The barrier-based system for major accident prevention: a system dynamics analysis

Ian Hoffman* and Peter Wilkinson**

* Hoffman Corporate Consulting Pty Ltd

100 Anglesea Street, Bondi, New South Wales, 2026

Telephone: +61 4 3418 8239, Facsimile: +61 2 9387 5741

Email: ihoffman@hoffmancorporate.com

** Peter Wilkinson Risk Management Pty Ltd

Abstract

Only a few months apart, two offshore oilwell blowouts in different parts of the world resulted in controversy about the safety of offshore oil and gas drilling. Both led to formal enquiries. They were also eerily similar in their technical causes. The key difference between the two events, (the Montara blowout in the Timor Sea, Australia and the Deepwater Horizon incident in the US Gulf of Mexico) was one of consequence. By chance, the Australian incident had fewer immediate consequences; there was no loss of life and apparently less damage to the environment.

This paper applies systems thinking and system dynamics to explore the barrier-based system of major incident management, the so-called "Swiss cheese" model of Reason (1997). We highlight counterintuitive features inherent to the system. We find that the number of barriers alone does not determine the effectiveness of the safety management system. Proper monitoring and understanding are vital. We also examine the impact of management and reporting focus. These insights lead us to make specific recommendations on the design and implementation of the safety management systems used by the oil and gas industry as a key pillar of their incident prevention policies.

Keywords: Oil and gas, Safety, Safety Management Systems, Deepwater Horizon, Montara

Executive Summary

Only a few months apart, two offshore oilwell blowouts in different parts of the world resulted in controversy about the safety of offshore oil and gas drilling. Both led to formal enquiries. They were also eerily similar in their technical causes. The key difference between the two events, (the Montara blowout in the Timor Sea, Australia and the Deepwater Horizon incident in the US Gulf of Mexico) was one of consequence. By chance, the Australian incident had fewer immediate consequences; there was no loss of life and apparently less significant damage to the environment.

This paper examines some of the principles upon which the oil and gas industry manages offshore petroleum hazards from a system dynamics view to see if any additional insights

into why these incidents occur can be obtained. In particular, the authors assume that major oil companies genuinely desire to have a good safety performance. However, rare but disastrous major accident events continue to occur.

Can system dynamics offer some insights into this? We believe it can. In particular, we explore the barrier-based system of major incident management, the so-called "Swiss cheese" model of Reason (Reason 1997). In this context, "barriers" are defences or safeguards consciously introduced to prevent major incidents. The barriers typically comprise a combination of "hard" engineering barriers and "soft" barriers consisting of interactions between people and processes. "Hard" engineering barriers include designing pipe work to withstand the maximum pressure of the contained fluids and engineering systems such as devices to detect escaped gas or fires whereas "soft" barriers cover procedural controls such as permit to work systems.

Applying systems thinking and system dynamics we highlight some counterintuitive features that are inherent to the barrier-based system. We find that the number of barriers alone does not determine the effectiveness of the safety management system. Proper monitoring and understanding are vital. We also examine the impact of management and reporting focus. Finally, the insights of the analysis lead us to make some specific recommendations on the design and implementation of the safety management *systems* which the oil and gas industry uses as a key pillar of their incident prevention policies.

1. INTRODUCTION

The aim of the paper is to examine two recent major accident events from a system dynamics perspective to see if these insights can generate suggestions for improvement in the management systems currently in widespread use in the industry. The paper is based on the necessarily limited evidence available on the Deepwater Horizon disaster pending the publication of the Chemical Safety Board's investigation which we understand is likely to focus on the organizational causes of the disaster. (The Montara Commission of Inquiry only dealt with the organizational issues in a limited way). So our conclusions can only be regarded as preliminary.

The paper is organized as follows. The remainder of this section sets out some important definitions and assumptions. The next section defines and briefly discusses major accident events that are the focus of the paper. Section 3 considers the safety management systems in use in industry. The system dynamics model framework and the resulting insights are presented in Section 4. We present our conclusions and our recommendations in the final section.

There are some initial definitions and assumptions we should discuss. These include a definition of "*major accident events*" and a brief discussion on *safety management systems.* We also make an important assumption on the mental model many western oil and gas companies claim to use to help manage the risks of major accident events. Many companies (implicitly or explicitly) use the concept of "barriers" to prevent incidents more or less based on the "Swiss cheese model" articulated by James Reason (Reason 1997).

We acknowledge the important paper "Nobody Ever Gets Credit for Fixing Problems that Never Happened" (Repenning and Sterman 2001). In the context of performance improvement, this paper discusses some key system dynamics ideas. For example, the subtle,

yet powerful, results of unintended side-effects, using feedback loops to clarify the consequences of a short-term versus a long-term organizational focus and the impacts of dynamic and detail complexity. A collection of papers that deal with a system dynamics view of accidents are reviewed in Goh (Goh, Love and Lo 2010). In particular, Marais (Marais, Saleh and Leveson 2006) apply system archetypes to accident management systems.

It is striking, but not surprising, that our examination of these major accident events (MAEs) reveals many of the common elements of system behaviour also discussed in Repenning and Sterman. For example, our consideration of MAEs highlights a number of counter-intuitive effects in the prevention and management of MAEs. One effect is the role of insufficient reporting of failures in the defences or barriers to major incidents compared with the focus on minor incidents. Another effect is the complacency that can arise when an organization fails to properly grasp the complexity of MAEs and the measures need to prevent them. Finally the impact of a short-term organizational focus versus a long-term focus on the quality of an organization's risk management is noteworthy.

2. MAJOR ACCIDENT EVENTS, (MAES)

For the purposes of this paper we will describe incidents, such as the Montara blowout or the Deepwater Horizon disaster in the Gulf of Mexico as a "major accident event" or MAE. We have adopted the definition used by the International Association of Oil and Gas Producers for major incidents, (OGP Report No. 415, December 2008) which regard MAEs as:

> "***unplanned events with the potential to escalate causing multiple fatalities and serious asset damage***."

In the offshore oil and gas industry, these are typically caused by losses of containment of hazardous materials such as hydrocarbons, which can lead to fires and explosions. This was the case of the Montara and Deepwater Horizon incidents and the earlier Piper Alpha disaster in 1988 which resulted in the deaths of 167 people. MAEs can also be caused by loss of structural integrity or loss of stability in the marine environment as in the case of the sinking of the offshore production platform, the P36, near Brazil in 2000 or the Alexander Kielland disaster in the North Sea in the 1980s where 123 people died.

2.1 Common Characteristics of MAEs

It is presumed that MAEs come as a surprise to the senior management of those organizations to which they occur. The alternative is that they *did* know what was coming but were unable to take appropriate action to avert the MAE for some reason. We have found no evidence to sustain this in a review of the literature of MAEs. However, after these events, a common feature seems to be that there is evidence of individual warning signs which were either not recognized as symptoms of an impending MAE by senior managers or these warnings did not reach an appropriate level of management who could take the requisite action.

Dr Tony Barrell, formerly Chief Executive Officer of the UK Health and Safety Executive's Offshore Safety Division, who led the development of the regulatory response to the 1988 Piper Alpha oil field disaster in the North Sea, in which 167 men lost their lives has observed:

> *'...there is an awful sameness about these incidents...they are nearly always characterised by lack of forethought and lack of analysis and nearly always the*

problem comes down to poor management, it is not just due to one particular person not following a procedure or doing something wrong..'.(BBC TV Programme)

The similarities in these incidents always seem to include multiple failures in the "barriers" which exist to prevent a MAE occurring and the existence of warning signs which were not acted upon. Of particular interest is that these barriers that organizations put in place are *deliberately* erected with the intention of preventing incidents occurring. One would have thought that organisations would be particularly sensitive to gaps or failures in these barriers but this does not seem to be the case. Another characteristic of MAEs seems to include missed opportunities to act upon observed (or observable) deficiencies in these barriers.

3. SAFETY MANAGMENT SYSTEMS (SMS)

To provide an organizational framework to help manage these barriers, companies typically put in place a Safety management system. Such systems are regarded as an important feature of the countermeasures companies put in place to guard against those very rare but disastrous "accidents" that occur from time to time. Indeed safety management systems, (variously referred to as health, safety and environment management systems, Operations Integrity Management systems or more recently as Integrated Management Systems), are often specifically required by law such as in the Australian and UK offshore petroleum safety regulations. This move to develop and then mandate HSE Management Systems, (at least in some jurisdictions), grew out of some well-known disasters. The Exxon Valdez oil spill off Alaska in 1989 was probably the most well-known oil spill prior to the Deepwater Horizon incident in the Gulf of Mexico in 2010, (although there have been other major oil spills). Another major stimulus to the development of safety management systems occurred the year before the Exxon Valdez incident. The fire and explosions on the Piper Alpha platform in 1988 with the loss 167 lives led to major changes in the regulatory approach, (at least in the UK and some other countries such as Australia) including the requirement for "safety cases" a key constituent being a safety management *system*.

3.1 What is a system?

Authenticity Consulting, LLC in their Free Management Library online guide, (see http://www.managementhelp.org/systems/systems.htm), describe a system as:

"...an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs which together, accomplish the overall desired goal for the system. So a system is usually made up of many smaller systems, or subsystems. For example, an organization is made up of many administrative and management functions, products, services, groups and individuals. If one part of the system is changed, the nature of the overall system is often changed, as well -- by definition then, the system is systemic, meaning relating to, or affecting, the entire system. "

3.2 Are Safety Management Systems, Systems?

Just because something is called a system it does not mean it necessarily is. However, the early proponents of safety management systems in industry and government were drawing on (at least in part) on the quality management approaches then prevalent in industry which themselves used system language and structures including feedback loops. For example Lord

Cullen in his report into the Piper Alpha disaster, The Public Inquiry into the Piper Alpha Disaster, said, "I consider...[oil] operators should draw on principles of quality assurance similar to those contained in ...ISO 9000." He also said the SMS should set out:

- The safety objectives
- The system by which those objectives were to be achieved
- The performance standards to be met, and
- The means by which adherence to those standards was to be monitored.

These are the essential elements of a control system and are directly analogous to control systems used for example controlling an air conditioning system, although in this case applied to the management of safety. Lord Cullen did not make explicit the importance of the feedback loop but from the context of this part of the Inquiry Report this is implicit in the last dot point. Thus, we believe it is reasonable to say that the use of the word *system* by the advocates and administrators is an intentional reference to systems thinking and not accidental or loose use of the term. To test this further we examined a major company's SMS, the guidance provided by an industry association working globally and a respected government health and safety regulator, to see what they regard as being the essential elements of a safety management system. The results appear below in Table 1.

Table 1: *Comparison of International Association of Drilling Contractors, (IADC), Chevron and UK Health and Safety Executive Safety Management System Elements*

Management System Elements (IADC)	**Management System Process (Chevron)**	**UK Health and Safety Executive Guidance on Safety Management Systems**
+ Policies and Objectives + Organisation, Responsibilities and Resources + Standards and Procedures + Performance Monitoring + Management Review and Improvement	+ Purpose, Scope and Objectives + Procedures + Resources, Roles and Responsibilities + Measurement and Verification + Continual Improvement	+ Policy + Organising + Planning and Implementing + Measuring Performance + Audit + Review
IADC HSE Case Guidelines Part 2.0.1	Chevron Operational Excellence Management System (OEMS) 2007	HS(G)65 Successful Health and Safety Management, HSE Books, UK.

A feature of the English language is the large number of words which can be used to describe similar concepts. Although all these frameworks in Table 1 are expressed slightly differently, their origin in systems thinking is clear. Furthermore, the introductions to all of these documents make explicit that they are consciously using the word *system* in a similar manner to the definition offered above.

3.3 Safety Management System Assumptions

We conclude that the safety management systems in use do owe their origin to systems thinking and are designed with the intention of operating as a system. However, there are a

number of important but usually unstated, assumptions which underpin the concept of *safety management* systems, which include the notion that people are "rational actors" and that *appropriate* management system feedback is generated, is timely and is capable of being acted upon to correct the "error." As we will see later in our paper, it is far from clear that this is so in relation to MAEs. BP, Transocean and Atlas in the case of the Montara blowout all had safety management systems constructed on the system principles discussed above.

4. A SYSTEM DYNAMICS VIEW OF MAJOR ACCIDENT EVENTS

We adopt the approach that the typical safety regime, (following Reason) consists of a number of barriers erected to provide multiple layers of protection from actions and events that could cause major accident events. Accordingly, accidents occur in a context of the alignment of a sufficient number of broken barriers allowing the possibility of a "trajectory of accident opportunity" in conjunction with events or actions traversing that trajectory.

Thus the state (simplified here as either "Effective" or "Broken") of the barriers forms the basis of the organization's defences against accidents. However, it is crucial that the organization monitors the state of its barriers and takes action to maintain their effectiveness.

Thus we look at the dynamics of the barrier states and the interplay between the barriers and organization culture and behavior. We find that, contrary to the naïve approach that more barriers enhance risk management, sometimes "more is less". Beyond a certain threshold, additional barriers can detract from accident prevention and mitigation. An important implication of our analysis is that there may be an optimal number of barriers. We believe that each organization should examine its risk management and practice in the light of this finding to determine the optimal settings for the organization. We investigate this further in the sections that follow and draw some conclusions from our examination.

4.1 Effective barriers

Since we focus on the role of effective barriers in the prevention of MAEs, we begin by looking at a high-level system dynamics representation of the breakdown and repair of these barriers. This first part of this representation is shown in the diagram in figure 1 below.

The first variable in the diagram shows the number of effective barriers and that this number is reduced when barriers break down. This process is shown as the arrow labeled "Barrier Breakdown", which represents the rate at which the barriers become ineffective. In this context, a barrier is ineffective if it will not fully perform its intended role as part of the accident prevention system.

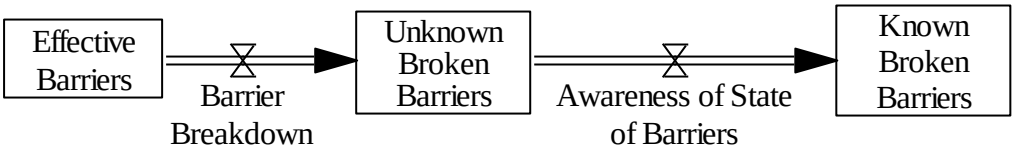
A large number of competing priorities and pressures that confront any organization and it must also absorb and understand a significant volume of information. Thus it is not uncommon for the organization to be initially unaware that the barrier has become ineffective. We illustrate this in the diagram by having the rate of barrier breakdowns add to the number of unknown broken barriers.

If the organization eventually realizes that the barrier has become ineffective, then the status of the broken barrier passes from unknown broken to known broken. The number of unknown broken barriers decreases and the number of known broken barriers increases. This is shown in the diagram where the two sets of broken barrier variables (unknown and known) are joined by the arrow called "Awareness of State of Barriers" connoting the rate at which the organization finds out about the broken barriers.

It should be pointed out that the process of awareness is far from automatic and guaranteed. Tragically, an organization may not become aware that one or more of the barriers are broken until it is too late to prevent a MAE and or until after a MAE has occurred.

In a later section, we discuss the better situation where the organization does become aware that the barrier is broken and the organization's response to this realization.

Figure 1: *Effective barriers.*



Given the extensive literature on oil and gas incidents where the investigation into the incident identifies the failure of barriers which where detectable *before* the incident, this area would seem *a priori* to be an important area for company managers to focus on and for safety management systems to emphasize. (See for example the Piper Alpha disaster, (1988), Longford, (1998), Bhopal, (1984) reported in "Incidents that define Process Safety" (Atherton and Gil 2008).

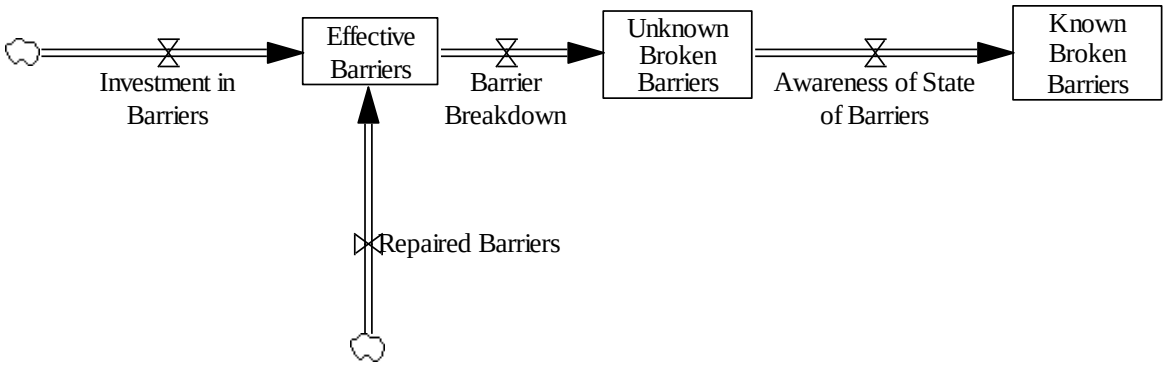
4.2 Adding effective barriers

The next stage in the system dynamics representation of the state of the barriers to accident prevention is shown in figure 2 below. When it is realized that the barriers are broken and an organization has decided to act on this information, there are a number of ways to supplement the effective barriers, including investing in new barriers and rectifying existing barriers that are currently ineffective.

These two ways, investment and repair, are shown in Figure 2 as the arrows "Investment in Barriers" and "Repaired Barriers", signifying the rate of investment in barriers and the rate of repair of barriers, respectively. These two rates contribute to the increase in the variable "Effective Barriers".

We note that organizational awareness of broken barriers is not synonymous with organizational action to address it. The organization may believe, rightly or wrongly, that the lack of this particular barrier will not compromise the overall efficacy of the safety management system. We deal with the specific issue of organizational complacency in a later section. We note that assessing the impact of the loss of a particular barrier can indeed be difficult, especially in light of the complexity of safety management systems and the dynamics of MAEs. For example, when the system, as a whole, is in a fairly stable state, the impact of a specific barrier breakdown may be minor, but when the system approaches a highly unstable region of operation, the failure of the same barrier may precipitate a MAE.

Figure 2: *Adding effective barriers*



For example, the knowledge and skills on the part of key individuals can constitute a barrier to a MAE. The knowledge of how to diagnose and then address the early warning signs of a possible blowout is clearly an important competence to have amongst one or more people on a drilling rig looking for hydrocarbons. However, the crew missed a number of crucial signs that they had problems in the well. (For a detailed account of these see Chapter 4 of the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp109 et seq).

4.3 Challenges in managing the barriers

Given the importance of effective barriers in preventing or mitigating the results of major accidents, it would seem to follow that an ever increasing number of effective barriers would equate to an improvement in accident risk management. Unfortunately, the system is more subtle.

In fact, we suggest that the introduction of additional barriers can increase the complexity of the safety management system, both the detail and dynamic complexity. For example, the interaction between the physical elements of the safety system and the culture and attitudes of the organization is complex. In addition, there is almost always a strong connection between the culture and attitudes found throughout the organization and the attitudes of the senior officers. Those attitudes are, in turn, affected by a number of factors including the respective historical experience of MAEs of the organization and its senior officers.

We have focused on several of these counterintuitive phenomena in the next two sections.

4.3.1 Complacency

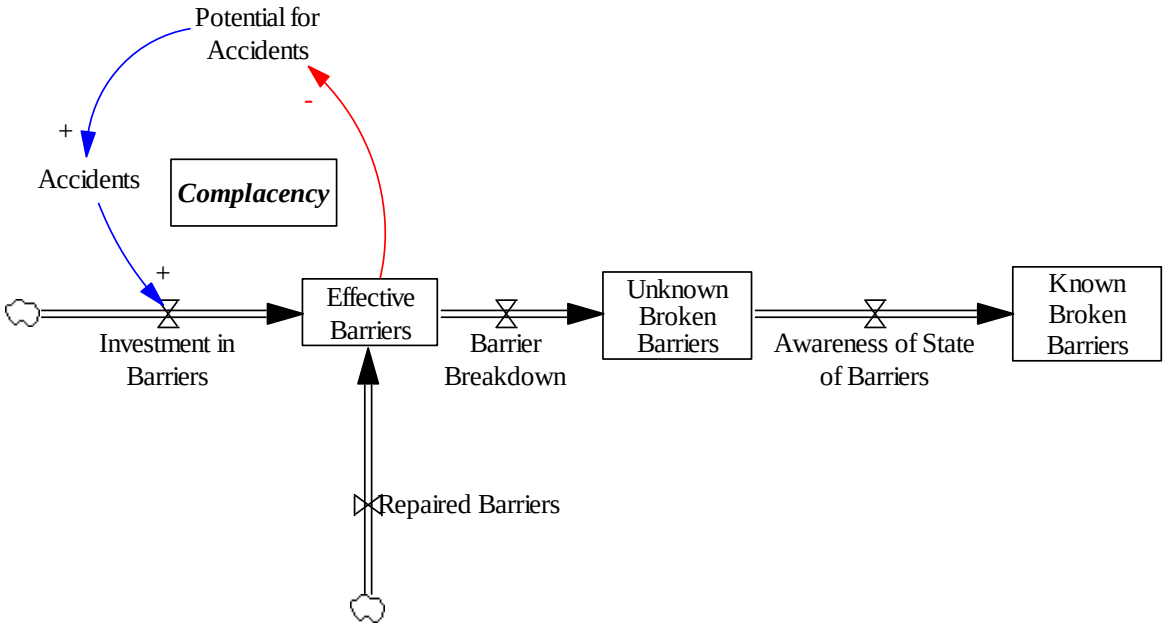
An example of the additional dynamic complexity that can attend these additional barriers is a feeling of complacency about the health of the safety management system (SMS) and the need to check and monitor the system's status. The extent of this complacency can range from a slight easing in the intensity of the risk management effort through to the firm belief that these extra barriers render the organization immune to the occurrence of MAEs. This belief tends to be accompanied by the assumptions that all the required actions are being taken and that there is no need to check on the actions and the overall health of the organization's safety management regime.

We have portrayed this complacency effect in the loop labeled "Complacency" in figure 3 below. The variable "Effective Barriers" is connected in a negative sense to the "Potential for

Accidents". An increase in the number of effective barriers leads to a decreased potential for accidents. In turn, this decreased potential should lead to a decreased number of accidents, so these two variables are connected in the positive sense. A decrease in the number of accidents tends to induce a feeling that these are "travelling OK" with safety and hence there is a decreased imperative to invest in additional barrier. Hence the variables "Accidents" and "Investment in Barriers" are connected in the positive sense.

We note that this "Complacency" loop is a balancing loop, implying the counterintuitive effect that an increase in the number of effective barriers can ultimately lead a decreased emphasis on further increasing the number of effective barriers.

Figure 3: *The Complacency loop*



The Montara blowout provides some support for this. In evidence given at the Montara Commission of Inquiry the Chief Operating Officer of the oil company concerned, PTTEP AA gave the following evidence in answers put to him by Counsel assisting the Inquiry:

> *Q. You seem to be saying that, to your knowledge or understanding, no one in PTT would have credited at this time that people involved in well management and well control might have succumbed to any sort of corner cutting or inattention to proper procedures by virtue of the desire to achieve time and cost savings.*
>
> *A. Mmm-hmm, yes.*
>
> *Q. I'm suggesting to you that the very fact that you are giving that evidence identifies a problem, namely, senior management did not properly recognise the plain fact of ordinary human nature and a known phenomenon, namely when you have lots of people applying themselves to achieving time and financial efficiencies, they can lose sight of the need to properly attend to processes.*

A. On the basis that there weren't systems in place to ensure that the barriers, et cetera were identified as being in place and verified and that, yes, I can accept that.

Q. So if you like, senior management almost seem to have approached the matter on the basis that everyone could be relied upon to do a perfect job without investing time and effort into really monitoring what was happening and ensuring that their expectations about people doing their job properly were fulfilled?

A. That certainly would be a way of viewing it. Again, I don't believe there was any conscious decision not to do things. They had an expectation that people would be fulfilling their roles. I agree with you that the documentation and recording of those critical elements would be a far more satisfactory way of ensuring that they have been achieved.

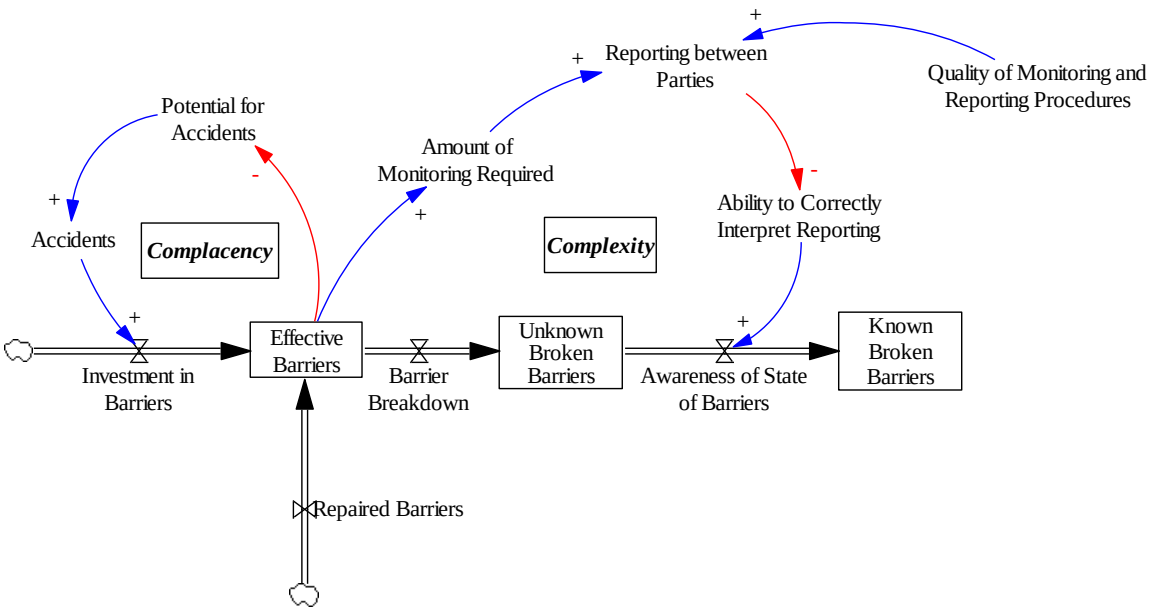
4.3.2 Increased Reporting burden

Another challenge with additional effective barriers is the increased burden of monitoring and reporting on the status of the greater number of barriers and correctly understanding the implications of the information in these reports. The increased volume of communication has aspects of detail complexity in the additional number of pieces of information that need be analysed and evaluated to see what action, if any, is required. But extra dynamic complexity has also been added to the system since the various effective barriers can interact with each other and the organization's risk culture.

The complexity added to the system by more barriers can adversely affect the organization's ability to monitor the barriers and comprehend the implications of changes to the states of the barriers. So, more can be less.

This is illustrated in the partial loop labeled "Complexity" in figure 4 below. Additional effective barriers lead to a greater need for monitoring of the state of the barriers, which, with strong reporting procedures, leads to more reporting on the barriers. But this "information overload" can hamper the organization's ability to properly interpret the information and understand its implications, which can ironically lead to a decreased awareness about the state of the barriers.

Figure 4: *The Complexity effect*



We examined the stated barriers or risk controls identified in the safety management system of a semi-submersible drilling rig, (similar to the Deepwater Horizon and using similar risk management techniques), to try to assess how complex they were. (We believe this rig is not atypical based on the personal experience of the author). We focused on those barriers intended to prevent a "well kick" which if not controlled could be the precursor to a well blowout. We chose these because of their direct relevance to the Montara and Deepwater Horizon incidents. Some ten "threats" or "causes" were identified and for each threat a number of specific barriers were identified. In total, some 45 barriers intended to prevent a well kick were listed. We believe this is intrinsically complex both from a system and dynamic perspective. This is particularly so when one considers that a "well Kick" was but one of the 20 hazards faced by this rig. All 20 threats or causes had preventive and mitigating barriers identified. So the actual complexity of the risk controls seems to be quite marked. From what we know of human error it seems inevitable there will be some errors in the execution of these barriers.

The published accounts of the Deepwater Horizon disaster describe significant problems in identifying a well kick and then implementing the appropriate controls in time, see for example Chapter 4 of The National Commission Report and "Deepwater Horizon's Final Hours" by David Barstow, David Rohde and Stephanie Saul, published by the New York Times, December 25, 2010.

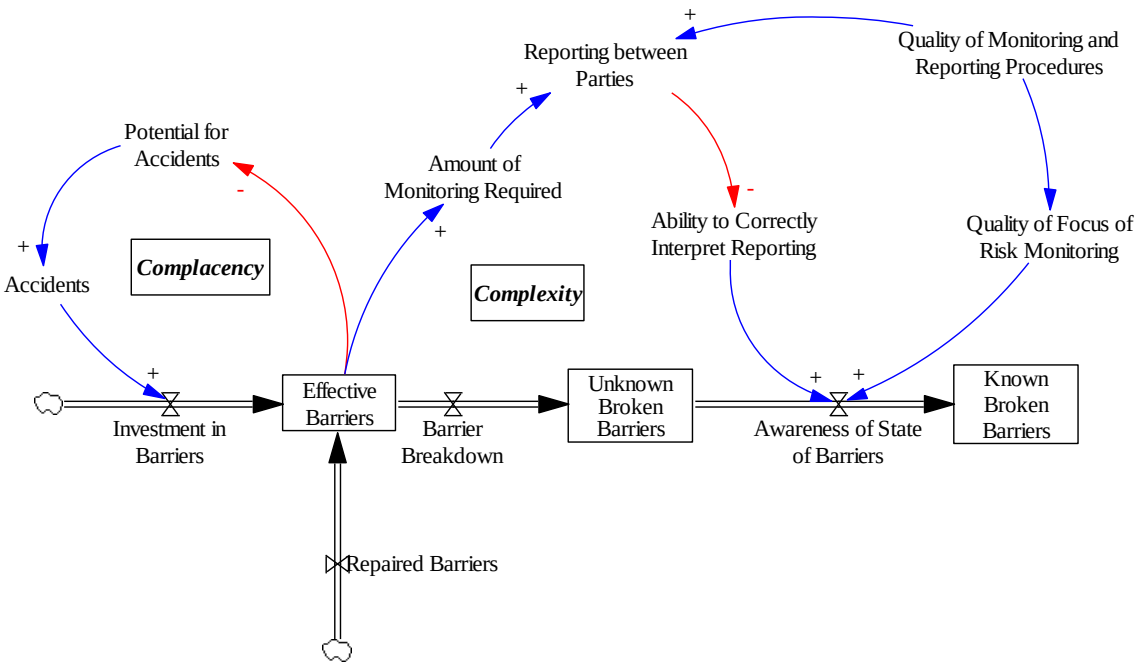
4.3.3 Management focus

Effective management of major accident events (MAEs) requires a depth of understanding on the part of the organization since, many times, the dynamics of the ultimate causes of MAEs are subtle and not apparent. One consequence of this need of the proper prospective is that an organization can also be lulled into a false sense of security about the state of its risk management by confining its focus to events such as lost time injuries (LTIs. These are often more apparent, easier to measure and easier to effectively address. While LTIs must also be attended to, an undue focus on personal safety can lead an organization to believe that it has

entirely fulfilled its responsibility to manage accident risk. This belief can have serious consequences and also tends to distract the organization from monitoring the state of the barriers to MAEs.

This is shown in Figure 5 below, where the better monitoring and reporting procedures improve the quality of focus of risk monitoring which correctly leads to a greater awareness on the part of the organization about the state of its barriers to MAEs. Conversely, an organization whose risk monitoring focus is confined to LTIs and other personal safety issues runs the real risk of remaining unaware of major holes in its defences to MAEs.

Figure 5: *Management focus*



There has been and continues to be a strong desire on the part of major corporations and hence senior executives to deliver an improving safety performance. This is entirely appropriate but seems to have biased prevention activities towards "personal" safety at the expense of MAEs. As quoted in (Repenning and Sterman 2001) "Nobody ever gets credit for fixing problems that never happened."

Andrew Hopkins in his paper "*Management Walk-Arounds: Lessons from the Gulf of Mexico Oil Well Blowout (unpublished – personal communication to the author)* discusses the mindset of the senior managers who were making a safety visit to the Deepwater Horizon *on the day* of the explosion and whilst control of the well was being lost.

> *"Their informal safety auditing activity was focused on occupational safety, not process safety. Hence they were highly focused on things that might cause injury to an individual – a slip hazard, a faulty harness, house keeping not up to scratch. They were not at all focused on major hazard risk and made no efforts to ascertain how well it was being managed (e.g. how effectively the reduced pressure test was being*

carried out) or whether people were following procedures that were designed to protect against major hazard risk (e.g. monitoring mud flows)"

Because of the focus on the reduction of the numbers of LTIs, understandably this leads to pressure on the part of the workforce to reduce incidents. Most of the actions taken are likely to have some benefit and contribute to reduced incident numbers. Examples include improved training or early injury management programs which by providing early effective treatment can prevent an injury becoming more chronic and "lost time injury" statistic. However, personnel can also perceive the pressure to reduce injuries in such a way that leads to incidents which should be reported, being hidden. A recent example from the UK railway industry illustrates this graphically. The body which regulates safety on the railway found that:

> *... significant under-reporting has taken place – and estimates that between 500 – 600 ... reportable accidents were not reported between 2005 and 2010. Some of the under-reporting relates to misinterpretation of the [regulatory] requirements,* ***but the majority is explained by staff and contractors choosing not to report accident events. This was caused by both real and perceived pressure, and in some cases fear****, felt by Network Rail staff and contractors if they reported accidents. The reason this was not identified by Network Rail itself was because it believed that the significant efforts it was making to improve safety, including investment in protective clothing, quantified targets and league tables, were driving the numbers of accidents down.*

In the case of Deepwater Horizon, the National Commission reports (p224) on a survey on safety management and culture carried out with Transocean and on four of its rigs including the Deepwater Horizon. The Commission quotes the report as finding the Deepwater Horizon "relatively strong in many of the core aspects of safety management." But it also reports that 46% of crew members surveyed felt that some of the workforce feared reprisals for reporting unsafe situations.

The authors speculate that paradoxically, to improve the ultimate safety performance of an organization may require, at least in the short term, a campaign to **increase** the reporting of incidents. In this way senior managers might be more aware of the true level of incidents (such as near misses or weakened barriers). After all it is difficult to manage what you do not know about.

4.4. Addressing ineffective barriers

As mentioned previously, an organization can move to restore the effectiveness of its SMS by repairing broken barriers or investing in additional barriers. However, this can only occur if the organization knows which barriers are broken, resolves to take the required action and follows through on that resolution. Thus, rectifying ineffective barriers requires awareness of the health of the SMS and the strength of organizational culture and risk management to address any issues.

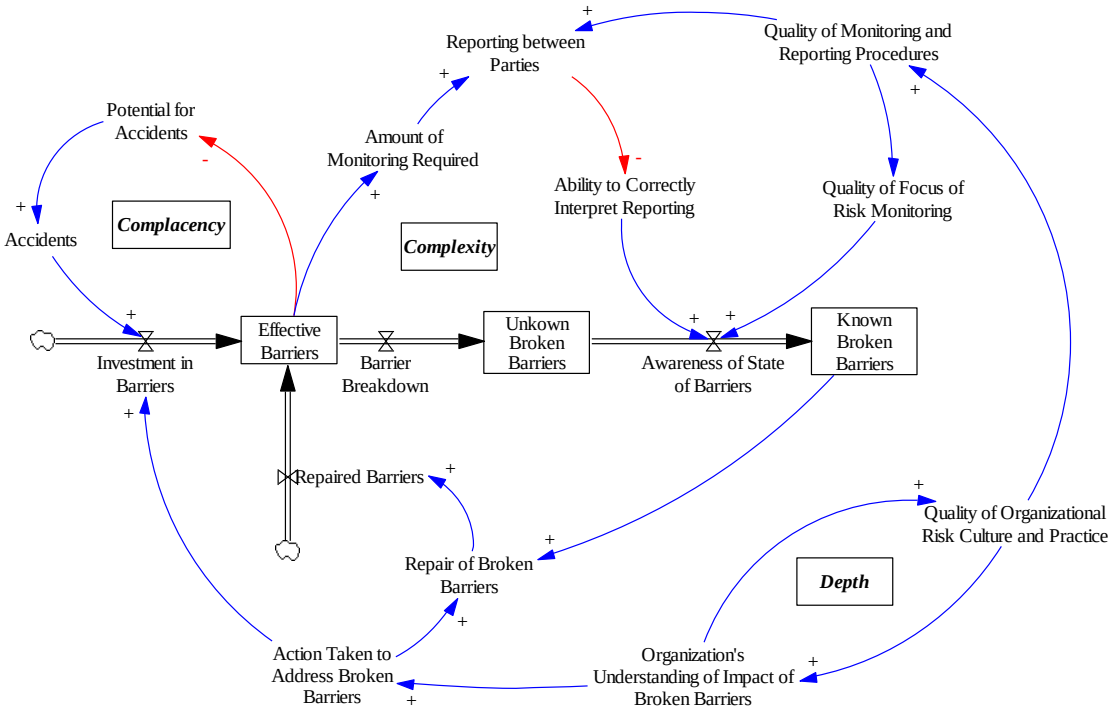
Investing the necessary time, resources and attention to restore the SMS typically presents a challenge since organizations must balance competing claims on these investments. On one hand, there are issues of operational and financial performance. These issues often have a short-term focus (e.g. regular reporting of project deliverables and quarterly financial reporting) and are more apparent. Also, the operational or financial improvement program (cause) and the results (effects) are frequently close in time and space.

In contrast, issues with the SMS are frequently subtle, insidious, long-term and largely hidden from view. In addition, we have suggested that the SMS is complex and have highlighted some issues with them that are likewise complex. Consequently, the achievements for investment in operational and financial issues are often easier to measure, demonstrate, communicate and explain than the corresponding results of investment in the SMS. Thus, the short-term needs are often met at the expense of the investment in the long-term matters of safety. Thus strong organizational culture and risk management combined with sound organizational perspective is needed to maintain the SMS.

This view of the role and impact of barriers in accident prevention is supplemented with the links related to the repair of broken barriers and investment in additional barriers, as shown in Figure 6. The stimuli for action come from two main sources. The first is the organizational awareness of the state of the barriers. But this knowledge is often not enough to trigger the organization to take the necessary action to rectify or supplement the barriers. A crucial additional ingredient is the quality of the organization's risk culture and practice, which causes the organization to better understand the impact of the state of the barriers and the requirement to take action.

The system shown in figure 6 below incorporates these points. We note several aspects of the diagram. First, the variable "Action Taken to Address Broken Barriers" is impacted by the variable "Organization's Understanding of Impact of Broken" indicating that awareness of a breach in the SMS must be accompanied by understanding to precipitate the repairs or investment in new barriers. Second, the reinforcing loop between the organizational understanding of its SMS and the quality of its risk culture and practice illustrates that the culture has the capacity to give rise to a vicious or virtuous circle. Third, the "Complexity" loop is now complete. This can be seen tracing a path starting with the variable "Effective Barriers" then around the part labeled "Complexity" to "Awareness of State of Barriers", "Known Broken Barriers", "Repair of Broken Barriers", "Repaired Barriers" and back to "Effective Barriers". Fourth, the "Complexity" loop it is a balancing loop. Hence the added complexity of additional barriers can ultimately detract from the health of the SMS.

Figure 6: *Addressing ineffective barriers*



A critical aspect of this is the ability of the organization to not just identify the weakened barriers but also to allow and actively encourage this information to percolate (upwards) to those who have the ability to deploy resources to repair the broken barriers. These are often likely to be more senior personnel. The implication of this is that to be effective, safety management systems must actively encourage (and welcome) the reporting of barrier failure. We believe this to be a difficult cultural trait to encourage but seems to be very important in the effective prevention of MAEs.

Indeed The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling quotes the earlier Chemical Safety Board's Report into the BP Texas City fire and explosion in 2005 which described "organizational causes embedded in the refinery's culture," including:

> *"BP Texas City lacked a reporting and learning culture. Reporting bad news was not encouraged and often Texas City managers did not effectively investigate incidents or take appropriate corrective action."* (National Commission Report p221).

This suggests companies need to take specific action to ensure reporting information about weakened or failed barriers is positively encouraged. There are also implications for regulators who assess safety management systems as part of their regulatory activities need to specifically focus on this aspect of organizational culture or climate.

5. CONCLUSIONS

Major oil and gas companies use safety management systems as an important tool to manage the barriers intended to prevent safety incidents. An implicit but important assumption is that for a safety management system to work effectively there must be feedback on the "health" or efficacy of the safety barriers.

The limited but persuasive evidence available so far from both the Montara blowout and the Deepwater Horizon disaster is that in both cases key "barriers" were not healthy "allowing" these incidents to occur. This is typical of other major accident events. In our paper we have focused on some of the problems identified in the official reports and looked at these from a system dynamics perspective. These problems include a focus on personal safety at the expense of MAEs, a failure to have effective feedback loops in safety management systems to determine accurately the "health" of barriers and how system complexity in terms of safety barriers can obscure effective safety management.

5.1 Feedback Loops (or inadequate monitoring of safety barriers)

We have seen the lengths offshore oil companies go to in identifying the "threats" to safety and the relevant defences or barriers. However, we have not seen equal attention being paid to *how* appropriate information on the health of the barriers is obtained, communicated and acted upon. These feedback loops are crucial to the effective working of a safety management system. In the case of the Montara, this much was admitted in evidence before the official Inquiry by the Chief Operations Officer. Our recommendation is that more effort is put into the design and implementation of these feedback loops so there is more and better information on the "health" of important barriers.

5.2 Encouragement of Feedback

As we explain in Section 4.3.3 we speculate that improvements in safety depend on understanding the weaknesses in barriers. In turn this means that there must be open and honest reporting of safety incidents. The evidence suggests that frontline workers may feel inhibited from reporting failures. Consequently, reporting needs to be encouraged and specifically rewarded.

5.3 A focus on personal safety as opposed to MAEs

In the case of BP, according to Hopkins (Hopkins 2011), senior officers of both Transocean and BP were focusing on safety during a visit to the rig on the day of the incident. Unfortunately, their focus was on "personal" or occupational safety rather than on MAEs. We have shown in figure 5 how this inappropriate focus can affect safety outcomes by focusing on personal safety at the expense of MAEs.

5.4 System Complexity

The apparent complexity of these safety management systems can be counterproductive. We have found that the techniques of risk assessment appear to be rigorously applied and large numbers of "barriers" identified. However, the communication flows required to keep track of the "health" of the barriers affects the ability of the organization to monitor their health and thus accurate and timely feedback may not occur. The inquiries into both the Montara and Deepwater Horizon incidents comment negatively about the quality of the communications. If the sheer number of barriers is required we believe much greater attention to identifying the communication protocols in relation to the barriers is likely to be needed.

This paper has looked at two recent MAEs through the lens of system dynamics. It is not a comprehensive study of MAEs. Inevitably therefore the evidential basis for our conclusions is limited. However, at the very least these incidents seem to confirm earlier work on the importance of ensuring companies have an appropriate focus on MAEs and not just personal safety. Additionally, we do not believe these incidents negate the value of safety management systems as a technique for managing the barriers or defences against MAEs. However, these incidents **do** suggest that more specific attention is warranted in the design and implementation of the feedback loops.

In particular, this requires specific attention to ensure the feedback mechanisms are able to provide accurate information in a timely manner so that any "error" or divergence from a healthy state on the part of a barrier is detected and acted upon. In safety management systems terminology these feedback loops are variously described as "monitoring," "audit" and "review." This would seem to suggest that safety management systems should give much greater prominence to these feedback loops. In summary, this equates to clear identification of these barriers, systems to monitor their "health" and reporting on their health to managers sufficiently senior to take corrective action. More detailed research using system dynamic principles is surely warranted.

References

Authenticity Consulting, LLC in their Free Management Library online guide, (see http://www.managementhelp.org/systems/systems.htm

John Atherton and Frederic Gil, *Incidents that define Process Safety* (Center for Chemical Process Safety: 2008). See for example the accounts of the Piper Alpha disaster, (1988),pp277 - 283; Longford, (1998), pp167 – 174; Bhopal, (1984), pp25 – 30.

BBC Education and Training DVD "Spiral to Disaster" (1997).Tony Barrell quoted in this training video.

David Barstow, David Rohde and Stephanie Saul "Deepwater Horizon's Final Hours," *New York Times*, December 25 2010.

Chevron Operational Excellence Management System (Private communication to the author).

William Douglas Cullen, *The Public Inquiry into the Piper Alpha Disaster* (Cmnd 1310, HMSO: 1990). See page 370 and in particular paragraph 21.56 et seq on the nature of safety management systems.

Yang Miang Goh, Peter Love and Daniel Lo, "System Dynamics Analysis of Organizational Accidents: A Review of Current Approaches" (paper presented at the 28th International Conference of the System Dynamics Society, Seoul, Korea, July 25-29, 2010).

Health and Safety Executive, (1997) "Successful Health and Safety Management" HS G 65, UK HSE. See Chapter 4, pp 48 et seq on "Risk Control Systems" and Chapter 5 pp 55 et seq about "Measuring Performance."

Anthony Hopkins, "Management Walk-Arounds: Lessons from the Gulf of Mexico Oil Well Blowout," (unpublished – personal communication to the author, 2011).

IADC HSE Case Guidelines, (2010) Issue 3.3, see for example the Introduction to Part 2. http://www.iadc.org/hsecase/index.html

Karen Marais, Joseph H. Saleh, and Nancy G. Leveson, "Archetypes for organizational safety", *Safety Science* 44 (2008) (7): 565-582.

Montara Commission of Inquiry, Evidence given on 9 April 2010 pages 1784/5, http://www.montarainquiry.gov.au/transcripts.html

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, (2011). http://www.oilspillcommission.gov/final-report. See Chapter 4 for an account of the causes.

Offshore Petroleum and Greenhouse Gas Storage Act 2010, No 10 of 2010 (Australia) and Offshore Installations (Safety Case) Regulations 2005.

OGP, International Association of Oil and Gas Producers (December 2008) Report No. 415, Asset Integrity – the key to managing major incident risks. (see page 4 for a definition of MAEs).

Rail Safety and Standards Board (UK) (25 January 2011) Press Release. http://www.rssb.co.uk/SiteCollectionDocuments/press/2011/RSSB%20RIDDOR%20Review%20Press%20Release.pdf

James Reason, *Managing the Risks of Organizational Accidents* (Hampshire: Ashgate, 1997). See page 9 for an account of the "swiss cheese model.".

Nelson Repenning and John D. Sterman, "Nobody Ever Gets Credit for Fixing Problems that Never Happened: Creating and Sustaining Process Improvement," *California Management Review* 43 (2001) (4): 64-88.