INTegrity MANAGEMENT, BLACK SWAnS AND FANtasy PlANNING: THE SAN BRUNo PIPELINE RUPTURE

GESTION DE L'INTEGRITE, CYGNES NOIRS ET PLANIFICATION FANTAISISTE: LA RUPTURE D'UN CANALISATION DE TRANSPORT A SAN BRUNO

Dr Jan Hayes
The Australian National University
School of Sociology
College of Arts and Social Sciences
Canberra ACT 0200
Australia
T +61 2 61252140, F +61 2 61252222, E jan.hayes@anu.edu.au

Abstract

In September 2010, eight members of the public were killed when a gas transmission pipeline ruptured at San Bruno, California. This paper describes the causes of this serious organisational failure. The rupture occurred when a longitudinal seam weld failed. The weld had been poorly made at the time the pipeline was fabricated and installed in 1956. The line had not been inspected or tested since that time. On that fateful day more than 50 years later, failure of pressure control at the upstream terminal led to a pressure rise in the line to close to the maximum allowable operating pressure. Control room operators chose to troubleshoot the pressure problems but not to isolate the downstream pipelines. After exposure to higher than normal pressure for approximately one hour, the line failed. The maximum allowable operating pressure for the pipeline that ruptured had been determined based on the highest operating pressure seen in the system in the previous five years, rather than by testing. Pressure testing requirements of the relevant standard had been grandfathered.

Whilst the details are specific to the case at hand, organisational lessons are valid for other organisations operating complex socio-technical systems. This analysis focuses on the organisational arrangements that led to such ineffective integrity management, in particular how the potential for an event such as the one that occurred was systematically ignored by the operating company for many years.

Résumé

Huit personnes ont été tuées en septembre 2010 quand une canalisation de transport de gaz naturel s’est rompue à San Bruno en Californie. Cet article décrit les causes de cette sérieuse défaillance organisationnelle. L’évènement a été provoqué par la rupture d’un cordon de soudure longitudinal. Le cordon de soudure n’a pas été bien réalisé au moment de la fabrication et de l’installation en 1956. Ensuite, la canalisation de transport n’a été ni inspectée, ni testée. Le jour de l’accident, 50 ans après, une élévation de la pression, trop proche de la pression maximale autorisée, s’est produite à cause d’une défaillance de contrôle de pression au terminal amont. Les opérateurs de la salle de commande ont choisi de résoudre les problèmes de surpression sans isoler les canalisations en aval. Après une exposition à une pression anormalement élevée pendant environ une heure, la canalisation a rompu. La pression manométrique maximale de service a été déterminée en utilisant les observations des cinq dernières années, plutôt qu’à partir d’essais. Les exigences de tests en pression de la norme applicable n’ont pas été mises en œuvre en raison de clause d’antériorité.

Bien que les détails soient spécifiques à l’affaire en question, les leçons organisationnelles s’appliquent à d’autres organisations exploitant des systèmes sociotechniques complexes. L’analyse se concentre sur les modalités d’organisation qui ont mené à telle gestione inefficace de l’intégrité, en particulier comment l’entreprise a ignoré la possibilité d’un événement de cette nature pendant de nombreuses années.

1. Introduction

On 9th September, 2010, a high pressure natural gas transmission pipeline operated by the Pacific Gas and Electric Company (PG&E) ruptured under the suburb of San Bruno, near San Francisco, California. The resultant fire burned for two days. Eight people died, and many others were injured. Thirty eight homes were destroyed and most buildings in the suburb were damaged.

Unfortunately, serious pipeline incidents are not unknown in the US. According to a US Senate Subcommittee hearing following the incident, there have been ‘an average of 42 serious gas pipeline incidents per year over the last decade, resulting in an average of 14 deaths, 16 injuries and over $432 million in property damages each year’. (United States Senate, 2011, pg 4). The pipeline sector in Europe has also suffered serious gas transmission pipeline failures including the rupture and explosion at Ghislenghien, Belgium in 2004 that caused 24 deaths and many serious injuries.

The actions of various people involved in integrity management and pipeline operations within PG&E, the choices they made and the organisational circumstances prevailing at the time are all addressed here. The analysis is critical of the actions of some people and it could therefore be read as saying that those people are responsible for the accident or even that we should blame them. Investigations aimed at prosecution often take this view, as the law seeks to look at actions in order to determine where blame should be allocated. This paper has a very different focus taking the view that, whilst individuals are able to exert professional judgement based on their experience, their actions are significantly determined by their organisational circumstances – the priorities, values and norms of their employer. These are the issues that are of primary interest for any analysis aimed at preventing future disasters.
We aim to describe this single case study in a way that allows broader lessons to be learned by those responsible for system integrity. In seeking to interpret the specific events in broader terms that can apply to any organisation, the work draws on the tradition of high reliability theory (Bourrier, 2011), which highlights the common organisational factors relevant to managing such activities despite differences in technology. Further, the use of case studies has a strong tradition in both social science (Flyvbjerg, 2001) and theories of how experienced people learn (Dreyfus & Dreyfus, 1986). By engaging with complex descriptions of case study material, people can see their own experience in a different light. In this way, the findings of the analysis are generalised. In the context of prevention of complex accidents, the ultimate aim is for decision makers to see the potential for failure in their own particular circumstances (and hence take a different course of action) as a result of their reflection on the events at San Bruno.

2. Method

This study is based on document analysis of investigation reports, transcripts of evidence and other primary source materials related to the three main investigations:

In this paper, we focus on the experts inside PG&E who were responsible for pipeline integrity management planning.

The factors contributing to the incident are identified based on an organisational view of accident causation, in particular the Swiss cheese model of James Reason (1997). In this view of accidents, workers are not seen as free agents, but as individuals whose actions are highly dependent on the organisational circumstances in which they work. Errors of individuals in the field are the result of workplace factors such as shift patterns, job design, task design etc. which, in turn, are linked to organisational factors such as structures, rewards and policies. These factors are also the source of latent errors which can create dormant problems in systems designed to act as defences.

The determination of the causes of the pipeline rupture has also drawn on Rasmussen’s work (Rasmussen and Svedung, 2000). His accident analysis method is similar to the well-known Six Sigma method (and other commercial root cause analysis processes) of asking ‘Why?’five times. Similarly to James Reason’s work, Rasmussen advocates starting with the final outcome and moving through physical events, processes and conditions that contributed, then to organisational factors and finally external factors. These two methods of analysis of the facts surrounding the incident provide a structure to the organisational and technical circumstances that lead to the individuals involved acting as they did. Both causes and recommendations operate at a system level.

3. Planning under conditions of uncertainty

The analysis draws on two main bodies of theory linked to planning under conditions of uncertainty. The first relates to the role of planning itself. Under conditions of high uncertainty, Clarke (1999) has highlighted the extent to which planning can become a symbolic, rather than instrumental, activity and it appears that this was the case at PG&E. When planning takes on a primarily symbolic role, the purpose of the plan becomes “asserting to others that the uncontrolled can be controlled.” (1999, p. 16). Clarke also points to the manner in which symbolic plans represent a fantasy – in the sense of a promise that will never be fulfilled – and are often couched in a special vocabulary which then shapes discussion.

Another concept useful in exploring how events such as San Bruno might be prevented is the metaphor of the black swan which has been gaining currency in risk and safety discussions (Taleb, 2007). A black swan is an event which is not expected and has an extreme impact. Most importantly, the concept of black swan is that such an event could not be predicted based on available knowledge. Seeing accidents as black swans potentially introduces a fatalistic view of accident causation or at least a sense of not being responsible - what Pate (Comelill2012) calls the ‘stuff happens’ view of risk analysis. On the other hand it is important to note the situated nature of the definition – it’s about current knowledge held by a specific individual or group. It does not seem to be pushing the metaphor too far to point out that black swans are in the eye of the beholder. For the Noongar people of southern Western Australia, black swans were, and still are, common. The metaphor highlights the critical role of knowledge and learning, specifically a diversity of views, experience and expertise, in risk management.

4. The Incident and its immediate causes

Just after 6pm on 9th September, 2010, a large fire erupted in the residential area of San Bruno, in northern California. Initial news reports speculated that the fire was the result of a plane crash (since the area is only five miles from San Francisco airport) but it soon became clear that the source of fuel was natural gas escaping from a ruptured high pressure gas transmission line which runs under the suburb. The pipeline is owned and operated by the Pacific Gas and Electric Company (PG&E). Supply of gas to the fire was isolated after 90 minutes, although the firefighting effort continued for two days. As a result of the fire, eight deaths and numerous injuries occurred, all amongst local residents. Thirty eight houses were destroyed and seventy were damaged. The rupture itself created a large crater and a section of pipe weighing well over 1000kg was thrown approximately 30m.

The section of pipeline that failed is known as line 132, section 180. The failure point was soon identified as a longitudinal seam weld that was poorly made when the line was installed in 1956. Apparently, no effective integrity testing was done before the line was put into service and it had not been tested or physically inspected in the intervening decades. PG&E’s integrity management system was based

---

This video shows an early television news bulletin.

http://www.youtube.com/watch?v=EZ6YbUmxVM&list=LPDs3tGxmbLMQ&index=1&feature=plcp
on flawed processes, poor record keeping and optimistic assumptions about the state of this pipeline (and others). The primary focus of the system was not on fault identification and repair, but on a database that contained inaccurate data, inappropriate algorithms and lacked any real-world connection.

In summary, shortcomings in the GIS (geographic information system) and associated procedures include:

- The database used as the basis for risk ranking included physical data that was optimistic and/or incorrect and there was no system of data checking in place.
- Algorithms for establishing inspection priorities were flawed both in concept and in execution.
- Regardless of the identified threat, higher risk segments were mostly subjected to ECDA inspections which determine pipeline integrity problems for external corrosion threats only.
- There was no system in place to review the performance of the integrity management system overall i.e. to compare high risk segments identified with inspections done and with actual leaks seen to determine if the system was effective and/or how it might be improved.
- The system produced only a prioritised list of segments based on threats to integrity. Whilst such a system could, in theory at least, be used to determine where funds should be spent to improve integrity, it makes no attempt to comment on overall risk acceptability and the total budget required.

On 9th September, field maintenance work was going on at the upstream Milpitas Terminal. This work was subject to a work clearance system and sign off by the operators in the SCADA (supervisory control and data acquisition) centre in San Francisco. The fieldwork interfered with the operation of the terminal inlet pressure control system which led to an increase in the pressure in line 132. This increase in pressure above normal operating levels apparently caused the faulty weld to fail. Nevertheless, there is no evidence that the pressure in the line rose to be above the designated maximum allowable operating pressure (MAOP). The regulatory requirements for establishing MAOP by testing were ‘grandfathered’ for old pipelines. Instead, the MAOP had been set at the maximum operational pressure to which the system had been exposed in the previous five years – in effect a service test. PG&E had used this method to establish and maintain the pipeline MAOP without the need for any integrity testing.

In summary, the pipeline was faulty when installed and had been in service for over fifty years without ever being subjected to any integrity testing or inspection.

5. The Company

The Pacific Gas and Electric Company (PG&E) operates 5557 miles of natural gas transmission pipelines, making the organisation the 16th largest gas transmission pipeline operator in the US (based on 2009 data). Almost one fifth of PG&E’s pipelines operate in a High Consequence Area (HCA)\(^2\). This is high when compared to other US operators. There are only two other companies in the top twenty with over 10% HCA miles and one of these (Sempra at 31.2%) is another Californian operator\(^3\). With pipelines running through urban areas as such a key part of the business, risk management is clearly a particularly important business consideration. The organisation had an enterprise-wide risk management plan which was reviewed by the Independent Review Panel who noted that a San Bruno-type event was anticipated as a risk that needed to be addressed. A PG&E document dating from July 2010 summarising the status of safety items in gas distribution described several of them as ‘weak’ but this was not the trigger for any urgent remedial action. (CPUC, 2011)

PG&E is a regulated entity. Whilst it aims to provide a financial return on investment for its parent company (PG&E Corporation), some key aspects of the financial environment differ from a typical company operating in a competitive market. Given that PG&E has a monopoly on retail energy supply in northern California, customer interests are represented by the California Public Utilities Commission (CPUC). Each year, PG&E presents to CPUC a budget including capital and operating expenditures, in order to justify the rate it wishes to charge consumers to achieve its mandated target rate of return. In this way, a regulated entity is prevented from making excessive profits by overcharging consumers in a monopoly market.

Critically, the organisation can also never fail in the way that an entirely profit-driven enterprise can. In 2001, due to problems with the California electricity market, PG&E had been forced to pay very high prices on the spot market without the ability to pass on the costs to customers. As a result the company filed for bankruptcy. The government could not allow the company that provides domestic gas and electricity supply to northern California to stop trading, so CPUC agreed a settlement which stabilised PG&E's finances and included, amongst other things, a guaranteed rate of return on equity.

As a result, PG&E has direct experience of financial difficulties and the extent to which the Californian public purse can be used to ensure that they continue to operate. On the other hand, the regulatory arrangements permit higher than mandated rates of return. Once the CPUC has approved PG&E’s annual budget, there is no further check that actual expenditure matches that which was estimated. If expenditure does not meet projected levels, there is no commensurate reduction in cost to consumers. This situation simply leads to a higher rate of return and higher profits to the listed parent company. This fact, combined with incentive payments to senior managers based on stock performance, seriously distorts management priorities in favour of cost cutting.

The accident has had a major impact on the corporate finances both in terms of penalties and a substantial program of pipeline testing activity, at least some of which should have been going on before the accident. PG&E reporting conflates these two aspects, reporting the cost of an intensive integrity testing program as a cost of the accident. To October 2012, PG&E had incurred $915 million in costs of ‘continuing work to validate safe pipeline operating pressures and conduct strength testing, as well as legal and other expenses in

\(^2\)HCA is defined in 49 CFR 192.903. Qualitatively, it means areas where a pipeline leak could impact many people.

\(^3\)This data is taken from page 29 of the IRP report and purports to be 2009 data. The PG&E web site (http://www.pge.com/about/company/profile/, accessed 15 October 2012), says that the company operates 6438 miles of gas transmission pipelines.
connection with the accident’. All of this ‘has been incurred at shareholders’ expense’⁴. In addition, PG&E accounts are holding an accrual in the range of $445 to $600 million for third party claims, some of which will be recoverable from insurance. PG&E are also reportedly holding a further $200 million in reserve for payment of fines⁵.

Few people come to work deliberately intending to do a poor job, especially those working in a hazardous industry such as a high pressure gas pipeline company. Nevertheless, there are many ways in which work done at PG&E did not achieve the desired outcomes and, in fact, contributed to catastrophe. PG&E’s operations included many of what Reason (1997) would call latent errors – faults in the risk defences that had been present for an extended period of time and came to light only when those defences were called upon to operate.

The next section addresses the extent to which issues of public safety related to the potential for pipeline rupture were systematically ignored. Across the organisation, PG&E failed to understand both the potential consequences to the public of dealing with high pressure gas. Instead, safety was understood to be about the company’s own workers. Public safety was addressed only indirectly by reference to compliance with standards and regulations for system integrity.

6. Managing low frequency/high consequence hazards

PG&E’s practices in managing the potential for a major hazard accident prior to the rupture provide some important lessons in how such processes can fail to achieve the desired result. Three areas are discussed further below. These are:

- Personnel generally had little regard for the potential consequences of their actions specifically, how their actions could contribute to causing a disaster,
- PG&E focused on worker safety, not public safety.
- Public safety was addressed as a matter of compliance with codes and standards.

6.1 Linking actions to consequences

No organisation that operates a system with the potential for disaster would accept a design where a single failure or error could lead to catastrophe. Organisations always intend that engineering and procedural risk controls combine to form layers of protection – that there is redundancy in the system. This approach is ubiquitous because we all know that, despite our best efforts, risk controls are not 100% reliable. The Swiss cheese model is the iconic representation of the idea that accidents happen when weaknesses in systems accumulate so that all controls fail – with catastrophic consequences.

The actions of individuals in widely differing roles contributed to the rupture of line 132. Engineers doing integrity management planning, maintenance people in the field and SCADA operators in the San Francisco centre all failed to link their actions to the potential for disaster and so let practices slide. Examples include:

- The people who planned the work going on at Milpitas Terminal completed work clearance documentation that was not fit for purpose. It provided little detail and did not acknowledge the potential impact of what they were doing i.e. the potential to disable key safety systems and cause the overpressure of downstream pipelines.
- The SCADA operators signed the clearance paperwork despite missing details, not seeking to verify the impact of the planned work on the operational equipment.
- The site safety briefings held at Milpitas Terminal on the day of the rupture (in accordance with work clearance procedures) focused only on workplace health and safety issues, not the potential public safety impacts of the tasks at hand.
- The SCADA operators had some indications that the pipelines downstream of the Milpitas Terminal were in very real danger of being over pressured for almost one hour prior to the rupture of line 132 and yet they took no action to isolate the downstream system to prevent this.
- The emergency response arrangements were impractical and untested as if no-one had ever thought such an event could really happen.
- Engineers and managers responsible for the integrity management system failed to understand that incorrect and/or missing data in the GIS influenced the scope of inspection work undertaken and hence had a direct impact on pipeline integrity.
- Engineers and managers put in place an inspection program using an inspection method that was cheap, but did not address the full range of possible threats to pipeline integrity.

No single poor decision or inappropriate action has the potential to cause a major disaster if the rest of the system defences are working. An effective safety culture where individuals understand their role in major accident prevention can withstand occasional errors but in this case there is a consistency to these choices made. Ignoring the potential consequences of one’s actions was, at PG&E, ‘the way we do things around here’ (Schein, 1992).

With an entrenched norm such as this, any organisation becomes simply an accident waiting to happen. All staff members with safety-critical roles must understand the consequences of their actions and be given the necessary organisational resources and support to carry out their roles effectively.

6.2 Focus on worker safety

As with many other companies, PG&E public statements in annual reports and the like placed a strong emphasis on safety. In 2008, an introductory letter to the annual report stated:

‘Nowhere has this [accelerating progress] been more critical than on safety. In 2008, we significantly improved benchmarks for lost workdays, OSHA recordables, and motor vehicle incidents…. Sadly, any glow associated with these results was dimmed by the loss of two employees and a contractor on the job. In the wake of these and other tragic accidents, we are now

⁵This has been frequently quoted in the press following this investor event, e.g. http://www.businessweek.com/news/2012-10-11/pg-and-e-should-pay-significant-fine-for-pipeline-explosion
implementing safety policies and practices that we believe are the most exacting ever at PG&E... our sights are set on a goal of zero injuries. This is, above all, the right thing for our people. But it is also right for the business — excellent safety results are a leading indicator of overall operational excellence. (PG&E 2008 annual report as quoted in (2012, pg 151))

The last sentence is misleading. Whilst an organisation with a poor workplace health and safety record is unlikely to have a good record for ‘operational excellence’, indicators of the potential for major accident (such as leak history) have a much more direct link to operational performance.

The failure to distinguish between personal safety and the potential for major accidents is unfortunately common. Major accident prevention (or process safety, as it is sometimes called) is about keeping the process under control or, more colloquially, keeping the hydrocarbons in the pipes, or otherwise contained. Failure to do so can lead to catastrophic consequences for workers and the public. Personal safety, on the other hand, concerns hazards that are not directly related to the process fluid itself, but which can injure or even kill workers, e.g. falling from a height whilst doing maintenance. PG&E focused on worker safety, but did not treat public safety in the same way. Despite the glowing words in the annual report quoted above, during 2008 a member of the public was killed and five other people were injured when a leaking PG&E gas distribution line led to an explosion in a house at Rancho Cordoba, California. PG&E technicians had been on site for four hours at the time of the explosion and one of the technicians was injured in the blast. PG&E were subsequently fined $38 million as a result of this event (2012, pg 151), although neither the event itself, nor the possible liability, is mentioned in the annual report.

Many organisations fall into this trap, but a well-known example is BP in relation to their drilling activity in the Gulf of Mexico before the Deepwater Horizon blowout (Hopkins, 2012). In one sense, those responsible for work on the Deepwater Horizon were very safety conscious. The managers on the rig at the time of the blowout were there partly to present an award to the crew for a very creditable seven years’ operation without a lost time injury. Based on this measure of safety, the rig was a standout performer within Transocean and BP. More broadly, BP overall claims a serious commitment to safety and before the accident reported that ‘since 1999, injury rates and spoils have reduced by 75%’ (National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011, pg 218). Hopkins’ analysis of the causes of the Deepwater Horizon blowout shows that BP had an admirable focus on personal hazards, but an entirely inadequate appreciation of process hazards.

As quoted above, PG&E saw worker safety as something that was good for business. They failed to understand their corporate responsibility – both for moral and business reasons - for preventing major hazard accidents.

6.3 Safety as compliance

In the absence of a real understanding of the potential for disaster, PG&E’s strategy for managing public safety was based simply on compliance with codes and standards.

With regards to integrity management at PG&E, RMP-01 states, ‘The Integrity Management Program (IMP) is a program established by PG&E to address the integrity management rules in 49 CFR Part 192 Subpart O.’ This is an important point – the premise was not minimisation of the potential for accidents, reduction of risk to ALARP or any other goal directly related to safety, but one of compliance with the regulation. The NTSB’s Investigator in Chief pointed out during the hearings into the rupture that ‘the PHMSA regulation or the CPUC’s regulations are minimum safety standards. Is there a PG&E policy … that says wherever possible for public safety, thou shalt exceed those standards?’ In response, PG&E’s Senior Vice President Engineering and Operations said ‘there’s not a standard that specifies thou shalt exceed, although there are cases where we do … it’s really an engineering judgment.’ (National Transportation Safety Board, 2011, pg 132 line 25 ff) Whilst it may be true that standards were sometimes exceeded in particular cases, the overall approach in written procedures and as found by NTSB regarding implementation was one of compliance.

Compliance with safety rules (in the form of regulations or internal company procedures) is clearly a key strategy in ensuring safe outcomes. The problem comes when compliance rules with standards are seen as an end in itself. Other research has highlighted the trap of framing safety only in terms of compliance (Hale & Borys, 2013a, 2013b). Grote (2014) has highlighted the potentially positive role of uncertainty and the need for flexible rules amongst other examples. Equating safety with compliance can lead to a short-term view of requirements and a ‘tick in the box’ mentality rather than the long-term perspective necessary to ensure long-term public safety. Perhaps most importantly in this case, removing the moral dimension from discussion of safety puts compliance issues on par with other organisational goals, such as cost and schedule. This is certainly something in evidence at PG&E.

7. Dealing with uncertainty

Managing the potential for major hazard accidents is difficult because such accidents are rare. Even given the problems at PG&E, the pipeline operated for more than fifty years before it failed. This long lead time highlights the level of redundancy in entrenched industry practices. Sometimes equipment can operate without incident for years, even with major flaws. On the other hand, the pipeline rupture also dramatically highlights how difficult it is to be sure that a system is safe. Overall track record is not necessarily a good predictor of future success. Maintaining an organisational focus on the potential for disaster in the face of little feedback is a challenge faced by industries such as nuclear power generation, offshore oil and gas exploration and production, aviation and similar. Put simply, we learn by experience, by trial and error, but this is not a strategy that is effective for preventing rare events i.e. it is not acceptable to wait for a major failure to learn that the integrity management system is not functioning as intended.

The GIS and associated procedures detailing integrity management algorithms applied to the PG&E network constitute a form of planning. Planning is a straightforward instrumental activity (a means to an end) in cases where uncertainty is low. Integty management is a very different case. For a complex network of facilities such as PG&E’s system, many things are not certain. Data for old pipelines may be missing. Not all lines have been tested or inspected so their condition is uncertain. More than that, sometimes data itself may be unreliable in ways that are not obvious so there are ‘known unknowns’ and ‘unknown unknowns’. Effective planning to achieve an important goal under these conditions is much more difficult.
Clarke’s work regarding fantasy planning in the face of such uncertainty explains both how and why the integrity management system at PG&E had taken on a symbolic, rather than functional role. We have seen that PG&E’s integrity management system was flawed in many ways and was not effectively performing the function for which it was originally intended. ‘Knowing’ about the system was grounded in elaborate algorithms and graphs purported to show risk was declining, and yet this analysis was only tenuously linked to the actual level of danger. This is not to suggest that in these circumstances, companies or individuals are deliberately fabricating this type of plan in order to deceive themselves or others but rather that, in the face of significant uncertainty, earnest attempts to plan can lose touch with reality. In the case of San Bruno, this included problems with records of physical data where dummy values had been used in the place of missing information for old pipelines. Over time this data came to be seen as an accurate record of reality. This is very similar to the organisational problem identified by Turner and Pidgeon(1997) as ‘disaster incubation’ - where organisational beliefs about control of hazards are at odds with actual events.

A key factor in maintaining this flawed view about the integrity of the network appears to lie in the extent to which the integrity management system was isolated from information about the actual state of the pipelines in the ground as revealed by the history of leaks. The NTSB report (2012, Table 2, pg 39) details eleven leaks or seam defects on line 132 over the period 1948 to 2011. In particular eight months after the accident, PG&E advised the NTSB that, in 1988, there had been a longitudinal seam failure on a section of line 132 approximately nine miles from the 2010 rupture location. This leak and other earlier problems with seam defects were not taken into account in integrity management planning because ‘PG&E stated that when it transitioned to its GIS in the late 1990s, only open (that is, unresolved) leak information was transferred. Closed leak information—such as the October 27, 1988, leak, which had been repaired—was not transferred to the GIS.’ (NTSB, 2012, pg 109-110) It is clear that the integrity management system was not linked to PG&E’s leak history. If such a link had been in place, it is likely that questions would have been raised about the usefulness of the system.

The lack of understanding of the importance of leak history in understanding system integrity was also highlighted in an early interview with the NTSB by the responsible PG&E manager. The Director of Integrity Management was asked about PG&E’s history of leaks and the identified causes. His repeated response was ‘there’s leaks and there’s repairs’. (NTSB Investigation Hearing, 2010, pg 36, line 22 ff) He and other PG&E staff members interviewed by NTSB have great difficulty understanding why the organisation should have done anything as a result of leaks other than repair each one. Trend analysis or formal feed back to the planning of integrity management do not seem to have been understood as critical activities to ensure that the integrity management system was effective. In addition to information about past leaks, there were other possible sources of information that PG&E could have used to improve integrity management, including:

- Base physical property data in the GIS. The NTSB found that ‘many of the pipe segments for which records had missing, assumed, or erroneous data had previously been exposed in connection with ECDA excavations as part of the integrity management program.’(NTSB report, page 108) In other words, corrections could have been made to some erroneous GIS data as a result of feedback from the inspection program, but this was not done.
- PG&E had in place a ‘self-assessment’ system which was supposed to check on the overall effectiveness of the inspection program. Primary documents such as audit reports are not in the public domain, but the NTSB described the system as ‘superficial’ and pointed out the very slow follow up e.g. two years between the December 2007 audit and the internal response.
- The general industry accident record (as quoted in Section 1) includes accidents, many of which have been investigated by the NTSB with detailed causal information released into the public domain. This could have been used by PG&E to undertake targeted reviews of their system to see if they were vulnerable to the problems identified elsewhere.

In fact, no efforts were made to use any of these sources of input to feedback to ground integrity management planning in the real world. Rather than effectively manage integrity, the planning function had become a system of symbolic value in being able to assert that risks are controlled. With this primary function, links to real world data, especially data that might provide a conflicting view are not seen as relevant.

The San Bruno rupture clearly came as a surprise to PG&E, even to the point of the control room personnel taking some time to realise that the loss of pressure in the pipeline and the huge fire at San Bruno were related. This raises questions about whether such rare events are fundamentally predictable. This issue has been discussed at some length in the safety literature in recent years using the concept of the black swan event in safety therefore raises fundamental questions about the degree to which these types of safety incidents are foreseeable. In the case of San Bruno, the incident was certainly not expected, extreme in impact and was not predicted by the integrity management system. But could it have been foreseen? It would be an overstatement to suggest that the failure of line 132 specifically could have been predicted but as described above there was evidence available if only PG&E had chosen to look to suggest that such a failure was possible or perhaps even likely given the weld problems identified over several decades. This event only defined prediction because the integrity management system was a ‘fantasy’. Those responsible for integrity management could not foresee problems because the model itself had taken on a life of its own and become for all intents and purposes the reality of what was being managed, rather than the physical system that it was originally intended to represent.

8. **Senior management at PG&E**

The primary evidence we have used to analyse PG&E’s actions in the lead up to the San Bruno rupture is mainly testimony from middle managers and field workers, plus company records, procedures and publications. Other aspects are drawn from the three published investigation reports. There is little evidence that comes directly from senior management of the company. Despite this, senior management views on safety and integrity management pervade our analysis. Models of safety culture and organisational accidents stress the importance of senior management attitudes due to the power that they hold over their staff both directly and indirectly. It is
because senior management as a group is so influential that we can draw some tentative conclusions about the attitudes and motivations of the PG&E Board and executive team and how they contributed to the catastrophic events that unfolded.

It is the role of leaders to direct the attention of the organisation to what is important and in this PG&E senior management have demonstrably failed. An analysis such as this does not seek to allocate blame to individuals (neither managers nor workers) but rather to seek explanation to prevent recurrence. There is little doubt that the PG&E Board and executive thought that they were doing the best for shareholders - and perhaps for themselves personally given the strong alignment between profit and their remuneration. Their remuneration incentive scheme was aligned with the organisational focus on cost minimisation and profit. It is not difficult to imagine that cutting costs on maintenance and inspection was seen as a question of efficiency – elimination of needless costs. The important implication here is that, if it was considered at all, senior management may have assumed that if the cuts went too deep that there would be warning signs in the form of small incidents in time for them to take action before any major failure occurred.

Trial and error learning such as this is a common, and often effective, strategy for management decision making, but this strategy is fraught with danger if applied to the potential for high consequence but low frequency accidents. Cost cutting in this environment requires that decision makers have (or have unfettered access to) expertise about the integrity of the system and that the impact of decisions can be carefully considered in advance. It appears that this was not the case at PG&E. We have no information on executive decision making processes but the IRP report (CPUC, 2011, pg 17) comments on the extent to which senior management positions in PG&E were held by individuals with qualifications in telecommunications, finance and law, rather than those with experience in gas engineering or high pressure gas transmission operations. The base data that leads to this comment is not available, but this supports the view that relevant experts, if they existed in the organisation, were not in key decision making roles. Absence of incidents is not of risk in this industry and the executive team apparently failed to understand this.

9. Summary and Conclusions

The manufacturing and/or construction faults that led to the catastrophic events in San Bruno had their origins more than five decades earlier. This very long lead time without any major incidents was taken by PG&E as feedback that public safety was well-managed. In fact, prevention of major hazard accidents needs special attention because they are so rare. Worker safety is important but public safety cannot be managed in the same way. Failure to understand the potential consequences of actions can be a literally fatal mistake.

Latent defects in any complex system are hard to find and so even the slightest evidence of problems should be valued. PG&E had warnings, particularly the problems in 1988, which might have given a clue that more investigation on the state of old pipelines was warranted, but these messages were not heeded. Leaks were repaired and then forgotten.

Instead, we have seen that the integrity management system was divorced from field data and took on a life of its own, with complex qualitative algorithms, graphs of risk reduction and other artefacts that had no grounding in reality. This is a warning that systems can take on a symbolic value that is detached from the originally intended use of the system, especially when divorced from any real world feedback. Risk management is always problematic when the model itself becomes reality.

10. Acknowledgements

This work was funded by the Energy Pipelines Cooperative Research Centre, supported through the Australian Government’s Cooperative Research Centres Program. The cash and in-kind support from the Australian Pipeline Industry Association Research and Standards Committee is gratefully acknowledged.

11. References