdown valves fail in the safe position)?			
23	Are process changes that modify the risk level clearly identified when, for instance, safety critical equipment or systems are removed, deactivated or bypassed/inhibited for maintenance?			
24	Is the availability of safeguards and further risk control/mitigation measures addressed?			
25	Were critical equipment and components with limited life spam properly identified? Were replacement operations affecting safeguards and/or increasing risk addressed?			
26	Is quality control an active element of the risk assessment? Is it compatible with operational requirements for systems and equipment?			
27	Are suitable quality indicators proposed to verify critical system elements status? Is there an auditable failure log, to confirm that the expected performance of components and systems is maintained through time?			
28	Are chemical reactions and adverse events associated with housekeeping procedures (e.g. cleaning and painting substances, dust management), inertisation processes, equipment and pipeline deposits removal and necessary tests (e.g. hydrostatic tests) contemplated by the studies?			
29	Were the design and process reviewed aiming at their optimisation to avoid pocket/stagnant zones for dusts, gases, fumes and fluids (e.g. reducing elevated spaces and corners prone to dust/particles built-up or minimising lower pipeline sections subjected to particles/heavier fluids decantation)?			
30	Is the necessary information supporting non-routine tasks aiming at the risk reduction (e.g. pre-operational or restart inspections) sufficiently detailed, allowing the identification of process weak-points such as deposits accumulation, valve misalignments, damaged seals and rupture disks and equipment condition after, for instance, a process halt, or after maintenance works nearby and before resuming operations?			

www.manaraa.com

31	Are permanent cues and signals (e.g. pipeline and equipment marking to indicate content, maximum pressure and direction of flow) proposed as risk reduction measures for standard and non-standard operations? If so, is the permanent marking wear through time a factor considered?			
32	"The operator" is an entity sometimes subjected to extreme variations. When human intervention is considered by safety studies, are the expected skills (e.g. practical experience, acceptable performance variability level) and knowledge (e.g. the situational awareness level and the academic level – technician, engineer, expert) clearly indicated?			
33	Underperforming when conducting non-standard operations (e.g. start-up, commissioning or partial plant operations) was also a noteworthy pattern. Were situations and conditions where an enhanced level of training (skills or knowledge) or even the support of specialised companies (e.g. to control an offshore blowout) are required to keep risks controlled or to reduce the consequences of undesirable events identified?			
34	Is the essential risk information and knowledge arising from safety studies, which should reach the involved personnel, identified? Are there any special provisions to ensure that critical information will be conveyed by proper means (e.g. awareness campaigns, training, written procedures, simulation exercises) and will be accessible where needed?			
35	Is operational reality such as process conditions (e.g. background noise, fumes, heat, wind from exhaustion systems or alarms) considered as a possible disturbance when some sort of communication is required to convey important information?			
36	Are administrative/management aspects affecting the seamless continuity of operations (e.g. loss of information due to shifts, personnel replacement or reduction) addressed during the identification of safety critical tasks hazards? Is the prospect that obvious unusual situations (e.g. seemingly small leakages, unfamiliar odours and a flange missing some screws) may not be reported to supervisors promptly, affecting the effectiveness of risk reducing measures such as process plant walkthroughs, considered?			
37	Do supervisory control and data acquisition systems produce a real-time operation overview, not being excessively focused on individual parameters?			
38	Were the accessibility and visibility of instruments and equipment identified as critical in the risk studies and been ensured by an examination of the design drawings? Were 3-D models and/or mock-ups used to facilitate the visualisation of complex areas and reduce the possibility of interferences/visualisation issues? Are the external critical indicators/gauges fitness to the operational environment verified (e.g. visual impairment or working issues due to snow, rain or sun radiation)?			
39	Was the possibility of obstruction of water intakes, air inlets, sensors and filters (e.g. by water impurities, air particles or formation of ice) assessed? Are mitigation measures in place?			

www.manaraa.com

40	Have operators examined if the information supplied by indicators, panels and displays are sufficient, as active members of the safety assessment team? Do they have similar training level (skills and knowledge) as required for the operation of the system?			
41	Is there an assessment of the usefulness of the information provided by supervisory control and data acquisition systems? Are the functions and outputs clear, in particular to operators? Do they know when and how to use the information provided, or some of the signals are perceived as excessive/useless?			
42	Was the need to diagnose the system status and conduct special operations from alternative places (e.g stop the operation from outside the control room) considered?			
43	Are supervisory control and data acquisition systems failure modes assessed as critical hazards? Is the possibility that spurious or ambiguous error messages or information insufficiency/delays triggering human or automatic actions that can jeopardise the stability or integrity of the system carefully analysed? Were adequate mitigating measures put in place?			
44	Is the damage to power and control cables, pipelines and hydraulic systems, their routing and its consequences to the supervisory control and data acquisition systems considered by the risk assessment?			
45	Are safety critical alarms clearly distinguishable from other operational alarms?			
46	Are process facilities and hazardous materials located within a safe distance from populations, accommodation modules, administrative offices and parking spaces? Is the storage volume of hazardous substances optimised to reduce risks? Is the transportation route for hazardous materials optimised in a way that the exposure of people to risks is reduced to the minimum practical?			
47	Are control rooms and survival/scape structures protected from damage and located within a safe distance from the process plants? Does the risk study consider a scenario of control room loss? Is there any redundancy in place for emergency controls (e.g. fire control systems, shutdown systems)?			
48	Are visual aids used as risk-reducing measures to increase the awareness level of operators? Are reactors, vessels and equipment arrangement and dimensions visually distinctive from each other (e.g. by position, size or colour) to minimise swap-overs or inadvertent manoeuvres?			
49	Is the possibility of inadvertent connections of similar electrical, mechanic and hydraulic connectors an assessed risk? Are measures in place (e.g. using different connector dimensions or distinct thread types) to minimise hazardous interchangeability among connectors, elbows and other parts from different systems or functions?			
50	Is the inadvertent operation of temporarily or permanently disabled components, equipment or systems considered as a risk-increasing factor? Are measures in place to enhance the visualisation of non-operational parts such as isolated valves? Are overpressure safeguards (e.g. safety valves and rupture disks) accessible and visible from the operational area of the equipment or system they are designed to protect?			

www.manaraa.com

51	Are ignition sources (e.g. exhaustion, electrical equipment) optimised in order to be located within a safe distance from significant inventories of flammable materials (including piping) or in a position in which ignition is minimised, in case of leakage? Was the position of flares and vents revised by safety studies? Are exhaust gases routed to and flares and vents located in areas where the risk of ignition is minimised?			
52	Are different scenarios (e.g. in distinct plant locations, with variable volumes) for pipeline and vessels leakages considered by safety studies? Are there risk-reduction strategies to limit the released inventory in case of leakage (e.g. the installation of automatic emergency shutdown valves between sections)?			
53	Are safeguards prescribed by safety studies to minimise the possibility of creation of explosive atmospheres in enclosed compartments (e.g. deluge or inertisation (CO_2 or N_2) systems; exhaustion/vents)? Have the possibility of backflow in heating, refrigeration or ventilation systems been examined? Have the logic of automatic systems (e.g. automatic shutoff of air intakes after the detection of gases) and the reliability/availability of surrounding-dependent systems (e.g. positively pressurised rooms and escape routes) been assessed?			
54	Are fire systems, emergency equipment, escape routes and rescue services designed to withstand extreme conditions expected during an accident (e.g. blast, fumes and intense heat)? Are accident probable effects (e.g. impacts from fragments of explosions or the duration/intensity of a fire) considered in the evaluation of the effectiveness/survivability of these systems?			
55	Are alternative emergency power sources provided? Do the safety studies assess their functionality under distinct accident scenarios (e.g. main power cuts, flood, lightning storms and local fires)? Does the transition time from main to alternative power sources pose non-considered risks?			
56	Is there a main safe escape route and further alternatives designed, including load-bearing structures such as anti-blast and firewalls calculated to resist until the facility has been fully evacuated?			
57	Does the escape route contain clearance warnings by means of visual and audible cues? Are local alarm switches located in adequate positions to alert the remaining workers about the best available escape route? Are emergency lighting and alarms connected to the emergency power system (or have their own battery power source)?			
58	Have safety studies assessed the possibility of collisions (e.g. with cars, boats and airplanes) and external elements (e.g. projectiles from firearms) affecting equipment and the structure of the facility? Are measures in place (e.g. mechanical protection, administrative prohibitions, policing) to minimise these risks?			
59	Are distances among pipelines, equipment and modules optimised in order to consider the contents volatility, temperature, pressure and other risk-increasing factors? Is the separation among adjacent elements sufficient to avoid electromagnetic interferences, energy transfer or domino/cascading effects in case of failure? Were additional measures (e.g. physical separations and blast and fire protection walls) evaluated?			

www.manaraa.com

60	When physical separation is not possible, does the safety study evaluated if the surrounding equipment endurance time is sufficient to withstand the consequence of possible failure modes (e.g. a release followed by a jet fire from a failed adjacent element, for the inventory depletion time)?			
61	Does the safety study consider multiple safety barriers prone to common cause failures as a single barrier? Are alarms and sensors subjected to the same failure modes (e.g. same power supply or same cable routing) considered as non-redundant systems? Were redundant safety barriers subjected to an independence evaluation by safety studies?			
62	Are the risk scenarios demanding automatized responses (e.g. fire alarm demanding the activation of deluge systems or gas detection demanding the neutralisation ignition sources) identified and assessed? Does the supervisory control and data acquisition system have the capability of interpreting multiple alarms and command automatized actions or present consistent diagnostics to operators though the interface? Is the harmonisation of automated functions and personnel actions assessed?			
63	Is the position and type of sensors representative of the category of information they intend to convey? Are failures in sensors and indicators auto-diagnosed and clearly indicated by the interface?			
64	Is there a consistent assessment of safety alarms? Is the alarm precedence logic based on its safety significance? Are they prioritised according to how quickly personnel should respond in order to avoid undesirable consequences?			
65	Is the number of simultaneous alarms considered as a risk-increasing factor capable of disturbing cognitive functions? Are less important signals and alarms reduced/supressed (to minimise mental overburden) when the supervisory control and data acquisition system diagnoses a critical situation demanding full attention from the personnel involved?			
66	Are reduction measures for the initiation and escalation of fires and explosions proposed (e.g. reduction of ignition sources, material selection based on flammability level, ability to spread flames, generate smoke or propagate heat and the toxicity level)? Is the likelihood of ignition assessed in susceptible sections of the installation, by consistent means?			
	Total			

*non-applicable to the assessed study**

It is suggested that a large number of positive answers would represent a safety study that intrinsically contains solutions for the accident causation patterns encountered in the MATA-D scenarios, which caused major disasters in high-technology systems. Negative answers would indicate possible weaknesses in the safety study, which should be addressed in order to improve trust. For items that are neither relevant nor related to the assessed installation or system, a neutral answer (non-applicable) can be given. After

www.manaraa.com

confirming that the major problems raised by the list were addressed, the safety study can be seen as robust, from a "lessons learned" perspective.

Although this work present a general list as an example, applicable to virtually any industrial sector, the tendencies drawn from the MATA-D with the SOM approach are perfectly adaptable to specific industries such as oil & gas or aviation, and can be further developed for particular applications, e.g. design reviews. The accident causation patterns can be also used as input to the development of risk scenarios.

5. Conclusions

Verification and validation schemes must analyse proposed risk reduction measures, taking into consideration that systems are dynamic. Assumptions such "as good as new" systems/equipment, perfect procedures and faultless operators are accurate only on paper, and should be challenged by verifiers. Table 3 presented a sixty-six-item attribute list, which enables this debate and exposes possible shortcomings, addresses major hazards and stimulates improvement. The objectives are to give impetus to broader considerations about risk in real projects and raise the discussion about the implementation or dismissal of recommendations and solutions, enabling the dialogue among stakeholders and bringing transparency to the whole process.

Also, the prime attribute of a project is its feasibility, which means cost. This attitude is absolutely normal and engrained in our social behaviour (Does anybody check safety records before booking a flight, or the price is the first – sometimes the only – attribute considered in the decision-making process?). Therefore, promoting the coexistence and balance between economic aspects (i.e. resources, budget) and safety performance is the ultimate goal pursued by risk managers. It is a permanent persuasion exercise to which the current research intends to contribute, by developing means to enlighten stakeholders to consider a wider picture of risk.

The problem of trust in risk management and risk validation is not surprising at all. Risk assessment is a complex and multidisciplinary matter, and there is no such thing as a definite standard reference on how to perform a safety study. Distinct techniques and approaches are not mutually exclusive and should be simultaneously used, making the development of a single verification/validation method or procedure hardly possible.

www.manaraa.com

However, the most import outcome of a risk study is to support the decision-making process. Hence, it must be able to communicate risks to stakeholders, addressing potential problems and solutions in a clear way, and using visual aids such as maps can help tackling this challenge.

In this regard, the conversion of the MATA-D dataset into self-organised maps and their subsequent interpretation successfully converged into a comprehensive checklist containing items representing major accident tendencies, to be verified against risk studies and to help developing confidence that critical issues were taken into consideration. These concerns arose from shortcomings in many different industrial segments, also promoting an inter-industry exchange of valuable accident lessons. The questions can be easily traced back to regions in the maps, and practical examples of flawed interfaces between humans, technology and organisations can be extracted, in order to illustrate the possible adverse effects of not dealing with specific conditions. The 2-D SOM maps can be used to communicate and describe complex interfaces to a broader public in a simpler way, enhancing stakeholder's confidence that genuine strategies to mitigate risks are in place and the study was adequately completed.

Acknowledging that there is not a single method to verify and validate risk studies, the application of the widest possible range of approaches to stimulate the comparison of alternatives and different experts' opinion can give some insight into how to enhance trust in risk management. This work focused on ensuring that lessons from several past accidents are considered by new risk studies as good engineering practice and a sensible approach to reduce risk, by means of a straightforward risk study verification checklist.

Furthermore, the verification framework can be easily applied by a range of independent reviewers from industry and academia, which could use the checklist output to involve experienced people and develop innovative risk approaches, bringing new ideas and insights to safety studies in a structured way.

6. Acknowledgements

This study was partially funded by CAPES [Grant nº 5959/13-6].

www.manaraa.com

Chapter 5: Human factors influencing decision-making: tendencies from first-line management decisions and implications to reduce major accidents

Overview

This chapter presents a second application example for this research. At this time, the scrutiny of accident's tendencies from the MATA-D dataset will focus on specific interactions involving managerial judgements and decisions. Decision-making processes control the development of organisations and shape operations, constituting an essential capability to fulfil companies' immediate and long-term objectives. Major accidents, however, can severely disrupt operations, and many investigation reports relate to poor managerial decisions as relevant contributors to recent catastrophes. These seemingly imperfect decision-making processes usually encompass field managers, which tend to be vulnerable to pressures related to the facilities' result (e.g. time constraints to solve a failure, poor incentives). First-line management is typically responsible for guiding employees, directing everyday objectives and dealing with production efficiency, while having to demonstrate satisfactory results to upper hierarchical levels, especially regarding companies' pre-defined goals (e.g. productivity, quality requirements). Thus, the purpose of this study is to analyse first-line management critical decisions in the field, by comparing them with tendencies and common patterns extracted from the MATA-D, in order to better understand the surrounding factors impacting human judgements and to discuss implications to improve decision-making processes.

Intricate interactions among different levels of a production oil & gas platform management will be initially presented, highlighting relevant changes in staff roles as soon as the facility shifts from a standard organisational arrangement (Figure 2, pp. 131) to an emergency response arrangement (Figure 3, pp. 131), due to a significant deviation from normal operation. Under a new set of responsibilities formally assigned by the organisation, personnel previously concerned with the operation will now interact for the duration of an apparent high-hazard scenario in a unique way, in order to return the industrial environment to its previous safe state. This decision-making process, which is designed to cope with critical decisions regarding safety, will be described.

Then, management decisions which culminated in the worst accident occurred in offshore Brazilian waters in the past 15 years (i.e. and explosion resulting in nine fatalities) are

www.manaraa.com

scrutinised, through the analysis of publicly available investigation reports from the two official regulatory bodies.

The SOM data mining and classification approach presented in Chapter 2 is revisited in the search for analogous tendencies, allowing the comparison of the MATA-D common patterns with the offshore facility case study. Shared features between specific regions of the MATA-D clustering (i.e. interactions involving Inadequate Task Allocation) and the event under scrutiny are successfully recognised, suggesting that well-defined patterns involving organisational issues and human factors shaped favourable conditions for the accident.

Human performance shortcomings arising from the lack of managerial rules and principles, inconsistent planning and inadequate working practices are then investigated, and practical implications to improve critical decision-making processes are finally discussed. Evidence suggested that deep changes, such as the development of a dedicated decision-support system and having personnel fully devoted to ensure the safety of the crew, should be considered, in order to minimise the possibility of similar process safety accidents.

www.manaraa.com

Human factors influencing decision-making: tendencies from first-line management decisions and implications to reduce major accidents [5]

Raphael Moura[a,c,*], Caroline Morais[a,c], Edoardo Patelli[a], Michael Beer[b,a] & John Lewis[a]

[a] Institute for Risk and Uncertainty, University of Liverpool, Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom
[b] Institute for Risk and Reliability, Leibniz Universität Hannover, Callinstr. 34, 30167 Hannover, Germany
[c] National Agency for Petroleum, Natural Gas and Biofuels (ANP), Av. Rio Branco, 65, CEP: 20090-004, Centro, Rio de Janeiro-RJ, Brazil
[*] Corresponding author at: Office G79 Chadwick Building, Peach Street, Liverpool L69 7ZF, United Kingdom.

1. Introduction

Decision-making processes are in the helm of organisations, constituting an essential capability to promote companies' mission and objectives. Although researchers exploring the fundamental causes of disasters (Pigeon & O'Leary, 2000, Hopkins, 2005) indicated that keeping the focus on top management is crucial, it seems to be reasonable to assume that a successful safety program will rely on the implementation capacity and on numerous local decisions from lower hierarchical levels. Many of these decisions are not trivial and involve constant trade-offs between safety, productivity and quality requirements. These trade-offs, particularly the conflict between safety goals and production, were summarised by Reason (2000), who pointed out an interesting paradox: although both safety and production are deemed to be equally indispensable, production is, in reality, the attribute that pays the bills. Therefore, while responsible for guiding employees, directing everyday objectives and dealing with production efficiency and safety, first-line management is expected to deliver satisfactory (and sometimes daily) results to upper hierarchical levels, mainly concerning companies' pre-defined productivity goals.

Major accidents, however, can deeply affect the continuity of operations and put an end to productivity goals, dramatically shifting the stakeholders' attention from periodic and consistent productivity indicators (e.g. barrels per day, in an offshore production platform) to the search for causes of the adverse event. Many of the findings arising from some well-

[5] Original Publication in Moura, R. et al., 2017. Human factors influencing decision-making: tendencies from first-line management decisions and implications to reduce major accidents, *Safety and Reliability – Theory and Applications,* Crepin & Briš (Eds), pp. 251-260. London: Taylor & Francis Group, ISBN 978-1-138-62937-0.

www.manaraa.com

known recent investigation reports (e.g. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011, Kurokawa, 2012) relate to poor managerial decisions in all hierarchical levels, which triggered operational arrangements that resulted in undesirable outcomes.

In February 2015, an explosion at the Floating, Production, Storage and Offloading Unit Cidade de São Mateus (FPSO CDSM) resulted in the most shocking accident occurring offshore Brazil in the last decade, and one of the top-three worst offshore disasters in Brazilian Offshore Oil & Gas history. Nine people passed away, and twenty-six workers sustained from minor to serious injuries after a hydrocarbon leakage and its consequent ignition at the FPSO's pump room. The facility was producing non-associated gas and condensate by the time of the event. The investigation from the Oil & Gas regulator (ANP, 2015) identified seven causal factors and twenty-eight root-causes, highlighting inadequate managerial decisions which exposed the facility to unmanaged risks. The investigation report from the Maritime Authority (DPC, 2015) mentioned that inconsistencies from the safety management system gave room for improvised decisions, ultimately resulting in non-conformities. Those supposedly flawed decisions involved middle and operational management working in the field, where dealing with dynamic pressures related to the facilities' result (e.g. time constraints to solve a failure, improper incentives) can be a substantial challenge.

The conclusions arising from those investigations leave us with some important questions regarding decision-making processes and the practicability of adopting alternative approaches to ensure facilities are designed and operated in a safer way. To what extent were these decisions actually poor, in the face of organisational scenarios and operational challenges encountered by decision-makers? Were these decisions improvised and unreasoned, or did they follow a well-defined and recognisable pattern, which could be considered natural and predictable if the outcome was different? How can we turn people in-between top management and workers at the sharp-end of operations into better decision-makers?

The overriding purpose of the current work is to analyse decision-making processes by using the real-life event that occurred in offshore Brazil waters to uncover the intricate conditions leading to questionable (at least in hindsight) human decisions. The ultimate

www.manaraa.com

objective is to give some indications on how to tackle decision-making limitations by improving managerial rules and principles.

2. Analysis Method

Moura el al. (2016) developed a major-accident dataset, which contains 238 disasters from different high-technology industrial sectors, including nuclear, aviation and oil & gas. The Multi-attribute Technological Accidents Dataset (MATA-D) was fed with information from detailed investigation processes conducted by independent investigation commissions, regulators, insurance companies and experts, in order to disclose the circumstances surrounding the undesirable events and prevent their reoccurrence. Although each investigation team followed particular directives, procedures and terminology to scrutinise the major accidents, the dataset classification method based on Hollnagel (1998) facilitates the application of a single framework, allowing the comparison of events from different industries and the search for common patterns. Previous work (Moura et al., 2017a) successfully applied a clustering approach, i.e. Kohonen (2001) self-organising-maps, to identify major design shortcomings and develop a checklist focused on the improvement of design. The development of this design checklist was based on common features identified in Cluster 3, where accidents containing design failures interfaced with human factors in most of the grouping cases. Figure 1 presents the clusters' arrangement after the application of the self-organising maps algorithm.

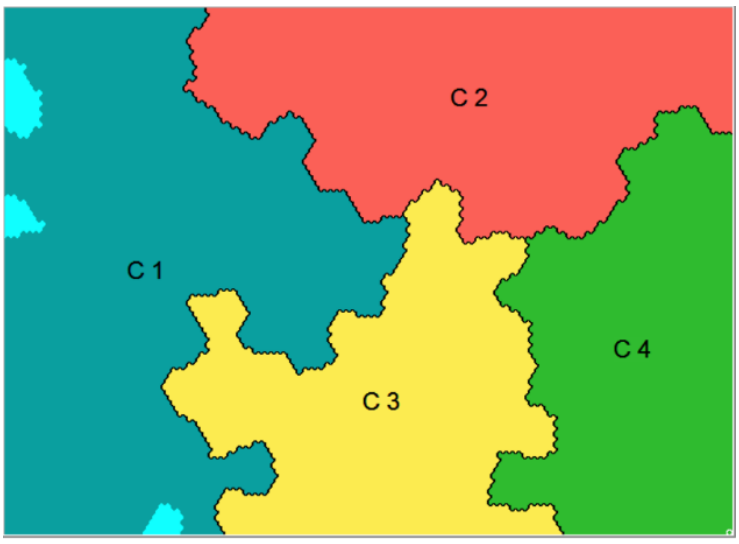

Figure 1. MATA-D Clustering Results using SOM, adapted from Moura et al. (2017b)

www.manaraa.com

The SOM data mining results will be revisited, in an attempt to disclose new links associated with decision-making processes and support the understanding of critical FPSO Cidade de São Mateus management decisions prior to the major event occurred in February 2015. Examples from the cluster of interest will be given, in order to illustrate similarities.

The reports on the FPSO CDSM accident (ANP, 2015, DPC, 2015) provide very detailed information about the disaster, based on engineering analysis of the facility, examination of documents and investigative interviewing of company staff in different hierarchical levels.

Therefore, after presenting the intricate interactions among different levels of an offshore production oil & gas facility management, basic responsibilities regarding safety will be assigned, in order to make the decision-making process exposed for further analysis. Based on the aforementioned in-depth accident accounts, critical decisions which were identified as contributing factors or root-causes of the event will be highlighted.

The deficiencies in the case study decision-making process will be then considered in the light of the tendencies disclosed by the application of the SOM algorithm, in order to enable the discussion of inherent conditions which increase the likelihood of flawed judgments and mistaken choices in a high-technology industrial facility.

3. Results

3.1 MATA-D mining for decision-making shortcomings

In the current work, the intention is to recognise common patterns associated with decision-making processes. In this regard, the statistical results from the SOM map indicated that Cluster 1 was dominated by the contributing factor named “Inadequate Task Allocation”, identified in 95% of the cases within this grouping (Cluster 1’s shadowed region in Figure 1).

The overwhelming incidence of this factor highlights situations where managerial instructions were poor and lacked clear rules or principles, task planning was largely inadequate and/or work execution directives were poor. Table 1 presents the leading features for Cluster 1, which contains 80 major accidents. Contributing factors in italic attained slightly higher scores in other clusters, but were still significant for the grouping.

www.manaraa.com

Table 1: SOM Cluster 1 Main Statistical Results

Human Factors	Execution Error	Wrong Place	52.50%
	Specific Cognitive Functions	*Observation Missed*	*20.00%*
		Faulty diagnosis	26.30%
		Wrong reasoning	*20.00%*
	Temporary person-related functions	Distraction	11.30%
	Permanent person-related functions	Cognitive bias	15.00%
Technology	Procedures	Inadeq. procedure	78.70%
	Interface	Incomplete info	36.20%
Organisation	Communication	*Communic. failure*	*16.30%*
		Missing information	37.50%
	Organisation	Maintenance failure	56.30%
		Inadeq. quality ctrl.	81.30%
		Design failure	*85.00%*
		Inadeq. task alloc.	**95.00%**
		Social pressure	17.50%
	Training	*Insufficient skills*	*56.30%*
		Insufficient knowledge	60.00%
	Working Conditions	Irregular working hours	10.00%

In Cluster 1, the map region occupied by the Inadequate Task Allocation factor was combined with design shortcomings, quality control problems, maintenance failures, training issues and communication difficulties, from an organisational perspective. The most relevant technological problem was having inadequate (incomplete or ambiguous) procedures. Inaccuracies in sequences of operational actions due to incorrect diagnosis of a situation or a faulty reasoning were also frequent.

3.2 The Decision Structure at the FPSO CDSM

The Offshore Installation Manager is typically the top authority on-board and the designated Offshore Incident Commander in case of an emergency. He is the key decision-maker and his personal judgment will direct the response efforts. Thus, his decisions will be now defined, considering the existing information and the available choices.

The standard organisation of a Production Oil & Gas Platform (Figure 2) is instantly transformed to respond an emergency, according to previous definition from the company's Emergency Plan. Figure 3 depicts the new roles for the operating staff.

www.manaraa.com

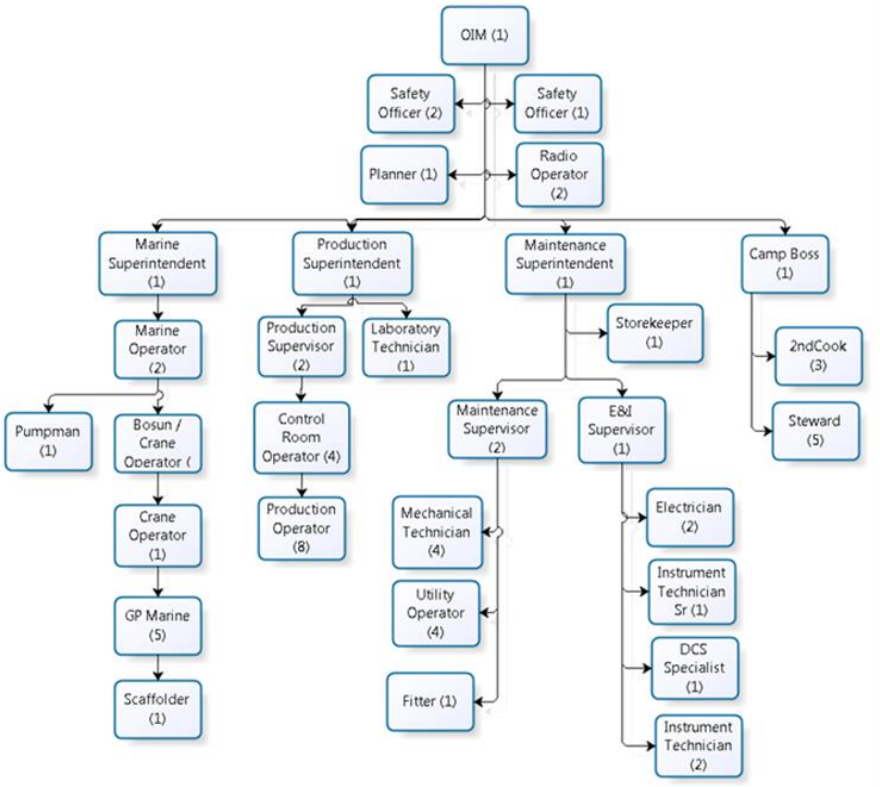

Figure 2 - Standard Organisational Chart, after ANP (2015)

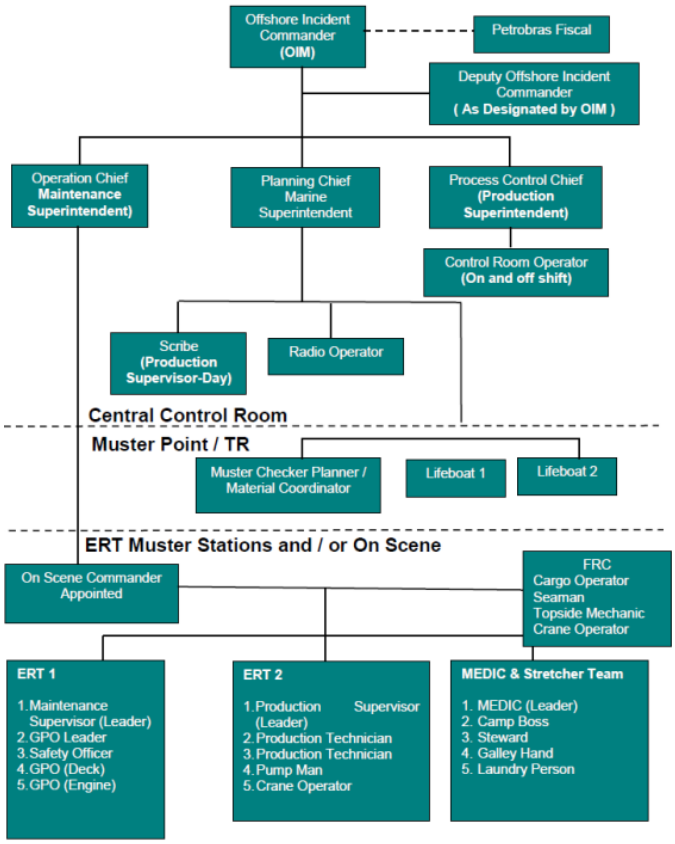

Figure 3 - Emergency Response Organisational Chart, after ANP (2015)

www.manaraa.com

Three groups were effectively involved in the Offshore Installation Manager decisions in the case study: (i) the Decision Board; (ii) the Emergency Response Team; and (iii) the Technical Advisory Response Team. The decision-making response structure for the FPSO CDSM is typical, having well-defined actors to pick a solution, to discuss options and recommend alternatives, to provide technical information about potential choices and their effects, and to confirm the capability and execute a sequence of tasks. Table 2 relates the FPSO CDSM personnel functions with standard roles of a classic decision or problem-solving structure.

Table 2: FPSO CDSM Decision Structure, adapted from Herrmann (2015)

FPSO CDSM Personnel	**Roles** (Spetzler, 2007)	**Roles** (Rogers & Blenko, 2006)
- Offshore Installation Manager	- Decision-maker	- Decide
- Marine Sup. - Production Sup. - Maintenance Sup.	- Decision Staff	- Recommend Alternatives
- Technical Advisory Response Team - Emergency Response Team (x2)	- Content Experts - Implementers	- Provide Input - Agree (confirm feasibility) - Perform

The Decision Board was composed by the Offshore Installation Manager, the Marine Superintendent, the Production Superintendent and the Maintenance Superintendent. There were two Emergency Response Teams aboard, composed of five members of the crew and having Safety Officers as leaders. The technical advisory response team had been created by initiative of the Offshore Installation Manager and was not on the formal Emergency Response Plan of the platform. Based on his experience in other platforms, he felt that it would be useful to have a technical advisory team to be consulted upon particular topics. It was made of relevant technical staff, e.g. the Pump Man. The informal group has participated in the three decision meetings, and its members accompanied the on-site fire brigade to the Pump Room in all occasions.

Although the investigation report (ANP, 2015) had suggested that the Onshore Emergency Central was contacted as soon as the gas alarms sounded, there was no input from the land staff to the Decision Board until the emergency had escalated after the explosion.

www.manaraa.com

All decision meetings took place at the Central Control Room, and additional people (e.g. production supervisor, control room operators, radio operator) were available to perform any action required and modify the production system configuration.

3.3 Response for a multiple-alarm event in the FPSO CDSM Pump Room

Dealing with a multiple-alarm indication in the Pump Room was a non-routine event, and its possible causes and effects were neither certain nor obvious to the crew. Formal emergency response procedures contained general instructions: (i) to deploy an equipped operator (with portable gas detector) to examine a single detection, or initiate the general alarm for a multiple detection; (ii) use the Public Address System to announce an indication of a fire or gas release; (iii) Order a local evacuation in the single detection case, or direct personnel to muster points under a multiple detection; (iv) confirm the designed automatic shutdowns (only for multiple detection); (v) Inform the Offshore Installation Manager.

According to the ANP's (2015) investigation report, there were no further formal procedures, and the Offshore Incident Commander (the Offshore Installation Manager in the case study) was responsible for assessing the situation and deciding what to do, after the initial steps above. For that reason, the Emergency Response Plan was considered incomplete by the investigators, and thus one of the root-causes for the accident.

The first response group assembly took place approximately four minutes after multiple alarms sounded. It was attended by The Decision Board and the Technical Advisory Response Team. The supervisory control and data acquisition system had automatically isolated the Pump Room by closing the ventilation dampers and entering the air circulation mode (DPC, 2015). Also, visual and audible alarms were activated in the whole facility and the personnel were directed to the muster points by the Public Address System. The Onshore Emergency Centre was also informed. As the leaked substance and its volume were unknown, the Incident Commander ensured the pumps stoppage (to eliminate possible ignition sources and reduce the leakage) and deployed a response team (members from the official Emergency Response Team and from the informal Technical Advisory Response Team) to the Pump Room, in the search for additional information. Gas detectors were inhibited and alarms were silenced to facilitate radio communications.

www.manaraa.com

The first response team successfully executed their mission and brought new information. They identified the leakage point (i.e. liquid dripping from a flange) and encountered a two square meters pool. The second decision meeting took place approximately fifteen minutes after the initial assembly. On this occasion, the Emergency Response Team joined the Technical Advisory Response Team and the Decision Board to evaluate the current situation. The Incident Commander decided to partially restore the ventilation system, in order to avoid any electrical overheating and maintain production, and a second team was deployed to the Pump Room to define the corrective measures required.

The second team accomplished their goal and communicated via radio the required tools for the repair implementation. The team left the Pump Room, allegedly to breathe fresh air, and the Emergency Response Team leader and one member of the Technical Advisory Response Team went to the Central Control Room to join the third decision meeting.

The third decision meeting occurred approximately fifteen minutes after the previous one. As a result, non-essential personnel were authorised to leave the muster points and have lunch. The necessary apparatus (e.g. absorbent pads, tools, fire hose, and ladder) to repair the piping joint was prepared, and a cleaning and repair team, composed of five workers, was sent to the Pump Room.

The cleaning and the repair activities were executed concurrently. During the cleaning, the absorbent pads were considered ineffective, and a water jet cleaning was initiated. After a request to increase the water jet pressure had been implemented, a major explosion occurred. Figure 4 represents the decision-making flow.

www.manaraa.com

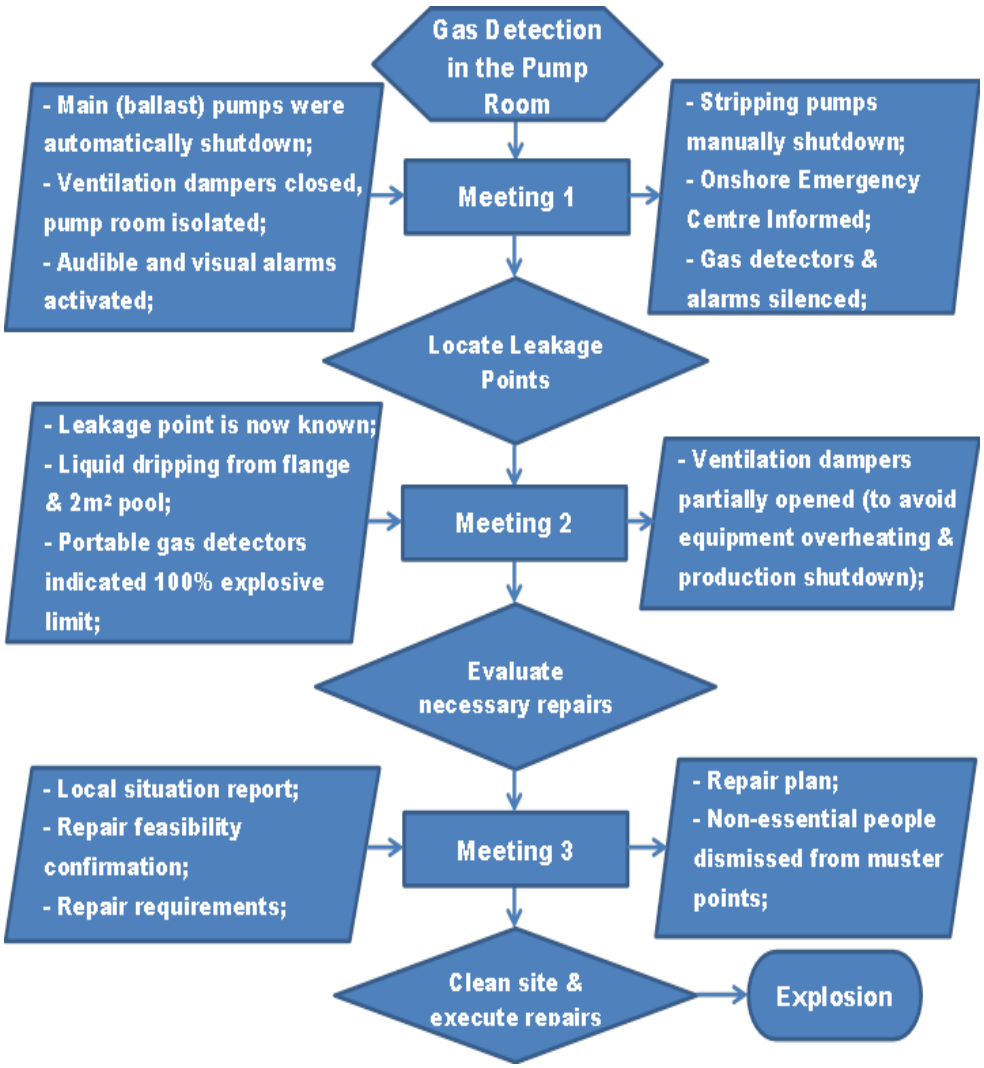

Figure 4 – Decision-making flowchart

3.4 FPSO CDSM surrounding factors and their connection with MATA-D tendencies

The application of the SOM algorithm grouped accidents with similar characteristics. The data mining process indicated a particular cluster of interest containing 80 accidents (Cluster 1), which has Inadequate Task Allocation issues as the prevailing contributing factor. The patterns disclosed by the SOM grouping were deeply associated with the sequence of events witnessed in the FPSO CDSM prior to the disaster. The complexity of the operation of an offshore platform is extraordinary, and there are many contextual factors embedded in such organisation which might prove to be pivotal in case of an accident. Latent failures such as design shortcomings and operational weaknesses can deteriorate the system to the point that people cannot compensate for a degraded operating environment.

www.manaraa.com

The FPSO CDSM investigation revealed many surrounding factors contributing to the events on the day of the accident. According to the report (ANP, 2015) the marine team was largely undermanned. The lack of a safety critical function (senior marine operator or marine supervisor) and the regular accumulation of management and operational roles (an operator was performing marine superintendent functions for a long period prior to the event) led to difficulties to control cargo transfer tasks and to undertake judicious handovers between shifts. The handover between Offshore Installation Managers also failed to convey significant information regarding the ongoing cargo transfer manoeuvre (DPC, 2015). Human resources management problems and the lack of clear definition of responsibilities were contributing factors directly identified under the tag Inadequate Task Allocation in Cluster 1 (Table 1) of the Self-organising Map (Figure 1).

There is an expectation that the organisation will provide enough personnel not only to operate the industrial facility under standard conditions, but also to deal with abnormal situations. However, the recurrent approach to operate with low manning levels results in serious vulnerabilities, particularly in case of atypical operational scenarios, a recognisable pattern heightened in Cluster 1 accidents. Many examples are in line with the conclusions from the FPSO CDSM report. The investigation on the Varanus Island accident (Bills & Agostini, 2009), for instance, highlighted low manning levels in various disciplines and having key competences outsourced or restricted to specific members of the team as contributing factors to the disaster. Deficiencies in the shift handover and communication issues were also considered contributors for the Buncefield accident, according to the COMAH report (2011).

Another pattern identified in Cluster 1 suited the FPSO CDSM event surprisingly well, i.e. the link between inadequate procedures, flawed safety analysis and inadequate task allocation. The investigation report indicated that emergency procedures were short on detail, lacking adequate hazard mitigation measures for a scenario of confirmed gas detection in the pump room. Moreover, operational procedures (e.g. cargo transfer) and plans (e.g. Process & Instrumentation Drawings) directly related to the manoeuvres which caused the gas leakage were obsolete and mismatched the existing process plant configuration. Many examples showing similar tendencies can be extracted from the cluster, such as the incomplete procedures for cargo transfer (i.e. tank filling) in the Buncefield accident, or the lack of emergency procedures for safe and proper response to a

www.manaraa.com

hazardous scenario (i.e. diesel engine over-speed) in the Rosharon plant vapour cloud fire (US-CSB, 2003).

The normalisation of deviance was also a recurring issue in the FPSO CDSM operation. Normalisation of deviance occurs when the group incorporates erratic operational conditions and accept risks as part of their work culture (Vaughan, 1996). In those cases, individual risk perception and consideration of hazards are shaped by group thinking and, in a broader perspective, can be interpreted as a social pressure mechanism. It was known that the seat rings for the cargo transfer valves, which had a key sealing function, were inadequate for the type of condensate stored. The seals manufacturing material was susceptible to chemical attack, but maintenance and quality control measures failed to address the source of the problem, adopting alternative approaches to live with it instead. The storage of condensate itself played a significant role in the event. According to the investigation (ANP, 2015), the design conception and safety philosophy did not anticipate pure condensate storage, as the system was originally designed for petroleum or a mix of petroleum/condensate. Operational studies and safety analyses had taken place, but these were superficial and failed to identify hazards and address increased risks due to the modified storage and cargo transfer process. Other deviations identified, such as the regular use of in-house manufactured blind flanges without ensuring compliance with the adequate pressure class, were also discernible tendencies in Cluster 1, where mismatches between equipment/accessories and the required certification to operate under specific conditions were observed. Correspondingly, unsuitable bunds (were not impermeable) were evidenced during the Buncefield investigation (COMAH, 2011), and fixtures and further fittings in the Rosharon plant (US-CSB, 2003) were not certified for the operational environment.

Further significant design weaknesses, such as the lack of effective blast protection for the living quarters and muster points, also coincided with Cluster 1's patterns. Accidents involving failures in the fire/blast protection and the consequent impairment of relevant equipment and locations were persistent within the grouping. The control room damages after a jet fire in the Castleford Petrochemical plant (HSE, 1994) and the spreading fire to nonproduction areas in the Corbin facility (US-CSB, 2005a) which killed eight workers, are examples, to name but a few, of analogous cases.

www.manaraa.com

3.5 Comparison between the FPSO CDSM decision-making and MATA-D task allocation shortcomings

The environmental factors surrounding the decision-making process in the FPSO CDSM showed deep correspondence with the tendencies disclosed by the SOM clustering method. Once the scenario is set and the surrounding factors are exposed, the decision-making process immediately preceding the explosion can be disclosed under a well-defined context. The decision context is vital to comprehend the strategy, the objectives and the available choices to solve a problem, i.e. a gas release in the Pump Room.

Snowden and Boone (2007) suggested a context classification scheme for decision-making, dividing it into 5 groups: simple, complicated, complex, chaotic and disorder. According to their approach, the existing decision context in the FPSO CDSM ranged between complicated (relationship between cause and effect is clear but not recognisable by everyone; may contain multiple right answers and thus require investigating several options; requires expertise) and complex (right answers cannot be ferreted out; unpredictability; experiments which can safely fail lead to instructive patterns).

The context faced in the FPSO CDSM is very similar to the patterns from the SOM Cluster 1. The application of the SOM algorithm revealed particular cognitive mechanisms underlying failures to perform a sequence of actions in analogous cases. The diagnosis of system state was incomplete, as the gas presence in the Pump Room was acknowledged, but not its possible effects (i.e. explosion). A faulty reasoning links to the decision-maker strategy, inferring that the solution applied before (enter the compartment and execute repair services) would work well again. Some personal cognitive biases also exist, such as: (i) the belief that the situation was under control (reinforced by two successful excursions to the Pump Room); (ii) the incorrect review of probabilities, after people returned from the Pump Room with portable detectors indicating that the atmosphere was significantly above the lower explosive limit; and (iii) the hypothesis fixation, as the decision-maker was focused on a single solution and thus constraining the sequence of actions to a particular approach which matched his assumptions.

Additionally, the Offshore Installation Manager only boarded on the day of the accident, and was not aware of all ongoing operations, including the one which gave rise to the flammable gas cloud. After the alarm, the organisation adapted to a non-routine arrangement (From Figure 2 to Figure 3), and the required decisions were of uncommon

www.manaraa.com

nature. The lack of practical experience to define and perform tasks (lack of skills) and the unsatisfactory theoretical knowledge regarding the scenario and associated risks indicated that the FPSO CDSM manager lost the overall situation awareness.

The decision-maker, with the support of experts, was confident in accomplishing the final goal (stop the leakage by detecting and repairing the escape point), but missed a crucial step: making the compartment safe and serviceable, despite all relevant signals (initial detection from fixed sensors, and later from portable detectors). The task planning was inconsistent, the work procedure was poor and the managerial rule lacked clear principles such as reducing the personnel exposure to risks. All these elements are satisfactory captured under the Inadequate Task Allocation tag, which was the dominant element for Cluster 1, as many analogous examples show.

4. Discussion

The analysis of the MATA-D clustering after the application of the SOM algorithm revealed common patterns linking Inadequate Task Allocation, a key managerial problem, with several surrounding factors found in Cluster 1. Similar patterns and linkages among contributors were disclosed by the post-accident examination of the explosion in the Pump Room of the FPSO CDSM, which occurred in February 2015.

Many contributing factors arose from earlier decisions, such as the modifications of the original design to adapt the operation to new conditions without a thoughtful consideration of risks. Therefore, the decisions with the intent to interrupt the leakage in the day of the accident were taken under a previously degraded decision-making environment, as production objectives appear to have prevailed upon safety in some design, maintenance and quality control choices.

During the event on the FPSO CDSM, the decision-maker was essentially left on his own, as clear instructions on how to proceed in case of gas confirmation in the Pump Room were missing from the emergency procedures. Therefore, he appeared to be in need of further information to decide what to do next. Accordingly, his first objective was to search for additional data, which he accomplished by gathering information from operators in the Control Room and by sending a recognition team to the Pump Room. Before sending people there, he ensured that the pumps were disabled, valves from the cargo system were

www.manaraa.com

closed and the air exhaustion system was shut. The leaked gas was certainly confined to the Pump Room. Moreover, he might have assumed that the local system halt reduced the leakage and/or eliminated possible ignition sources inside the compartment.

The first excursion to the compartment was very successful, and this repeated action – groups were sent to the gas-filled room three times – might have reinforced the (wrong) impression that it was safe to go there. Not only the decision-maker appeared to be confident that the developments of the system were under his control, but also the remaining participants of the decision-making process, including the emergency team members. It is important to notice that the investigation reports (ANP, 2015, DPC, 2015) did not capture any signal of opposition to the strategy of entering the compartment, not even from the most vulnerable ones – the people who were responsible for performing the recovery tasks in an extremely dangerous site, and eventually died doing so.

Signals of overconfidence are overwhelming. After the second excursion to the compartment, the Offshore Installation Manager decided to release people from muster points and authorise them to have lunch, retaining only essential people to execute the required repair. The belief that the strategy was good – the leakage point had been identified and a repair plan was conceived – made the members constrain their alternatives to current assumptions, i.e. that the situation was reasonably controlled. This appears to be due to the absence of active ignition sources and the compelling fact that people do have entered the place twice, with positive results.

The whole group – decision-maker, decision staff, experts and implementers – restricted their choices to a sole hypothetic solution. Under an unusual, complex scenario, the individuals immediately jumped to the only definitive solution available (repairing the leakage), disposed to solve the problem as soon as possible and return to a safe operating status. This recognisable hypothesis fixation might have made them skip two alternative solutions. The first one, to conduct operational manoeuvres to ventilate the room, in order to eliminate the explosive atmosphere indicated by the local sensors and later confirmed by the crew. The second option would be a more conservative one: to abandon the ship. If the Offshore Installation Manager had recognised the imminent risk of explosion, he could have commanded an evacuation, aiming at the safety of the personnel.

www.manaraa.com

The uncertainties related with all possible scenarios, even in hindsight, turn the review of probabilities for the outcomes into a subjective problem. We can only be sure that the solution adopted had a negative consequence (thus was an error), but we cannot guarantee that the alternative solutions would present a positive outcome. In the case study, trying to ventilate the flammable gas cloud from the compartment, for instance, is a very complex, high-knowledge dependent procedure. For the first alternative solution, the design of the ventilation system, especially of the location of air outlets, should be understood to the point that people could make sure the discharge would not find an ignition point in a location even closer to the ship living quarters. Special knowledge about the ducts dimension and flow speed would be required, to minimise the possibility of forming an explosive atmosphere in another place. It would be an exceptional operation, without any parallel with the routine of the crew and with no guarantee of success. Additionally, it would still require the repair of the leakage point afterwards.

The second option, consisting of directing the crew to muster points, shut-down the plant and directing the evacuation, is the most conservative one. Since the accident investigation indicated that the possible ignition sources were static electrical or mechanical sparks introduced by the repair procedure, it would be sensible to assume that the ship abandonment would be successful. However, some individual and corporate negative effects would be certain. The decision-maker was the Incident Commander, but above all he was the full-time Installation Manager, predominantly responsible to deliver a production result to his superiors. If he evacuated the unit and the explosion did not occur, he might have been considered excessively conservative, and jeopardise his career as a manager. Furthermore, having a high-potential event stressed by the abandonment of the unit would put the company in the glare of the media spotlight, and under regulatory scrutiny.

Therefore, the latter option involves a situation where the main objective of the company (continuous production) would be unquestionably compromised (with 100% certainty), against responding and tolerating some degree of risk (in fact, a subjective probability that safety will be compromised) to attempt an immediate solution to the problem.

This is the main reason why the decision-making process outcomes at the FPSO CDSM are not surprising at all. On the contrary, it followed a very well-defined pattern, exposed by

www.manaraa.com

the region of the self-organising maps where the work organisation lacked clear framework guidelines and safety values/principles.

5. Conclusions

The decision-making process developed during the FPSO CDSM event resulted in an unsatisfactory but plausible outcome. Several relevant aspects leading to the disaster, which were embedded in the organisation, were revealed by the two official investigation reports considered in this research. These factors were successfully related with common patterns belonging to one of the areas (i.e. Cluster 1) of the SOM map, indicating that known trends prevailed in the FPSO CDSM accident. It was made clear that the workgroup has inherited many organisational latent failures, including unsound design choices, which might have consciously or unconsciously encouraged an atmosphere of decisions favouring production over safety. Considering the environment and the nature of the position of the decision-maker, it should be anticipated that a predilection for a quick solution, which would pose less impact to his (and the company's) perceived key objectives, would overpower any presumably safer but certainly riskier choice to the production upkeep.

The decision-maker has not entirely overlooked safety principles. He took rational preventive actions before sending the team to the Pump Room (e.g. confirmed shutdown of possible ignition sources and the closure of ventilation dampers to avoid escalation), monitored the risk (through the information he received) and updated his decision-making process in an optimistic way: he believed (and most likely received ratifying indications from local teams) that the repair was possible and reasonably safe. Of course, some measures taken were questionable, such as having members of the Technical Advisory Response Team entering the Pump Room along with the Emergency Response Team. This exposed a larger than necessary group to the explosion and challenged any cautionary principle. It is not very surprising though, as it might be the case that he diagnosed the likelihood of an explosion as extremely low, during his quick mental review of probabilities, and understood that the risk was worth taking.

It is not possible to assume that another Offshore Installation Manager, with the same level of skills and knowledge and under the same scenario, would adopt a different solution. Hence, considering the intrinsic and immediate goals of the work position, the specific training and information required to solve complex, non-routine problems, the normal

www.manaraa.com

variability in human behaviour and the organisational pattern in line with many major accidents from MATA-D, it is supposed that improved organisational configurations would be necessary to reduce major accidents.

For example, in the case of production platforms, a conceivable solution to improve emergency on-board decisions would be to dedicate one or two people to damage control. These people would take responsibility for leading emergency operations, immediately exchanging information with the land Emergency Control Centre and gathering data from on-board operational personnel. The key objective of the damage control personnel would be safety, substantially reducing any conflicting goals, especially with production maintenance. Skills and knowledge of these professionals would be planned to improve the understanding and operation of important systems during an emergency. In the case study, gas detectors and alarms were disabled to improve radio communications. It is obvious that the human-machine interface was not ideal. Therefore, it appears that a dedicated console (e.g. a Damage Control Console) would be desirable, in order to provide adequate information for the recovery of emergency scenarios and assist the decision-making process.

Certainly, these changes in the sharp-end of the process would need to be accompanied by high-level measures involving, for instance, the design. In the case study, many latent failures imbedded in the concept of the plant (e.g. lack of blast protection for the living quarters; decision to convert a Very Large Crude Carriers into a Production Platform, inheriting the arguable location of the accommodation module above the Pump Room) appear to have contributed to the event. Those earlier decision-making processes could also be thoughtfully investigated and discussed, in order to identify further improvement opportunities.

6. Acknowledgements

This study was partially funded by CAPES – Brazil (Proc. No. 5959/13-6).

www.manaraa.com

II. Conclusions

i. Research Highlights

This thesis delivered an in-depth assessment of the intricate interactions between human factors, technology and organisations, focusing on major accidents in high-technology environments. Common patterns associated with disasters from different industrial backgrounds were revealed, enabling an improved understanding of the mechanisms leading to human errors and major accidents. The information arising from the creation of the MATA-D and the accident tendencies disclosed by the application of advanced data classification and clustering methods assisted the development of novel approaches to (i) understand and communicate risk; (ii) to build trust in safety studies; (iii) to minimise human errors; and (iv) to develop mitigation strategies, satisfying the objectives set for the research project.

The first objective was to develop a dataset capable of capturing major accidents from different industries under a common framework, in order to enable further analysis and the identification of shared features. The statistical analysis of the MATA-D confirmed that multiple interactions among a number of influencing factors are necessary to cause major accidents in high-technology facilities. Most importantly, accidents were made comparable, and results cast some light on the most frequent factors leading to disasters. Organisational factors were recognised as the foremost contributors, being identified in 95.38% of the cases. Specifically, design failures (66%), inadequate quality control (60.5%) and inadequate task allocation (60.1%) were the most frequent factors disclosed by the general dataset analysis. A very significant tendency has been identified among the major accidents contained in the dataset: 72.8% of the human erroneous actions and 74.34% of the identified flaws in specific cognitive functions were associated with design failures. Specific cognitive functions are the mental processes generally involved in the human ability to react to stimuli, represented in the current research by the sequence of (i) observing cues and signals, (ii) interpreting the scenario; and (iii) developing an accurate mental plan to respond to it. This key association provided unambiguous indication that design problems can be considered a major triggering factor for failures in mental processes and for erroneous actions, disclosing a clear path to the genesis of human errors. The identification of design shortcomings and the understanding of the interfaces among these accident contributors, especially in earlier stages of the lifecycle of engineering systems, are crucial to improve human performance and reduce the likelihood of accidents. The design

www.manaraa.com

influence is an important finding highlighted by this work, which added value to the successful completion of the first research objective, i.e. to develop a suitable multi-industry accident dataset.

A profounder analysis of the data indicated that the human capacity to interpret systems' status was severely compromised by the lack of suitable input (e.g. visual prompts, cues, signals and measurements) from the design. Dissonances between expectations on operators' performance (i.e. to detect, analyse, diagnose or formulate accurate hypothesis) and situations observed in real accidents, which resulted in human active failures, were highlighted by the current research. It has shown that design should take into account some performance variability and consider the non-mechanic behaviour nature of humans. Consequently, general guidelines for a design review, which consider the interfaces between human erroneous actions, cognitive functions and design failures, were successfully proposed. The lessons learned from the MATA-D allowed the development of a systematic verification process, focused on the quality of the inputs intended to support the diagnosis of undesirable operating circumstances, leading to actions that effectively control the developments of industrial systems.

The second objective of the research was to produce further insight into the genesis and perpetuation of human errors through the application of advanced clustering and classification methods to the MATA-D. Fully achieving the proposed objective, major findings were disclosed by the application of an artificial neural network approach, specifically the self-organising maps algorithm. The representation of the multidimensional data (a 238 x 53 matrix) in a graphical interface whose output are 2-D topographic maps exposed the mechanisms underlying human, technology and organisational interactions. Accidents were grouped by attribute similarity, enhancing the influence of certain contributing factors in each of the four distinctive clusters found, thus revealing key tendencies behind major accidents. The disclosure of a novel method to understand complex data and the interpretation technique for the SOM maps thrived, and some of the key findings will be summarised below.

The first cluster contained events in which design failures, inadequate quality control and inadequate task allocation were the leading factors, also emphasising a connection between inadequate procedures and insufficient knowledge. It became clear that written operating instructions were incomplete, ambiguous or open to interpretation, as it was

www.manaraa.com

expected from operators a certain situational awareness level to perform a task. These organisational and technology asynchronies resulted in failures to perform a logic sequence of manoeuvres, mostly related with basic to intermediate cognitive issues, i.e. to observe cues and signals and interpret the system status properly.

Major accidents involving adverse ambient conditions were primarily grouped in the second cluster. The key lesson from this grouping is that more frequent natural events like torrential rain, electrical storms and airborne particles can be as harmful to high-technology systems as extreme phenomena, such as hurricanes and earthquakes.

The third grouping was largely dominated by equipment failures, reaching approximately 95% of the cluster area. Design shortcomings and quality control problems, such as in Cluster 1, played a relevant part in these events, but now strongly associated with other organisational factors, such as communication failures and management issues. The incorrect use of equipment or having little experience or insufficient skills to perform properly were also noteworthy. Interestingly, the interpretation of the SOM maps showed that more complex cognitive functions were demanded in these cases, and the humans involved were required to not only observe and interpret, but also to create a mental plan to control the developments of the system. These cognitive failures tended to be associated with action errors involving wrong timing or wrong type, such as the anticipation, delay or omission to act, as well as using disproportionate magnitude, speed or moving in the incorrect direction. In addition, the comparison of individual maps indicated that the combination of maintenance problems with equipment failures is not as significant as one could expect, unequivocally showing that maintenance improvements *per se* are likely to have little impact in the prevention of major accidents involving equipment faults.

The last cluster was also dominated by equipment problems, occasionally accompanied by quality control issues and design shortcomings. Accidents contained in this grouping have shown the lowest incidence for human factors. It can be seen that the application of the SOM algorithm successfully isolated events with lower number of contributors (i.e. six or less factors, with mean of 3.1 events and mode of two), indicating that the grouping offered fewer opportunities for the disclosure of clear accident tendencies, if compared to former clusters.

www.manaraa.com

Apart from the effective disclosure of key features and significant trends in major accidents, the reduction of the multi-dimensional data to two-dimensional maps without any information loss successfully provided alternative means to disseminate risk information, opening the possibility of using graphics and visual aids to reach and influence wider stakeholder groups, entirely satisfying the third proposed objective for the research.

In the search for interesting features and in order to demonstrate the stability and usefulness of the dataset structure, different data analysis approaches were applied to the MATA-D. In Chapter 3, a tailored distance measurement was chosen to indicate proximity among events, and the hierarchical agglomerative clustering method output was presented in a dendrogram, which is a branch-type diagram hierarchically organised by property similarity. Consequently, accidents were displayed in nine clusters: (i) one remarkably different from the rest of the diagram and containing only two leaves (accidents); (ii) four containing organisation-technology events; and (iii) four containing organisation-human events. Results confirmed that accidents purely justified by human factors are extremely rare, representing less than 1% of the sample. This study also disclosed situations where personnel were unable to fully understand and recover from an accidental path, as a result of indistinct/incomplete error messages associated with the failure from the organisation to promote appropriate communication exchanges among peers. These poor feedback circumstances were accompanied by inadequate work conditions, such as irregular working hours and excessive demand, justifying the incidence of psychological stress, distraction and fatigue, and undermining the problem-solving capacity of operators. Some human erroneous actions were found to be based on failures to observe an indication or alarm, while others were associated with a wrong interpretation of the system status, usually an induction or deduction error. The former cases were mostly accompanied by equipment failures, while the latter were associated with inadequate procedures. It clearly indicates the lack of awareness to deal with degraded systems after equipment failures, and the limitations of written instructions to be representative of the operational reality, especially in abnormal situations.

Despite the productive application of alternative approaches, such as the hierarchical agglomerative clustering, the SOM results were revisited and further analysed in Chapter 4, with the main purpose of building trust and improve the quality of safety studies. This was the fourth objective established for the current thesis. The findings of this research project made clear that safety analyses will not be able to convey truthful results if the complex

www.manaraa.com

relationships between human factors, technologies and organisations are not properly considered. Therefore, strong connections among contributing factors in specific areas of individual clusters were mined, revealing common tendencies from past major accidents, which should serve as input to the verification of future safety assessments.

Examples of new findings included many designs that considered some components, equipment or sub-systems in isolation, disregarding risks related to the interaction with other systems and the environment. Besides, regions where system modifications took place without an adequate consideration of their impact, including the need to reshape the required training to understand and operate under new conditions, were clearly identified by the maps interpretation. Another relevant trend is the fact that routine, unpretentious maintenance issues (e.g. cleaning of drains and vessels, dust removal and simple repairs), usually executed by personnel with partial awareness of the system behaviour, can increase risk and decisively contribute to major accidents. Non-routine operations, such as the start-up of a process plant, testing or partial operating conditions, were also combined with training shortcomings, resulting in a tendency to underperform under special circumstances.

Specific communication issues were also highlighted. These include several occasions where verbal messages among personnel were misunderstood, due to common background noise or the poor quality of transmissions. Problems involving information transference between shifts and to computer-based systems were recurrent, as well as occasions where safety critical data was not properly examined or further communicated, because the information holder thought that his actions were sufficient to control the system. Interface problems, especially concerning the availability of information from supervisory control and data acquisition systems, were also an observed tendency in specific mapped regions, which gave rise to human errors. Situations causing analogous effects were identified when the absence, delay in displaying or excess of alarms and indications, among others human-machine issues, affected the human ability to understand an adverse scenario.

These are examples, to name but a few, of accident patterns mined from the MATA-D with the support of the SOM algorithm. Those trends were successfully mapped during the research project, and then converted into a checklist, as presented in Chapter 4. The verification process provided practical means to enhance stakeholders' confidence that

www.manaraa.com

safety studies have assimilated lessons from past major accidents. The disclosed tendencies can be now easily tested against and assimilated by new engineering developments, effectively completing the fourth thesis objective.

A subsequent application was envisioned by focusing on undesirable interfaces associated with the inadequate task allocation organisational factor. The primary goal was to shed some light on decision-making processes under high-hazard circumstances. Issues such as inappropriate task planning, inadequate managerial rules and principles, and poor work instructions (all captured in the MATA-D under the task allocation label) were compared with operational decisions that intended to control a real hydrocarbon leakage in an offshore platform. Eventually, the decision-making process was considered ineffective, as the course of actions resulted in a major disaster with nine fatalities. It was found that the operating environment has held staggering resemblance with undesirable interactions previously identified by the application of the SOM algorithm in many other facilities, thus deeply influencing the decision-making process. This gives strong indication that the decisions made and the resulting actions taken were not exceptional, but followed a well-defined pattern driven by multiple dynamic elements, meaning that tackling contributing factors individually (e.g. better detailing written procedures or improving training) will not suffice.

The case study scrutiny has shown that the mental review of probabilities during decision-making is highly influenced by some biases, such as the impression that it would be tolerable to enter a gas-filled compartment a third time, provided that an explosion has not occurred in two previous occasions. Another important finding was the crew hypothesis fixation in a single and definitive solution, which would solve not only the safety critical issue, but also would allow the return to normal operation. It is important to notice that this is perfectly explainable, as the emergency team was composed by technical crew normally responsible for running the maritime unit, thus the prime goal of resuming operation quickly and safely was deeply ingrained in their minds. Therefore, to simultaneously satisfy these two objectives (continue to operate the facility *and* restore safety), the repair of the source of the hydrocarbon leakage would be the perfect solution. However, other approaches could have given a satisfactory outcome for one of the objectives, e.g. ensuring the safety of personnel, by abandoning the facility and thus reducing the crew exposure to the effects of a possible explosion. This apparently less-than-perfect but, to some extent, effective solution was not even considered, as it would fail to

www.manaraa.com

entirely fulfil the initial premise (i.e. the resuming operation objective) set by the decision-makers. It was also pointed out that the man-machine interface, originally designed to deal with regular operations, failed to provide adequate information to support the recovery from emergency scenarios.

Accordingly, this research project, with the support of the MATA-D output, identified new solutions to improve decision-making processes, encouraging deeper organisational and technological changes. In facilities such as the one considered in the case study, for instance, having personnel entirely dedicated to damage control, with a new man-machine interface designed to give relevant information to the control of emergency scenarios, might offer an effective approach to reduce the likelihood of a major accident. This is a practical example on how the assessment of the complex interactions between human factors, technological aspects and organisational contexts in high-technology facilities can minimise the possibility of human errors, satisfying the last objective set for the current thesis.

ii. Concluding Remarks

This PhD research project reflected in the current dissertation successfully proposed a new method to learn from past accidents, through the creation of a major-accident dataset and the subsequent application of advanced data clustering and classification methods to disclose common patterns. The dataset structure has shown flexibility and aptitude to capture accidents from different industrial backgrounds, allowing the inclusion of several low-frequency, rare events, such as major accidents. The investigation reports were collected from knowledgeable institutions responsible for conducting thorough examinations of disasters, which are, presumably, the most reliable and wide-ranging data source available to offer profounder insights into the manifestation of these complex events.

Learning from accidents is not a simple process, as it involves not only the laborious collection and classification of meaningful data, but also the translation of the information into useful outputs to researchers and practitioners who need to understand how human factors, technology and organisations can come together to produce undesirable outcomes. Yet, the results obtained from the application of innovative data mining techniques to the

www.manaraa.com

Multi-attribute Technological Accidents Dataset strongly suggest that the aim and the main objectives of the research project were entirely satisfied.

The large-scale analysis of major events promoted an enhanced understanding of the so-called human errors, exposing the complex mechanisms and interactions behind disturbances in cognitive functions, which affected human performance in high-hazard environments. The lessons arose from the disclosed tendencies among major accidents, indicating a well-defined path to the genesis and perpetuation of human errors and to tackle complex risks.

The fact that major accidents are rare events, arising from a seemingly unique combination of multiple contributing causes, might give room to some biases, such as the belief that "it could not happen to us", resulting in some resistance to use lessons from disasters to recognise risks. The research findings, however, challenged this objectionable perspective. Provided that unambiguous patterns during the developments of catastrophes were successfully recognised, the "learning from accidents" experience can now be motivated by robust evidence that major accidents are not isolated events, but can be considered a product of repeatable dynamic processes. The existence of some high-technology sectors is very much dependent on the capacity to better understand these intricate processes.

The understanding of the tendencies associated with major accidents was boosted by the application of different data clustering techniques, which converted the multidimensional data to graphical interfaces and thus assisted the disclosure of significant features. The dataset responded well to a tailored hierarchical agglomerative clustering technique and to the application of an artificial neural network approach, which provided innovative means to identify and mitigate major risks.

The Self-Organising Maps algorithm proved to be extremely effective: the representation of significant features in 2-D topographical maps facilitated the communication of relevant risk information to wider stakeholder groups. The visual aids promoted a good alternative to traditional risk communication tools, successfully depicting complex, multi-attribute industrial engineering events in simple and clear images. The data mining strategy also supported the development of a novel risk assessment verification scheme, derived from the interpretation of the most relevant interfaces leading to major accidents. The verification list generated by this research can help specialists to confirm if major risks were

www.manaraa.com

taken into account and serve as input to the development of enhanced major hazard control strategies. The disclosure of common major accident patterns also allowed an improved interpretation of decision-making processes, undermining unbalanced efforts to improve risk, which might be excessively focused on individual human issues, or in the sharp-end of the process. Accordingly, raising stakeholders' awareness to critical safety data justifies profounder changes to sociotechnical systems, especially in the organisational level, as indicated by the current research project findings.

The exploration of the dataset by alternative means, i.e. multidimensional scaling, has shown a fair degree of similarity with the SOM output, supporting the implications of the SOM findings. Regions dominated by individual factors such as Equipment Failure, Inadequate Task Allocation and Design Failure were preserved. Furthermore, relevant features, such as the intersection between Inadequate Task Allocation, Design Failure, Inadequate Quality Control and Inadequate Procedure (discussed in Chapter 4), were also visible, suggesting the consistency of the thesis results.

iii. Future Work Recommendations

The establishment of the dataset, the statistical analysis and further data analysis approaches indicated a well-defined path to understand human errors and the interactions resulting in major accidents. Future research could focus on specific interfaces and approach other data relevant features, in order to improve particular organisational processes such as management, training or quality control. In Morais et al. (2015), for example, data mining was applied to MATA-D in order to disclose undesirable interactions between quality control and maintenance, which were compared to findings from routine offshore inspections. The study revealed that some offshore nonconformities were equivalent to the tendencies extracted from the MATA-D, indicating that these existent failures had the potential to trigger major events.

Following the same principles, practical applications could use the MATA-D output to analyse the current risk level of facilities, to assess the criticality of nonconformities or even to justify the need for investments in specific areas. Future research can build on the theoretical framework presented so far to develop more sophisticated accident causation models, including the investigation of broader influencing factors which are supposed to

www.manaraa.com

play some role in industrial disasters, such as the regulatory, political or the economic environment.

The current research project made use of two specific data analysis approaches to support the findings and conclusions presented. However, due to the characteristics of the dataset structure, other data mining and classification methods can be applied, in an attempt to disclose further features. Doell et al. (2015), for instance, applied frequent itemset followed by association rule mining to the MATA-D, to gain further insight into the main driving forces leading to undesirable outcomes. The dataset structure, containing binary indicators as well as detailed descriptions for contributing factors, favours the application of a wide range of data examination techniques, which might be tested and further interpreted in the search for features of interest. A version of the dataset containing the binary indicators for contributing factors is available upon request (to the Institute for Risk and Uncertainty, University of Liverpool, United Kingdom). The prospect of adding the detailed descriptions for contributing factors to the public version and further disclosure requirements will be discussed with sources, in an attempt to publish the dataset and make it fully available in the future.

Efforts to integrate or compare the MATA-D with existing datasets might well succeed, provided that the taxonomy is general and can be aligned to other dataset structures. The integration can be used to feed datasets with relevant data regarding critical events, and the comparison of the MATA-D with, e.g. a near-misses dataset, can give some indication of facilities or processes demanding special attention. This is particularly useful to institutions (e.g. companies and regulators) which hold extensive portfolios of facilities to manage, being advisable to allocate inspection and audit resources on risk-based grounds.

Apart from developing trust on safety studies, the checklist presented in Chapter 4 could be further adapted to give input to processes such as design reviews, or aligned with regulations to provide an effective verification tool to ensure that technical or mandatory documents (e.g. offshore safety cases) comprises the lessons learned from major accidents.

It is recognised that the major-accident common patterns revealed by the current study were fully based on the 238 events contained in the MATA-D, and future efforts to include further input data might not only strengthen existing findings, but also disclose new patterns and demand further solutions.

www.manaraa.com

The study of sociotechnical systems is a complex, multidisciplinary field, with intrinsic challenges still to overcome. Hence, applications requiring critical data from major accidents and a wider comprehension of relevant interactions involved in these undesirable events can take advantage of the findings hereby presented.

www.manaraa.com

III. List of Publications

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2015. Human error analysis: Review of past accidents and implications for improving robustness of system design, Nowakowski et al. (Eds), *Proceedings of the 24th European Safety and Reliability Conference, 14-18 September 2014, Wroclaw*. London: Taylor & Francis Group, pp. 1037-1046.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2015. Learning from Accidents: Analysis and Representation of Human Errors in Multi-attribute Events, *Proceedings of the 12th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP12, Vancouver, Canada, July 12–15, 2015.*

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2015. Learning from accidents: Analysis of multi-attribute events and implications to improve design and reduce human errors, Podofillini et al. (Eds), *Proceedings of the 25th European Safety and Reliability Conference, 07-10 September 2015, Zurich*. London: Taylor & Francis Group, pp. 3049-3056.

Morais, C., **Moura, R.**, Beer, M. & Lewis, J., 2015. Human factors and quality control procedures: An example from the offshore oil & gas industry, Podofillini et al. (Eds), *Proceedings of the 25th European Safety and Reliability Conference, 07-10 September 2015, Zurich.* London: Taylor & Francis Group, pp. 3835-3841.

Moura, R., Beer, M., Doell, C., Kruse, R. 2015. A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors, Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence (SSCI2015), Cape Town, South Africa, December 8-10, 2015.

Doell, C., Held, P., **Moura, R.**, Kruse, R., Beer, M., 2016. Analysis of a major-accident dataset by Association Rule Mining to minimise unsafe interfaces, Patelli & Kougioumtzoglou (Eds), *Proceedings of the 13th International Probabilistic Workshop (IPW 2015), Liverpool, UK, 4-6 November 2015*. Research Publishing, pp. 212-224.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2016. Learning from major accidents to improve system design, *Safety Science 84*: 37-45.

Moura, R., Beer, M., Patelli, E. & Lewis, J., 2017. Learning from accidents: Investigating the genesis of human errors in multi-attribute settings to improve the organisation of design, Walls et al. (Eds), *Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, Glasgow, Scotland, 25-29 September 2016*. London: Taylor & Francis Group, pp. 228-256.

Moura R., Beer, M., Patelli, E. & Lewis, J., 2017. Learning from major accidents: graphical representation and analysis of multi-attribute events to enhance risk communication, *Safety Science 99*: 58-70.

Moura R., Morais, C., Patelli, E., Beer, M., & Lewis, J., 2017. Human factors influencing decision-making: tendencies from first-line management decisions and implications to reduce major accidents, *Safety and Reliability – Theory and Applications,* Crepin & Briš (eds), pp. 251-260. London: Taylor & Francis Group.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2017. Learning from accidents: interactions between human factors, technology and organisations as a central element to validate risk studies, *Safety Science 99*: 196-214.

www.manaraa.com

IV. Bibliography

Andreev, A. and Argyrou, A., 2011. Using Self-Organizing Map for Data Mining: A Synthesis with Accounting Applications. *Data Mining: Foundations and Intelligent Paradigms*, vol 3. Ed 1. Berlin: Springer.

ANP - National Agency for Petroleum, Natural Gas and Biofuels, 2015. *Investigation Report – FPSO Cidade de São Mateus Explosion on 11 February 2015* [Online]. Rio de Janeiro: ANP. Available from: http://www.anp.gov.br/anexos/43C4E304D789C9DC83257F5C003527F6/ANP_Final_Report_FPSO_CDSM_accident_.pdf (Accessed: 18 December 2016).

Airbus, 2016. *Airbus Family Figures March 2016 Edition*. Blagnac Cedex: Airbus Print Centre. Available from: http://www.airbus.com/fileadmin/media_gallery/files/brochures_publications/aircraft_families/Airbus-Family-figures-booklet-March2016.pdf (Accessed: 04 May 2016).

Arstad, I. and Aven, T., 2017. Managing major accident risk: Concerns about complacency and complexity in practice. *Safety Science 91*: 114-121.

Aven, T., 2013. On the meaning of the black swan concept in a risk context, *Safety Science 57*: 44–51.

Aven, T., 2015. Implications of black swans to the foundations and practice of risk assessment and management, *Reliability Engineering and System Safety 134*: 83–91.

Barriere, M. *et al*., 2000. *NUREG-1624 - Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*. Washington, D.C.: US Nuclear Regulatory Commission.

BBC News, 2014. *South Korea ferry disaster: New arrests*. Available from: http://www.bbc.co.uk/news/world-asia-27124528 (Accessed: 01 March 2016).

Baysari, M., McIntosh, A. and Wilson, J., 2008. Understanding the human factors contribution to railway accidents and incidents in Australia, *Accident Analysis and Prevention 40*: 1750-1757.

Bell J & Holroyd J., 2009. *Review of human reliability assessment methods*. Suffolk: HSE Books.

Bell, J., 2012. The Gulf Spill: BP Still Doesn't Get It. In Allen, F. E. (ed), *Forbes, 20 April 2012*. [Online] Available from: http://www.forbes.com/sites/frederickallen/2012/04/20/the-gulf-spill-bp-still-doesnt-get-it/ (Accessed: 06 November 2014).

Bellamy L.J. et al., 2007. Storybuilder — A tool for the analysis of accident reports. *Reliability Engineering and System Safety 92*: 735-744.

Bellamy, L.J. et al., 2013. Analysis of underlying causes of investigated loss of containment incidents in Dutch Seveso plants using the Storybuilder method. *Journal of Loss Prevention in the Process Industries* 26: 1039-1059.

www.manaraa.com

Berthold, M. et al., 2010. *Guide to Intelligent Data Analysis: How to Intelligently Make Sense of Real Data*. Springer Science & Business Media.

Bills, K and Agostini, D., 2009. *Offshore petroleum safety regulation – Varanus Island Incident Investigation*. Government of West Australia. ISBN: 978-1-921602-56-6

Blajev, T., 2002. *SOFIA (Sequentially Outlining and Follow-up Integrated Analysis) Reference Manual*. Brussels: EATMP Infocentre.

Bray, J. and Curtis, J., 1957. "An ordination of the upland forest communities of southern Wisconsin." *Ecological monographs 27(4)*: 325-349.

British Petroleum, 2010. *Deepwater Horizon – Accident Investigation Report, 8 September 2010* [Online]. Available from: http://www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report.pdf (Accessed 25 September 2016).

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2011. *Final Report on the accident on 1st June 2009 to the Airbus A330-203* [Online]. Available from: http://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf (Accessed: 06 November 2014).

Bureau of Ocean Energy, Management, Regulation and Enforcement (BOMRE), 2011. *Report regarding the causes of the April 20, 2010 Macondo well blowout* [Online]. Available at: https://www.bsee.gov/sites/bsee.gov/files/reports/blowout-prevention/dwhfinaldoi-volumeii.pdf (Accessed 20 April 2017).

Burgherr P. & Hirschberg, S., 2016. Comparative Risk Assessment of severe accidents in the energy sector. *Energy Policy 74(1)*: S45-S46.

Casal, J., 2008. *Evaluation of the effects and consequences of major accidents in industrial plants*. Amsterdam: Elsevier.

Center for Catastrophic Risk Management (CCRM), 2011. *Final Report on the Investigation of the Macondo Well Blowout* [Online]. Available at: http://ccrm.berkeley.edu/pdfs_papers/bea_pdfs/dhsgfinalreport-march2011-tag.pdf (Accessed 25 September 2016).

Chang, J.Y. et al., 2014. The SACADA database for human reliability and human performance. *Reliability Engineering and System Safety 125*: 117–133.

Cohen, M., March, J. and Olsen, J., 1972. A Garbage-Can Model of Organisational Choice, *Administrative Science Quarterly 17(1)*: 1–25.

COMAH – Control of Major Accident Hazards, 2011. *Buncefield: Why did it happen? The underlying causes of the explosion and fire at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005*. London: H.M. Stationery Office.

www.manaraa.com

Cooper, S. et al., 1996. *NUREG/CR-6350 - A Technique for Human Error Analysis (ATHEANA) - Technical Basis and Methodology Description.* Washington, D.C.: US Nuclear Regulatory Commission Library.

Cottrell, M., Olteanu, M., Rossi, F. and Villa-Vialaneix, N., 2016. Theoretical and Applied Aspects of the Self-Organizing Maps, *Proceedings of the 11th International Workshop WSOM 2016*, Houston, Texas, USA, January 6−8, 2016.

Cullen, W., 1990. *The public inquiry into the Piper Alpha disaster*. London: Her Majesty's Stationery Office (HMSO).

Cuny, X. and Lejeune, M., 2003. Statistical modelling and risk assessment, *Safety Science 41*: 29–51.

Dahle et al., 2012. Major accidents and their consequences for risk regulation, *In: Advances in Safety, Reliability and Risk Management*, Bérenguer, Grall & Guedes Soares (eds). London: Taylor & Francis Group.

Davis, G., Wanna, J., Warhurst, J. & Weller, P., 1998. *Public Policy in Australia*. 1st edn. Sydney: Allen & Unwin.

Dekker, S., 2014. *Field Guide to Understanding 'Human Error'*. 3rd ed. Farnham: Ashgate Publishing Ltd, 2014.

Dhillon, B.S., 1986. *Human Reliability: With Human Factors*. New York: Pergamon Press Inc.

Dhillon, B.S., 2007. *Human reliability and error in transportation systems*. 1st ed. London: Springer-Verlag.

Doell, C., Held, P., Moura, R., Kruse, R., and Beer, M., 2015. Analysis of a major-accident dataset by Association Rule Mining to minimise unsafe interfaces, *Proceedings of the International Probabilistic Workshop (IPW2015)*, Liverpool, UK, November 4-6, 2015.

DPC – Directorate of Ports and Coasts, 2015. *Maritime Safety Investigation Report - "FPSO CIDADE DE SAO MATEUS" explosion with victims* [Online]. Rio de Janeiro: Brazilian Navy. Available from: https://www.dpc.mar.mil.br/sites/default/files/diian/rel_acidentes/smateus/fpso_cidade_smateus_en.pdf (Accessed: 18 December 2016).

European Safety, Reliability and Data Association (ESReDA), 2015. *Barriers to learning from incidents and accidents* [Online]. Available from: http://esreda.org/wp-content/uploads/2016/03/ESReDA-barriers-learning-accidents-1.pdf (Accessed 20 April 2017).

Evans, A., 2011. Fatal train accidents on Europe's railways: 1980-2009, *Accident Analysis and Prevention 43*: 391-401.

Everdij, M. & Blom, H., 2013. *Safety Methods Database version 1.0* [Online]. Amsterdam: National Aerospace Laboratory (NLR). Available from: http://www.nlr.nl/downloads/safety-methods-database.pdf (Accessed: 9 April 2014).

www.manaraa.com

Forester, J. et al., 2014. *NUREG-2127 - The International HRA Empirical Study - Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data*. Washington D.C.: US Nuclear Regulatory Commission.

Forester, J. et al., 2016. *NUREG-2156 - The U.S. HRA Empirical Study - Assessment of HRA Method Predictions against Operating Crew Performance on a U.S. Nuclear Power Plant Simulator*. Washington D.C.: US Nuclear Regulatory Commission.

Fowler, T., 2013. BP Faces New Bout of Spill Liability. *The Wall Street Journal, 18 February 2013*. New York: Dow Jones & Company, Inc.

Fukasawa, J., Okusaki, M., 2012. *Reform of the Nuclear Safety Regulatory Bodies In Japan*, International Nuclear Law Association Congress, 8–11 October, Manchester, UK.

Gibson W. H. & Megaw T. D., 1999. *The implementation of CORE-DATA, a computerised human error probability database.* Suffolk: HSE Books.

Grabowski, M. et al., 2009. Human and organizational error data challenges in complex, large-scale systems. *Safety Science* 47: 1185-1194.

Grabowski, M. and Roberts, K., 1997. Risk Mitigation in Large-Scale Systems: lessons from high reliability organisations. *California Management Review 39(4)*: 152-162.

Graeber, C., 1999. *The Role of Human Factors in Aviation Safety in Aero Magazine QTR_04 1999* (p. 23-31). The Seattle: Boeing Commercial Airplanes Group.

Groth, K.M. and Mosleh, A., 2012. Deriving causal Bayesian networks from human reliability analysis data: A methodology and example model. *Journal of Risk and Reliability 226(4)*: 361–379.

Health and Safety Executive (HSE), 1994. *A report of the investigation by the Health and Safety Executive into the fatal fire at Hickson & Welch Ltd., Castleford, on 21 September 1992*. London: H.M. Stationery Office.

Heinrich, H., Peterson, D. and Roos, N., 1980. *Industrial Accident Prevention.* 5th Ed. New York: Mcgraw-Hill.

Herrmann, J., 2015. *Engineering Decision Making and Risk Management*. New Jersey: John Wiley & Sons, Inc.

Hollnagel, E., 1993. The phenotype of erroneous actions. *International Journal of Man-Machine Studies*, 39, 1-32.

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

Hollnagel, E., Paries, J., Woods, D.D. and Weathall, J., 2011. *Resilience engineering in practice: A guidebook*. London: Ashgate.

www.manaraa.com

Hollywell, P.D., 1996. Incorporating human dependent failures in risk assessments to improve estimates of actual risk. *Safety Science 22:* 177–194.

Hopkins, A., 1999. The limits of normal accident theory, *Safety Science*, 32, pp. 93-102.

Hopkins, A., 2003. *Working Paper 7 - Safety culture, mindfulness and safe behaviour: Converging ideas?* National Research Centre for OHS Regulation [Online]. Available at: http://regnet.anu.edu.au/sites/default/files/publications/attachments/2015-05/WorkingPaper_7_0.pdf (Accessed on 15 February 2017).

Hopkins, A. 2005. *Safety, culture and risk: the organisational causes of disasters*. Sydney, NSW: CCH Australia.

Hopkins, A., 2006. *A corporate dilemma: To be a learning organisation or to minimise liability. Technical report,* Australian National University, Canberra, Australia. National Center for OSH regulation Working Paper 43. Available from: https://digitalcollections.anu.edu.au/bitstream/1885/43147/2/wp43-corporatedilemma.pdf. (Accessed 20 April 2017).

International Atomic Energy Agency, 1990. Human Error Classification and Data Collection. *Report of a technical committee meeting organised by the IAEA, Vienna, 20-24 February 1989*. Vienna: INIS Clearinghouse.

Ishikawa, M., 2015. *A Study of the Fukushima Daiichi Nuclear Accident Process - What caused the core melt and hydrogen explosion?* Tokyo: Springer.

Johnson, C., 2008. Ten contentions of corporate manslaughter legislation: Public policy and the legal response to workplace accidents. *Safety Science 46*: 349-370.

Kim, Y, Park, J. and Jung, W., 2017. A classification scheme of erroneous behaviors for human error probability estimations based on simulator data. *Reliability Engineering and System Safety 163*: 1-13.

Kirwan, B., 1997a. Validation of Human Reliability Assessment Techniques: Part 1 – Validation Issues. *Safety Science 27(1)*: 25-41.

Kirwan, B., 1997b. Validation of Human Reliability Assessment Techniques: Part 2 – Validation Results. *Safety Science 27(1)*: 43-75.

Kirwan, B. and James, N.J., 1989. Development of a human reliability assessment system for the management of human error in complex systems. *Proceedings of the Reliability '89, Brighton, 14-16 June*: pp. 5Al2/1-5A/2/11.

Kirwan, B. et al., 2005. Nuclear action reliability assessment (NARA): a data-based HRA tool, *Safety & Reliability*, 25, No. 2, pp. 38–45.

Kletz, T., 1997. *Lessons from Disaster - how organisations have no memory and accidents recur*, Institution of Chemical Engineers, Rugby, UK.

Kohonen, T. et al., 1996. *Engineering Applications of the self-organizing map*, Proceedings of the IEEE 10, Vol. 84, October 1996.

www.manaraa.com

Kohonen, T., 1998. The self-organizing map. *Neurocomputing 21*: 1-6.

Kohonen, T., 2001. *Self-Organizing Maps*. 3rd ed. Berlin: Springer.

Kohonen, T., 2013. Essentials of the self-organizing map, *Neural Networks 37*: 52-65.

Kruse, R. et al., 2013. *Computational intelligence – A Methodological Introduction*. London: Springer, 2013.

Kurokawa, K. et al., 2012. *The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission - Executive Summary* [Online] Tokyo: The National Diet of Japan. Available from: https://www.nirs.org/fukushima/naiic_report.pdf (Accessed: 6 November 2014).

La Porte, T., & Consolini, P., 1998. Theoretical and operational challenges of high reliability organisations: air traffic control and aircraft carriers. *International Journal of Public Administration 21 (6-8*): 847-852

Le Coze, J-C., 2013. New models for new times. An anti-dualist move. *Safety Science 59*: 200–218.

Leveson, N., 2004. A new accident model for engineering safer systems. *Safety Science* 42: 237-270.

Leveson, N., 2011. Applying systems thinking to analyze and learn from events. *Safety Science 49(6)*: 55–64

Leveson, N., 2012. *Engineering a safer world: systems thinking applied to safety.* Cambridge Massachusetts Institute: The MIT Press.

Licu, T. et al., 2007. Systemic Occurrence Analysis Methodology (SOAM) - A "Reason"-based organisational methodology for analysing incidents and accidents. *Reliability Engineering and System Safety* 92: 1162-1169.

Lindberg, A-K., Hansson, S. and Rollenhagen, C., 2010. Learning from accidents – What more do we need to know? *Safety Science 48*: 714-721.

McLaughlin, T., Monahan, S., Pruvost, N., Frolov, V., Ryazanov, B. & Sviridov, V., 2000. *A Review of Criticality Accidents.* New Mexico: Los Alamos National Laboratory.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2015a. Human error analysis: Review of past accidents and implications for improving robustness of system design, Nowakowski, T. et al. (Eds), *Proceedings of the 24th European Safety and Reliability Conference, 14-18 September 2014, Wroclaw*. London: Taylor & Francis Group, pp. 1037-1046.

Moura, R., Beer, M., Patelli, E., Lewis, J. and Knoll, F., 2015b., Learning from Accidents: Analysis and Representation of Human Errors in Multi-attribute Events, *Proceedings of the 12th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP12*, Vancouver, Canada, July 12–15, 2015.

www.manaraa.com

Moura, R., Beer, M., Doell, C. and Kruse, R., 2015c. A Clustering Approach to a Major-Accident Data Set: Analysis of Key Interactions to Minimise Human Errors, *Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence (SSCI2015), Cape Town, South Africa, December 8-10, 2015*.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2016. Learning from major accidents to improve system design, *Safety Science 84*: 37-45.

Moura, R. et al., 2017a. Learning from accidents: Investigating the genesis of human errors in multi-attribute settings to improve the organisation of design, *Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, Glasgow, Scotland, 25-29 September 2016*. London: Taylor & Francis Group.

Moura, R., Beer, M., Patelli, E. & Lewis, J., 2017b. Learning from major accidents: graphical representation and analysis of multi-attribute events to enhance risk communication, *Safety Science 99*: 58-70.

Moura, R., Morais, C., Patelli, E., Beer, M., & Lewis, J., 2017c. Human factors influencing decision-making: tendencies from first-line management decisions and implications to reduce major accidents, *Safety and Reliability – Theory and Applications,* Crepin & Briš (eds), pp. 251-260. London: Taylor & Francis Group.

Moura, R., Beer, M., Patelli, E., Lewis, J. & Knoll, F., 2017d. Learning from accidents: interactions between human factors, technology and organisations as a central element to validate risk studies, *Safety Science 99:* 196-214.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling., 2011. *The Gulf Oil Disaster and the Future of Offshore Drilling – Report to the President* [Online] Washington D.C.: U.S. Government Printing Office. Available from: http://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf (Accessed: 20 July 2015).

National Transportation Safety Board (NTSB), 2013. *Crash Following Loss of Engine Power Due to Fuel Exhaustion, Air Methods Corporation, Eurocopter AS350 B2, N352LN, Near Mosby, Missouri, August 26, 2011. Aircraft Accident Report AAR-13/02.* Washington, DC: NTSB.

Nielsen, DS., 1971. *The cause/consequence diagram method as a basis for quantitative accident analysis*. Risø-M 1374.

Oxstrand J., 2010. *Human reliability guidance – how to increase the synergies between human reliability, human factors, and system design and engineering. Phase 2: The American point of view – insights of how the US nuclear industry works with human reliability analysis.* Nordic Nuclear Safety Research Council (NKS) Technical Report, NKS-229, December 2010.

Paté-Cornel, M., 1993. Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organizational Factors, *Risk Analysis*, Vol. 13, No. 2, 1993 215-232.

Paté-Cornell, M., 2012. On “Black Swans” and “Perfect Storms”: risk analysis and management when statistics are not enough, *Risk Analysis* 32 (11): 1823-1833.

www.manaraa.com

Pennycook, W. & Embrey, D., 1993. 'An operating approach to error analysis', *Proceedings of the First Biennial Canadian Conference on Process Safety and Loss Management*, April, Edmonton, Canada.

Perrow, C., 1999. *Normal Accidents: Living With High-Risk Technologies*. New Jersey: Princeton University Press.

Pidgeon, N. and O'Leary, M., 2000. Man-made disasters: why technology and organizations (sometimes) fail, *Safety Science 34*: 15-30.

Preischl, W. and Hellmich, M., 2013. Human error probabilities from operational experience of German nuclear power plants. *Reliability Engineering and System Safety 109*: 150-159.

Rasmussen, J., 1983. Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models, *IEEE Transactions on Systems, Man and Cybernetics* 3, May, vol. SMC-13.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem, *Safety Science 27*: 183–213.

Reason, J., 1990. *Human Error*. Cambridge: Cambridge University Press.

Reason, J., 1997. *Managing the Risks of Organizational Accidents.* Brookfield, USA: Ashgate.

Reason, J., 2000. Safety paradoxes and safety culture, *Injury Control & Safety Promotion 7(1)*: 3-14.

Reason, J., 2013. *A Life in Error: From Little Slips to Big Disasters.* 1st ed. Farnham: Ashgate Publishing Ltd.

Roberts, K., 1990. Some Characteristics of one type of high reliability organizations. *Organization Science 1(2)*: 160-176.

Roberts K. and Bea, R., 2001. Must accidents happen? Lessons from high-reliability organizations. *The Academy of Management Executive 15*: 70–78.

Rogers, P. and Blenko, M., 2006. Who has the D? How clear decision roles enhance organisational performance. *Harvard Business Review 84(1)*: 53-61.

Rousseeuw, P.J., 1987. Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. *Journal of computational and applied mathematics 20*: 53–65.

Sagan, S., 1993. *The Limits of Safety: organisations, accidents and nuclear weapons.* New Jersey: Princeton University Press.

Schneider et al., 2012. *The World Nuclear Industry Status Report 2010–2011 - Nuclear Power in a Post-Fukushima World and 25 Years after the Chernobyl Accident*. Washington, D.C.: Worldwatch Institute. Available from:

www.manaraa.com

http://www.worldnuclearreport.org/The-World-Nuclear-Industry-Status-51.html (Accessed 20 April 2017).

Schröder-Hinrichs, J-U., Hollnagel, E. and Baldauf, M., 2012. From Titanic to Costa Concordia — a century of lessons not learned. *WMU Maritime Affairs 11*:151-167.

Shappell, S., et al., 2007. Human Error and Commercial Aviation Accidents: An Analysis Using the Human Factors Analysis and Classification System. *Human Factors* 49(2): 227-242.

Shirley, R.B., Smidts, C., Li, M. and Gupta, A., 2015. Validating THERP: Assessing the scope of a full-scale validation of the Technique for Human Error Rate Prediction. *Annals of Nuclear Energy 77*: 194-171.

Skogdalen, J. and Vinnem, JE., 2011. Quantitative risk analysis offshore - Human and organizational factors. *Reliability Engineering and System Safety 96*: 468–479

Skogdalen, J. and Vinnem, JE., 2012. Quantitative risk analysis of oil and gas drilling, using Deepwater Horizon as case study, *Reliability Engineering and System Safety 100*: 58–66.

Snowden, D. and Boone, M., 2007. A leader's framework for decision making. *Harvard Business Review 85(11)*: 69-76.

Spetzler, C., 2007. *Building decision competency in organisations, Advances in Decision Analysis: From Foundations to Applications.* Edwards, W., Miles, R. and Winterfeldt, D. (eds.). Cambridge: Cambridge University Press.

Sträter, O., 2000. *Evaluation of Human Reliability on the Basis of Operational Experience*. Cologne: GRS. (English translation of the Report GRS-138: Beurteilung der menschlichen Zuverlassigkeit auf Basis von Betriebserfahrung.)

Swain, A., 1963. *A Method for Performing Human Factors Reliability Analysis,* Monograph-6851, Albuquerque: Sandia National Laboratories.

Swain, A., 1982. Modeling of Response to Nuclear Power Plant Transients for Probabilistic Risk Assessment, *Proceedings of the 8th Congress of the International Ergonomics Association*, August, Tokyo.

Swain, A., 1990. Human Reliability Analysis - Need, Status, Trends and Limitations. *Reliability Engineering and System Safety* 29: 301-313.

Swain, A., & Guttmann, H., 1983. *NUREG/CR 1278 - Handbook of Human Reliability Analysis with Enphasis on Nuclear Power Plant Applications*. Albuquerque: Sandia National Laboratories.

Taleb, N., 2007. *The Black Swan: The Impact of the Highly Improbable*. 2nd Ed. York: Allen Lane.

The Control of Major Accident Hazards Regulations, 1999 [Online]. Available from: http://www.legislation.gov.uk/uksi/1999/743/contents/made. Surrey: National Archives. (Accessed: 06 November 2014).

www.manaraa.com

The Offshore Installations (Safety Case) Regulations, 2005 [Online]. Available from: http://www.legislation.gov.uk/uksi/2005/3117/made. Surrey: National Archives. (Accessed: 06 November 2014).

Ultsch, A., 1993. Self-organizing neural networks for visualization and classification. *In: Opitz, O., Lausen, B., Klar, R. (eds.). Information and Classification*. Berlin: Springer: 307–313.

Ung, S-T., 2015. A weighted CREAM model for maritime human reliability analysis. *Safety Science 72*: 144-152.

United States Chemical Safety and Hazard Investigation Board (US-CSB), 2003. *Investigation Report No. 2003-06-I-TX, Vapour cloud deflagration and fire at BLSR Operating Ltd., Rosharon, Texas, on 13 January 2003*. Washington, D.C.: US-CSB Publications.

United States Chemical Safety and Hazard Investigation Board (US-CSB), 2004. *Safety Bulletin No. 2004-03-B, July 2004.*

United States Chemical Safety and Hazard Investigation Board (US-CSB), 2005a. *Investigation Report No. 2003-09-I-KY, Combustible dust fire and explosions at CTA Acoustics, Inc., Corbin, Kentucky, on 20 February 2003*. Washington, D.C.: US-CSB Publications.

United States Chemical Safety and Hazard Investigation Board (US-CSB), 2005b. *Case Study 2004-08-I-NM Oil Refinery Fire and Explosion*. Washington, DC: CSB Publications.

United States Chemical Safety Board (US-CSB), 2016. *Investigation Report – explosion and fire at the Macondo well* [Online]. Available at: http://www.csb.gov/macondo-blowout-and-explosion/ (Accessed 20 April 2017).

United States Coast Guard (USCG), 2010. *Report of Investigation into the Circumstances Surrounding the Explosion, Fire, Sinking and Loss of Eleven Crew Members Aboard the Mobile Offshore Drilling Unit Deepwater Horizon* [Online]. Available at: https://www.bsee.gov/sites/bsee.gov/files/reports/safety/2-deepwaterhorizon-roi-uscg-volume-i-20110707-redacted-final.pdf (Accessed 20 April 2017).

US Nuclear Regulatory Commission, 2008. Human events repository and analysis (HERA) database. https://hera. inl.gov. (Accessed 01 August 2017).

Vaughan, D., 1996. *The Challenger launch decision: risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press.

Williams, J.C., 1986. HEART - A Proposed Method for Assessing and Reducing Human Error. *Proceedings of the 9th Advances in Reliability Technology Symposium, Bradford, 2-4 April 1986.* Warrington: National Centre of Systems Reliability.

Woods, D. et al., 2010. *Behind Human Error*. 2nd ed. Farnham: Ashgate Publishing Ltd.

Zhou, Q. et al., 2017. An enhanced CREAM with stakeholder-graded protocols for tanker shipping safety application. *Safety Science 95*: 140-147.

www.manaraa.com

Zuijderduijn, C., 2000. *Risk management by Shell Refinery/Chemicals at Pernis, The Netherlands*. EU Joint Research Centre Conference on Seveso II Safety Cases, Athens.

www.manaraa.com