Safety Science xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Safety Science

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

Learning from accidents: Interactions between human factors, technology and organisations as a central element to validate risk studies

Raphael Moura [a,c,*], Michael Beer [b,a,e], 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
[e] Tongji University, Shanghai, China

ARTICLE INFO

Article history:
Received 18 November 2016
Received in revised form 15 March 2017
Accepted 2 May 2017
Available online xxxx

Keywords:
Risk studies validation
Learning from accidents
MATA-D
Human factors
Organisations
Self-organising maps

ABSTRACT

Many industries are subjected to major hazards, which are of great concern to stakeholders groups. Accordingly, efforts to control these 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 revealed that apparently rare or seemingly unforeseen scenarios, involving complex interactions between human factors, technologies and organisations, are capable of triggering major catastrophes. The purpose of this work is to enhance stakeholders' trust in risk management by developing a framework to verify if tendencies and patterns observed in major accidents were appropriately contemplated by risk studies. This paper first discusses the main accident theories underpinning major catastrophes. Then, an accident dataset containing contributing factors from major events occurred in high-technology industrial domains serves as basis for the application of a clustering and data mining technique (self-organising maps – SOM), allowing the exploration of accident information gathered from in-depth investigations. Results enabled the disclosure of common patterns in major accidents, leading to the development of an attribute list to validate risk assessment studies to ensure that the influence of human factors, technological issues and organisational aspects was properly taken into account.

1. Introduction

1.1. Accident causation models and implications to validate risk assessments

Accident causation models lie beneath all efforts related with safety engineering, as they serve as 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 (1984), 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 safely run these facilities: a military-shaped organisation, authoritarian and rigidly disciplined. However, he claimed that this administration

---

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

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

http://dx.doi.org/10.1016/j.ssci.2017.05.001
0925-7535/© 2017 Elsevier Ltd. All rights reserved.

Please cite this article in press as: Moura, R., et al. Learning from accidents: Interactions between human factors, technology and organisations as a central element to validate risk studies. Safety Sci. (2017), http://dx.doi.org/10.1016/j.ssci.2017.05.001

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, 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 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 and Roberts, 1997; La Porte and 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 (1984), 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 (see Table 1).

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 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

Please cite this article in press as: Moura, R., et al. Learning from accidents: Interactions between human factors, technology and organisations as a central element to validate risk studies. Safety Sci. (2017), http://dx.doi.org/10.1016/j.ssci.2017.05.001