What can we learn from the various non-technical accident causation theories?

Kehinde Shaba, Senior Consultant, DNV GL, 200 Great Dover Street, London, UK. SE1 4YB.

Following a major accident in the industry, engineers tend to place primary emphasis on the technical aspects of the event notably hardware and front line personnel. This is understandable and a natural starting point given what they do. But there is a lot that can be learnt from the perspectives brought to bear on the issue by other disciplines especially social scientists (e.g. psychologists). This paper outlines a selection of non–technical accident causation theories in literature that have been used to explain why accidents happen. It explores and examines their application to certain accidents and highlights the insights they have helped to generate. The trend to bring multiple disciplinary perspectives to bear on an unwanted event has gained traction in recent times and much more can be done to foster this development. Bringing such insights to the forefront in accident analysis and more importantly making them core considerations will help to ensure more robust lessons are indeed learnt from these accidents and should ultimately help to prevent their reoccurrence.

1. Introduction

Knowledge of the causal nature of accidents has vastly increased in recent times. The orthodox narrow and myopic focus on trigger events (people or equipment) has given way to detailed consideration of the way wider systemic considerations help influence and create the requisite preconditions for disaster. The view of front line personnel has changed from "accident instigators" to "accident inheritors". Causal factors are now generally seen as occupying a spectrum (active to latent/root to initial) as opposed to emphasis on a single fixed point. Also, as people do not work in a vacuum, the influence of the social context on the actions of individuals has also come into sharp focus. To what extent does their environment influence their actions? How much "agency" do they have in deciding their actions or is this structurally determined and influenced by the power structures higher up and further back within the organizational setting. Are there peculiarities about the system they work in (organization, institution, society) that are "disaster encouraging"? If so, what are these and how can they be made manifest? Additionally, systems typically incorporate both human (i.e. social) and technical components and as a result have come to be known as "sociotechnical" systems. Likewise, organizations operate within this socio-technical framework and thus the disasters they create are termed "sociotechnical" disasters in explicit recognition of the role that social or technical factors can play individually or in tandem in facilitating disasters.

To sum: a spectral based view of causal factors, broader systemic considerations, the characteristics of organizations, the acknowledgement of the sociotechnical environment and institutional design have all come to be part and parcel of how we currently understand accidents. But how has this come to be? Largely as a result of non-technical disciplines taking an interest in the issue and bringing their views to therein. This paper examines and explores five selected non-technical models of accident causation that are considered to have provided key insights and been seminal in improving and expanding how accidents are understood. The models are:

1. Disaster/Accident Incubation Theory
2. Normal Accident Theory (NAT)
3. High Reliability Theory (HRT)
4. Latent and Active Failures
5. Sociotechnical Systems

It is evident that other models exist. The goal here is not to identify every possible theory but to consider a select few and the insights that can be developed from these. Those listed above have been selected on the basis that they provide significant explanatory value to the nature of accidents.

A notable exception to the listing above is the concept of "Safety Culture". The concept has increasingly been used to explain the nature of accidents from an organizational perspective. The key elements of a safety culture are largely mirrored by the insights developed by HRT and are thus not outlined here for the simple reason of conciseness. It is important to note however, that the concept plays an important role in this area. Omission should not be construed as unimportant.

This paper is organized as follows. Section 1 (the introduction) outlines the subject matter and scope of the paper. The contention is made that a significant shift in how disasters are understood has occurred and that a core selection of five models of accident causation lie at the core of this change. A brief *introduction to* and *exposition of* the five identified accident causation models is the focus of Section 2. Each model is discussed in turn and the key insights identified therein are enumerated. References to their explicatory power are outlined in the form of their application to the understanding and analysis of selected historical accidents. Inherent model weaknesses are identified and discussed. Conclusions are then provided in Section 3. Works cited are detailed in Section 4.

2. Non-technical Theories of Accident Causation

2.1 Disaster/Accident Incubation Theory

At the heart of this is a concept called the "man-made disaster" an idea that places emphasis on the organizational and managerial processes which taken together incubate the disaster or crises (Turner, 1978, Turner and Pidgeon, 2003).

The model is predicated on two key insights. First, system failures are rarely ever the result of a single causal factor. Second, the requisite conditions for such a failure do not develop instantly but rather develop (or to paraphrase him "incubate" over a period of time). The upshot of this is that multiple causal factors interact, accumulate, and concatenate—for the most part unnoticed, in others noticed but underappreciated—over a period of time (the incubation period) and create the necessary conditions for the failure or disaster.

Retrospective analysis of the incubation period associated with system failures tends to throw up certain recurring themes as shown in Table 1.

Table 1: Recurring themes associated with system failures

Theme	Description	Possible causes	System failures identified in (examples)
Missed hazards/events/early warning signals	This refers to the situation where hazards are missed	Hazards are hidden from view/unnoticed possibly due to system complexity Hazards are noticed but no actions taken. Lack of appreciation for the significance of a hazard The relative significance of a hazard drowned out or diminished due to other visible and seemingly more pressing hazards or priorities (which also act as distractions). Tunnel vision. Narrow outlook of responsible persons	Brazil P-36, (Inquiry Commission P36 Accident, 2001) Montara (Borthwick, 2010) Macando Blowout (NAE/NRC, 2011) Mexico Usumancita (Comisión Especial Independiente, 2007)
Poor information handling in complex systems and situations		Poor communication channels Unclear and ambiguous orders and task definition Complex systems are characterized by an overabundance of information. Lack of processes to separate the "wood from the trees" i.e. what is significant and what is not.	Macando Blowout (NAE/NRC, 2011)
Poor decision making		Uncertainty/lack of procedures as to how to handle unprecedented events.	Brazil P-36, (Inquiry Commission P36 Accident, 2001) Mumbai High North (Verma, 2011)
Feeling of invulnerability		The belief that the danger will not happen here The tendency to reduce the significance of the danger as it develops Collective refusal by a team of responsible persons of evidence of a disaster. This is termed "Group think" (a socially determined form of mindset identified by Janis, 1971)	Macando Blowout (NAE/NRC, 2011)
Normalization of deviance		Operating outside the design envelope.	In most organizational disasters, this is often made manifest by the failure to act on relevant risk information because of deeply entrenched organizational assumptions. The lack of action around a known O-ring issue in the Space challenger disaster as pointed out by Vaughan (1996) is a case in point.

Each theme identified above, though considered independently, tends not to be unique in its own right, but is rather closely inter related and connected to other themes. For example, poor information handling clearly influences decision making ability.

2.2 Normal Accident Theory

Despite the best efforts of organizations to manage the attendant risks of high risk technologies, accidents continue to happen, and ones with catastrophic potential. These range from accidental releases of chemicals to accidents at nuclear power plants. Conventional thinking places the blame on factors such as human error; faulty design etc. and corrective measures follow suite.

Research by Charles Perrow, a sociologist, challenges this viewpoint (Perrow, 1984). The primary contention made is that certain characteristics of these high risk systems—namely, their "interactive complexity" and "tight coupling"—make them predisposed to accidents irrespective of any control measures in place. This work has come to be known as "Normal Accident Theory". These accidents as termed "normal", because they occur under standard everyday circumstances; understanding high risk systems is central to reducing the frequency of accidents or even eliminating them.

Interactive complexity refers to the processes by which multiple failures of components of a system can interact in an unforeseen manner; whilst tight coupling implies working with tight constraints, with limited margin of safety or error. The former introduces a degree a complexity that goes beyond our current understanding whilst the latter leaves little room for remedial action. Perrow explores his hypothesis using various high risk technologies as case studies. In Three Mile Island, he identifies a series of component failures that interact unexpectedly to trigger what might have been America's worst nuclear disaster. In the Texas City explosions of 1947 and 1969, similar interactions are observed.

Taken together, these two factors can be used in classifying various technologies (see Figure 1) and certain remedial actions can then be proposed to prevent crises based on the quadrant to which a technology lies. Centralization or decentralization of authority is a key consideration. The latter is recommended for systems that exhibit a high degree of complexity. It is important to note that conventional approaches to problem solving (such as increasing redundancy) only serve to increase the complexity of the system, thus increasing the likelihood for accidents and are generally not seen to be effective.

The figure shows that Chemical plants occupy quadrant 2 i.e. they exhibit a high degree of complexity and are tightly coupled. I would agree with the former classification and not the later. There are "buffers" designed into the system to cope with unexpected failures and as such they are not as tightly coupled as a first look would suggest. That said the recommendation to decentralize authority is particularly relevant. Review of some accidents has identified the lack of decision making capability as a key contributing factor. In others, personnel were nominally given the authority in theory but could not use it in practice. The Macando well blowout is a case in point. Consider the following conversation between personnel regarding the authority to trigger a critical safety device known as the EDS (Emergency Disconnect Switch) that could have mitigated the disaster if triggered early (taken from the presidential report into the disaster (National Commission, 2010)).

Steve Bertone was still at his station on the bridge and he noticed Christopher Pleasant, one of the subsea engineers, standing next to the panel with the emergency disconnect switch (EDS) to the blowout preventer.

Bertone hollered to Pleasant: "Have you EDSed?"

Pleasant replied he needed permission. Bertone asked Winslow was it okay and Winslow said yes.

*Somebody on the bridge yelled, "**He cannot EDS without the OIM's [offshore installation manager's] approval.**"*

Harrell, still dazed, somewhat blinded and deafened, had also made it to the bridge, as had

BP's Vidrine. With the rig still "latched" to the Macondo well, Harrell was in charge.

Bertone yelled, "Can we EDS?" and Harrell yelled back, "Yes, EDS, EDS."

The text in bold italics clearly suggests that a centralized system in which decisions could not be made without the authority of the rig manager was being used. The ability to directly make such time critical decisions to avert a visibly developing disaster cannot be overstated.

There are of course challenges with this model. The extent to which it can be applied universally (i.e. to all technologies) is not so clear. Also, determining the degree of complexity and coupling associated involves some degree of subjectivity (for some this would be described as arbitrariness) which creates certain methodological challenges in its application. One can readily expect variances in assessments done by various parties. Finally, it is questionable the extent to which the accident potential of high risk systems can be fully characterized and appreciated by just two dimensions.

Nevertheless, this theoretical framework—based on a systems approach— is useful to understanding why accidents happen and can help in identifying methods by which they can be reduced. It offers a platform by which the potential susceptibility of various systems to disaster can be compared on a rational basis. It also helps answer the question as to whether certain institutional designs or architecture are better for accident prevention than others.

FIGURE 9.1
Interaction/Coupling Chart

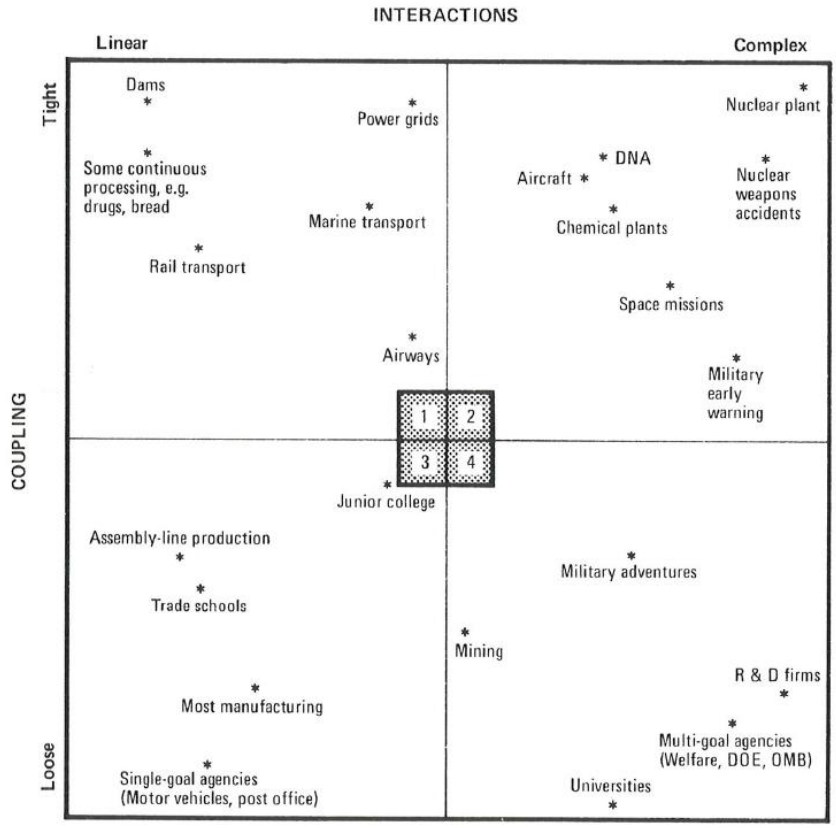

Figure 1: Classification of technologies based on degree of coupling/complexity (Reproduced from Perrow (1984)).

2.3 High Reliability Theory

High reliability organizations (HRO's) are defined as organizations that have a near perfect safety record despite managing high risk activities e.g. nuclear power or nuclear submarines. As a consequence, considerable effort has and continues to be placed on understanding the defining characteristics of such outfits. What is peculiar to them? What habits and cultures do they embody and what role do these play in helping to ensure high safety standards?

In research on HRO's, Weick and Sutcliff (2001) observe a dominant characteristic of HRO's is a "collective mindfulness of danger"; a characteristic that is central to managing the risk within their respective organizations. HRO's are constantly on the look-out for deviations, abnormalities and inconsistencies recognising that these may be early warning signs of a larger catastrophe in the making. This state of heightened risk awareness is central to risk minimization in HRO's. The word "collective" here is particularly key as it points to the fact that responsibility is a shared goal between all individuals. Risk (and blame) is elevated from the cradle of the individual to the entire organization. Thus risk is effectively internalized within the organization; a position that creates a more balanced approach in that the creators of risk are wholly accountable—both in word and in deed—for managing it. In this light, responsibility within the organization can be maintained by developing a collective sense of accountability between all individuals in the organization.

This "collective mindfulness" influences the way HRO's are organized. Weick and Sutcliff (2001) also note that they (i.e. HRO's) "organize themselves in such a way that they are better able to notice the unexpected in the making and halt its development".

Decentralized authority is a key defining factor of HRO's (Roberts, 1990). This has also been called a "flexible culture" or "deference to expertise". In high alert situations, decision making capability moves to the most knowledgeable and experienced persons even if they are at lower levels in the hierarchy. In such organizations, everyone is empowered to take

decisions in certain circumstances. This trait shows good agreement with the recommendations from Normal Accident theory on how decision making within high risk systems should organized.

Learning from past mistakes is also a key characteristic. Various authors have argued that failure to learn from past mistakes is at the core of most disasters (Kletz, 1993; Horlick-Jones; 1991). Blockley (1996) argues that "the best way of avoiding the disasters of the future is to create a…learning organization…" . Research into HRO's suggest that complete transparency from individuals is required for thorough error identification which in turn is critical for effective risk management and central to averting major accidents' (LaPorte, 1982; Roberts, 1989; Roberts & Gargano, 1989; Weick, 1989; Sagan, 1993).Table 2 lists the key characteristics and their significance.

Table 2: Summary of Key Characteristics of HRO's and their significance

Characteristic	Significance
High priority placed on safety by leaders	Leadership (setting the agenda and emphasis) has been identified repeatedly as key to ensuring safety objectives are met.
Decentralized authority	Those best placed to make decisions related to ensuring safety are empowered to do without fear of reprisal. This is especially important where decisions can have significant economic impact.
Ability to learn from past mistakes	Key to avoiding reoccurrences of unwanted events
Transparency	A key requirement for the ability to learn.
Collective mindfulness of danger	The core trait that animates all actions undertaken by the organization. The word "collective" indicates that it is system wide responsibility as opposed to focus on particular individuals.
Significance defence in Depth/Redundancy (also referred to as a Commitment to resilience)	Increases system resilience and thus the ability to compensate for failures. However, it adds complexity and increases opacity.
Just culture	This is key for learning from past mistakes. Systems that encourage reporting without fear of reprisal are employed in HRO's.
Preoccupation with failure	A robust understanding of the nature the diverse failure modes that obtain, particularly at their incipient stages is key to ensuring they can be prevented, detected or managed effectively.

Other notable traits of HRO's that have been observed include: Preoccupation with failure, Reluctance to simplify interpretations, Sensitivity to operations, Deference to expertise and Mindful leadership. Similar to the themes raised in Table 1, the traits listed here though considered independently, tend not to be unique but are rather closely interrelated and connected to other themes. For example, "just culture" clearly influences the "ability to learn from past mistakes".

2.4 Latent and Active failures

This is based on the work by James Reason, whose core argument is that "humans are not infallible" and as a result, the important consideration is "why the system in which the individual operates failed in managing these errors?". (Reason, 1990). In this theory, two types of errors – "Active" and "Latent" (synonymous with "immediate" and "root"). The former are those errors whose effects are felt almost immediately (e.g. crossing a red light). Whilst the latter group are comprise of errors with adverse consequences that lie dormant within a system until revealed by other factors that combine to cause failure. Reason argues that latent errors pose the greatest threat to safety.

A "resident pathogen metaphor" is outlined as a useful way of understanding the nature of latent errors. Basically, latent failures can be seen as resident pathogens in a living organism which on the whole are largely harmless and well contained but when combined with external trigger factors and under the right conditions will result in system vulnerability and bring about disease (or a major accident in the case of organizational disasters).

There are diverse sources of systemic latent error. Increasing automation (which reduces the role of the human and makes accident more sensitive to design issues); system complexity and thus opacity (reduces the ability to intervene) and redundancy (which can unwittingly conceal accumulating problems as noted by Rasmussen in the reactor safety study report (NRC, 1975) are a few readily identifiable examples.

This theory currently underpins a range of accident reporting and investigation systems such as HFACS (Human Factors Analysis and Classification System), Tripod, ADAMS (Aircraft Dispatch and Maintenance Safety) and SOL (Safety through Organizational Learning).

2.5 Sociotechnical systems

Systems that incorporate both human (i.e. social) and technical components have come to be known as "sociotechnical" systems. The heavily interdependent nature of the people (and their social organization and environment) and technology (how it is created, adopted and used) is a central consideration in the theory of such systems. As Blockley (1996) notes "People and technology interact with each other and, over a period, change each other in complex and often unforeseen ways". Organizations and institutions with responsibility for managing and preventing major hazards fall under this umbrella. Hence, it is self-evident that the theory of such systems is particularly relevant to understanding accident causation in this sphere. The theory places emphasis on the multi-level causality of accidents (to match the various levels of the system) and allows for a clear distinction between direct and underlying causes of an accident.

System failures are assessed using the traditional comparison of the actual system in practice versus what is called the ideal system. This is referred to as the "systems failure" method (Fortune and Peters, 1995). Analysis of the disasters (or accidents) in sociotechnical systems using this approach have demonstrated that they occur when human, organizational and technical systems breakdown in concert (Richardson, 1994). Shrivastava et al (1988) make a similar point but in a more general way. They note "contextual or environmental variables set up the preconditions for accidents…". System failures are also strongly associated with significant economic costs and large scale social impact.

The typically identified factors include:

- Lack of appreciation for the significance of a hazard (Hopkins, 2000)
- Poor institutional design (at the system level or with subsystems)
- Communication issues/barriers
- Internal conflict

A key challenge here is that what constitutes a system and the levels within it can be defined in various ways. This can have a significant impact on any analysis as the interaction potential for levels within a system is significantly influenced by their structural definition and relative proximity.

3. Conclusion

Five non-technical perspectives on accident causation have been outlined and reviewed in this paper. They are: Disaster/Accident Incubation Theory, Normal Accident Theory (NAT), High Reliability Theory (HRT), Latent and Active Failures and Sociotechnical Systems.

Although the starting points for each of the aforementioned theories differ, there are clear parallels in the messages they are the trying to convey. At their core, they challenge the "easy" explanation of operator error/equipment failure and shift emphasis to system level issues and beyond. They represent a clear paradigm shift in the understanding of accident causality. There is also a clear *shift to* and *emphasis on* systemic thinking.

What appear to be incongruities between the theories discussed can be seen. For example, HRT emphasize the importance of redundancy and defence in-depth; whilst this is eschewed by Normal Accident Theory on the basis that it adds complexity and increases opacity. The key lesson is to recognize that interventions are not "risk free" and that any associated risks need to be identified and mitigated for. Clearly some redundancy is desirable but the fact that it can increase complexity and opacity needs to be accounted for. "Mere redundancy" (i.e. redundancy without the handicaps) should be the goal.

These new ways/perspectives of looking at major accidents are significant. They demonstrate that accidents are multi-faceted and that it is important to look at the various lenses/underlying factors individually as well as how they interact with each other. The socio-technical view of a hazard are propounded by Blockey (1996) is instrumental in this regard. They also suggest that the orthodox engineering technical view needs to be broadened to embrace these new approaches. A good starting point would be to expand the curriculum in universities. The overall message that emerges is that there is a need to take a granular and holistic view on every aspect of a high risk system – both within and without – to understand what factors can play a role in facilitating a disaster.

Finally, there is a danger that by focusing on broader issues these theories relegate the role of the "front line" in disaster prevention to the margins such that they are seen as less important. The reality is that both dimensions are equally important. The front line is simply another level within the system and the hazards visible at this level should be identified controlled here. However, there will be hazards that are not visible or controllable at this level (perhaps due to lack of the requisite knowledge or other factor). Such matters are clearly the purview of management.

4. References

Blockley, D.I (1996) Hazard Engineering. In Hood, C. and Jones, D.K.C. (eds) 1996. Accident and Design: Contemporary debates in risk management. London: UCL-Press

Comisión Especial Independiente (2007). Recomendaciones De La Comisión Especial Independiente, Contingencia Usumacinta – KAB 101.

Fortune, J and Peters, G. (1995). Learning From Failure – The Systems Approach, J. Wiley, London, 1995.

Hopkins, A. (2000). Lessons from Longford. Sydney: CCH.

Horlick-Jones, T., J.Fortune, G.Peters (1991). Measuring disaster trends part two: statistics and underlying processes. Disaster Management, 4 (1), 41–8.

Horlick-Jones, T (1996) The problem of Blame. In Hood, C. and Jones, D.K.C. (eds) 1996. Accident and Design: Contemporary debates in risk management. London: UCL-Press.

Inquiry Commission P36 Accident (2001) Final Report, Rio de Janeiro, Brazil, June 2001.

Janis, I.L.(1971). Groupthink. Psychology Today (November), 335–43.

Kletz, T.A (1993). Lessons from disaster: how organizations have no memory and accidents recur. Rugby: IChemE.

LaPorte, T. (1982). On the design and management of nearly error-free organizational control systems. In Accident at Three Mile Island: the human dimensions, D.Sills (ed), 185–200. Boulder, Colorado: Westview Press.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2010) Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling (Report to the President). Available Online: http://www.oilspillcommission.gov/ [Accessed 10 February 2011].

NAE/NRC (2011) Macondo Well – Deepwater Horizon Blowout: Lessons for Offshore Drilling Safety, Committee for Analysis of Causes of the Deepwater Horizon Explosion, Fire and Oil Spill to identify Measures to prevent Similar Accidents to the Future; National Academy of Engineering and National Research Council.

Nuclear Regulatory Commission (NRC) (US) (1975), Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG 75/014).

Perrow, C. (1984). Normal accidents: living with high-risk technologies. New York: Basic books

Reason, J (1990) Human Error. Cambridge University Press: Cambridge.

Richardson, B (1994) Disaster Prevention and Management, 3, 61.

Roberts, K.H. (1989). New challenges in organizational research: high reliability organizations. Industrial Crisis Quarterly, 3 (2), 111–25.

Roberts, K.H. & G.Gargano (1989). Managing a high reliability organization: a case for interdependence. In Managing complexity in high technology organizations: systems and people M.A.Slinow & S.Mohrman (eds), 146–59. New York: Oxford University Press.

Roberts, K. (1990). Managing High Reliability Organizations. California Management Review. 32(4): 101-113.

Sagan, S. (1993). The limits of safety: organizations, accidents and nuclear weapons. rinceton, New Jersey: Princeton University Press.

Shrivastava, P. Mitroff, I. Miller, D and Migliani, A. (1988). 'Understanding Industrial Crises'. Journal of Management Studies, 25: 4, pp. 285 ff. (in Mars, G.and Weir, D. 2000. Risk Management Vol 1. Aldershot: Ashgate, pp. 181ff.)

Turner, B.A. (1978). Man-made disasters. London: Wykeham Press.

Turner, BA and Pidgeon, N (2003) Man-Made Disasters. this is also called 'disaster incubation theory'. See the review essay by J Rijpma, 'From deadlock to deadend: the normal accidents – high reliability debate revisited', Journal of Contingencies and Crisis Management 11, no 1 (2003): 37–45.

Vaughan, D (1996) The Challenger Launch Decision (Chicago: University of Chicago Press, 1996).

Verma, J.B. (2011), Mumbai High Incident and Regulatory Progress Since, Oil Industry Safety Directorate.

Weik, K. (1989). Mental models of high reliability systems. Industrial Crisis Quarterly, 3 (2), 127–42.

Weick, K and Sutcliff, K (2001). *Managing the unexpected: Assuring High Performance in an Age of Complexity*. Jossey-Bass, San Franscisco.