COULD CROSS-SECTOR PEER REVIEW HELP TO PREVENT MAJOR PROCESS INCIDENTS?

Gordon Sellers, Safety Management Consultant, Northwood, UK

As part of the project by IOSH Hazardous Industries Group to develop a cross-sector peer review process, we have reviewed the literature to identify the dominant causes of major process incidents. We have categorised the dominant causes of these major incidents to determine if cross-sector peer review might have been able to identify and correct the causes, had it been conducted at the correct time. Then we suggest enhancements that might be made to the technique to improve its effectiveness in identifying and correcting the causes.

RISING TO THE CHALLENGE FROM HSE

A paper at Hazards XXI [Sellers, Mason & Hemming, 2009] described how IOSH Hazardous Industries Group is rising to a challenge from HSE Chair Judith Hackitt to spread learning and good practice across all the major hazard industries, through a high level cross sector practical peer review process.

In response to this challenge, the Hazardous Industries Group of the Institution of Occupational Safety and Health (IOSH) set up a Working Party, which decided to lead cross-industry peer review on behalf of industry. A Stage 1 Pilot Study focussed on three control rooms in different safety-critical industries (nuclear, offshore gas storage and low pressure gas distribution) while a Stage 2 Pilot was of maintenance activities in another three different industries (gas processing and distribution, nuclear weapons, and submarine construction). The peer reviewers were all functional specialists – control room supervisors for the stage 1 study and maintenance managers for stage 2. For stage 1, the peer reviewers had a good understanding of 'what makes a good control room' but were able to bring a fresh perspective of best practices from their own industry sector; similarly for stage 2 with 'what makes a good maintenance operation'.

Safety in major hazard industries is often classified as:

- Occupational safety – the prevention of incidents that occur frequently and have relatively low consequences in that each incident affects only one person or a small number of people.
- Process safety – the prevention of high consequence incidents which occur only rarely.

The emphasis in peer review is to observe what is really happening, rather than to spend a great deal of time reviewing policies and procedures which tell us what is meant to happen. Therefore cross-sector peer review has a clear role in identifying the frequent situations and behaviours that may lead to occupational safety incidents. So the question has been asked, "Does cross-sector peer review have any role in identifying the infrequent situations and behaviours that may lead to process safety incidents?"

The purpose of this paper is to review the causes of major process incidents in order to identify which if any of them might realistically have been prevented by cross-sector peer review and, where appropriate, to suggest enhancements. But first we outline how cross-sector peer review works and how it has proved to be effective.

AN OVERVIEW OF CROSS-SECTOR PEER REVIEW

For peer review at a typical nuclear power station, a team of up to ten highly qualified staff from other nuclear companies will spend two to three weeks observing activities and physical conditions, conducting interviews and reviewing performance-related documentation, across all relevant activity areas in the power station.

Such a large scale peer review (up to 150 man days per site) was clearly far beyond the scope that we could hope to persuade organisations to invest their staff resources in our IOSH pilot project. So we chose the minimum possible scope to demonstrate whether peer review could be effective across different industry sectors; namely one working week focussing on the same activity area on each of three sites:

- Day 1 – training peer reviewers and planning the review
- Day 2 – peer review: site 1
- Day 3 – peer review: site 2
- Day 4 – peer review: site 3
- Day 5 – drafting observations and reporting back to Working Party

For the Stage 1 Pilot, we decided to focus on a control room on each site, as this is a clearly identifiable area which is central to all safety and production activities. Therefore we requested each of the three organisations to nominate as their peer reviewer a specialist from their selected control room, to work with a facilitator / team leader.

We thought carefully about the training and planning day, recognising that the peer reviewers had never done anything like this before; they were confident in their knowledge of their own control room but very apprehensive about their abilities to review a control room which was associated with very different plant equipment. So, after

brief introductions, we began by brainstorming "What are the key features for an excellent control room in a safety-critical organisation?" and we came up with about 30 of them. Then from various sources we selected 14 topics which covered all of our key features:

1. Leadership, accountability & commitment
2. Competence
3. Identifying and managing risk
4. Communication
5. Human factors & human performance
6. Security and access to control room
7. Work management
8. Plant status and configuration control
9. Managing maintenance activities
10. Emergency planning & response
11. Incident investigation & learning from experience
12. Deviations from normal conditions
13. Managing change
14. Continuous improvement

We assigned each team member three topics and asked them to draft a headline Principle for each topic and several associated criteria by which to judge whether that Principle was being met. For example:

Principle 2 – Competence
Personnel are selected and trained to have the required range of skills and knowledge, and these are regularly checked.

- Processes are in place for recruitment, appointment, promotion, succession planning and career development to ensure that personnel are capable to discharge their roles effectively, with a range of competences appropriate to the business.
- Training, supervision and guidance are provided as required for personnel roles and experience.
- Personnel performance is monitored and feedback provided.
- Control room personnel understand field operations, and vice versa.
- Personnel are coached to balance conflicting priorities, demonstrating flexibility and adaptability, and supporting requests from all parties.
- Personnel are encouraged to identify opportunities for enhanced performance, supported by objective analysis.
- Personnel are encouraged to take a lead role within their area of competence.

Note that the Principles and Criteria specify WHAT should be achieved but leave HOW it should be achieved to local arrangements.

This process by which the peer reviewers developed the Principles and Criteria, rather than having them handed to them, proved an important part of the training and increased the confidence of the team that they now knew what they should be looking for.

The training then emphasised that these were not checklists to be taken into the control rooms, but reference documents for use prior to the review, at intermediate points and as a reporting structure. The peer review is based on *observing activities*, supplemented by discussions with the staff being observed and by checking relevant documents such as handover logs.

Having discussed how the peer reviewer should best introduce him or herself to the person being observed, the core of the training was on how to write each observation as a 'fact', making clear whether it referred to an observed activity, an operator comment or an entry in a log, and the consequences. Facts are less likely to be disputed than opinions and assumptions and can be verified. This is based on a mantra developed by one of the authors for all his inspectors and assurance teams that "the advice we generate (good practice and opportunities to improve) is compelling because it is based in fact, it is targeted on business need and it is proportional to risk". This is exactly what Peer Review aims to do.

We documented both 'improvement opportunities' and outstanding 'best practices' to pass on to other organisations, but not normal good practices. To encourage openness, an important principle of peer review is that observation reports of improvement opportunities are confidential to the organisation being observed, with only anonymous summaries being published more widely.

We began each peer review with a kick off meeting with site management, to explain how we would carry out the review, and for them to give us a brief overview of the site and its activities. Then we spent the rest of the morning in the control room, with the peer reviewers singly or in pairs observing activities, holding discussions with the operators and team leader, and looking at control room displays and logs. When we broke for lunch, we each wrote up several of our observations and then discussed them as a team, with our advisor highlighting reports which were unclear or based on opinion not fact. Then we returned to the control room to observe the critical activity of shift handover, and continued our observations with the afternoon shift, taking care to gather data to back up some of the observations from the morning shift.

Towards the end of the afternoon, we met as a team to discuss the main 'facts' that we had observed – both best practices and improvement opportunities – and decided which to report back to site management at a short close-out meeting, at which we also agreed the next steps, namely within one month to provide management with a detailed report which the site's peer reviewer would then take a lead role in converting into an action plan. Good close-out meetings are an essential part of the peer review process and all led to site management agreeing that their peer reviewer would take a lead role in converting the report into an action plan for the site. Then we climbed into the minibus and headed off on a two- to four-hour journey to the next site.

On our final day, we spent the morning writing up further observations, reviewing them as a team, and preparing an overview report for the IOSH Working Party, covering both findings (anonymous of course) and our comments

on the peer review process itself. For the latter, we answered three questions:

1. Did the Peer Reviewers find it worthwhile?

- "Extremely worthwhile to give context to the journey that we're on at our site and to ensure we're going in the correct direction"
- "I've been most struck by the commonality of the problems we face, despite being in very different industries and different environments. It's put my issues into perspective."
- "We tend to be blinkered in our control room environment and it's allowed me to step outside my industry to see how others tackle similar issues to ourselves"
- "Normally I go into my control room to deal with a particular issue then I go out again. This has allowed me the time and given me the skills to look around objectively and critically. It has opened my eyes!"
- "It's given me the drive and focus to tackle our issues"
- "I've now got a network of like-minded experienced diverse colleagues who I can contact"

Conclusion: it was very worth while for peer reviewers, who are now driving action plans in their own organizations.

2. Was the Pilot Peer Review any better than audits?

- The peer review observed activities and so in a very short time it identified deviations from good practice, irrespective of what the procedures specified. But most audits check the paper trail – procedures and records.
- The peer reviewers were perceived as control room experts who were genuinely looking for best practices which they could share and helping the control room personnel to identify improvement opportunities, rather than as auditors who had never run a control room. As a result, control room personnel were very open with the team.
- The greatest potential benefit of the peer review is that the peer reviewers themselves are now very committed agents for change back in their own control rooms. The reviewers have already agreed to network with each other to share experiences of implementing change.

Conclusion: the Peer Review process offers significant demonstrated and potential advantages over auditing.

3. Could the Stage 1 pilot peer review have been performed any better?

- **Number and diversity of locations**: good – three gives sufficient differences without overloading the team, excellent diversity
- **Scope**: control rooms are central to operations, excellent choice for 1st pilot
- **Roles and experience of peers**: excellent – all had good hands-on experience (>5 years) and sufficient credibility to implement change
- **Planning schedule (1 day)**: should have had 1 day training + 1 day to prepare Principles & Expectations
- **Peer review schedule on each site (1 day)**: should be minimum 2 days – 1st day fact-finding in control room, 2nd day drafting report/clarifying facts/finalising site report/close out meeting
- **Consecutive reviews on three sites**: depending on geography, must allow for travel time
- **Report back schedule (1 day)**: would have been OK if there had been 2 days per site and adequate travelling time

The peer review process is one that fundamentally challenges a company's *status quo* and therefore requires senior operational leadership support if full value is to be achieved. Normally improvements are driven 'top down' while in peer review they come 'bottom up'. And, as we found with behavioural safety, it's not just enough to get the support of top management for a shopfloor behavioural safety team because middle management can then feel bypassed – Sir John Egan once described middle management as 'the reflective layer' which quietly bounces back all suggested changes whether they come from above or below. So the key is to get support from senior operational management *and* all the managers between them and the peer reviewers. Otherwise the peer review process will result in a comprehensive report of best practices and improvement opportunities – but no significant changes will result.

LITERATURE SOURCES AND METHODOLOGY TO ASSESS APPLICABILITY OF CROSS-SECTOR PEER REVIEW

There are numerous books and papers on major process incidents, but the ones that we selected for this review were:

- The latest edition of Trevor Kletz's definitive book 'What went wrong' [Kletz, 2009].
- The book 'Incidents that define process safety' by BP's John Atherton & Frederic Gil [Atherton & Gil, 2008].
- A paper 'Cultural and Organisational Factors Leading to Major Events' by Lorenzo van Wijk, Richard Taylor and John May from the University of Bristol [van Wijk, Taylor and May, 2008].
- The final report on the 2005 fire at Buncefield oil depot [Buncefield, 2008].
- BP's internal investigation into the very recent *Deepwater Horizon* incident [BP, 2010].

Of these, we found that the most useful for this review were:

- Atherton & Gil's book which described 42 major process incidents in some detail (two of the 'incidents' each consisted of three similar incidents, so 46 incidents were actually reviewed, but for our purposes we considered them as 42), analysing each one under:
  - Hazard Evaluation and Management;
  - Major Accident Potential;
  - Management of Change;
  - Engineering Authorities;

- Plant Integrity;
- Protective Systems;
- Competent Personnel and Procedures;
- Incident Investigation; and
- Emergency Response.

We noted that information on some incidents, especially the older ones, was scanty and much of the information focussed on 'hard' issues and ignored 'soft' issues such as leadership – as did BP's recent investigation report into the *Deepwater Horizon* incident [BP, 2010]. Therefore the data are incomplete but we consider that they are the best which are readily available.

- Van Wijk, Taylor & May's paper, which identified eight main areas of organisational and cultural findings in ten events which occurred across a wide variety of industries. These eight areas overlapped to some extent with those of Atherton & Gil, but we found them more useful for our purposes of determining issues that could be identified (and hence potentially corrected) before an incident occurred:
  - Leadership issues;
  - Operational attitudes and behaviours (operational 'culture');
  - The impact of the business environment (often commercial and budgetary pressures);
  - Oversight and scrutiny;
  - Competence and training (at all levels);
  - Risk assessment and risk management;
  - Organisational learning; and
  - Communication issues.

Therefore we decided to analyse the 42 'incidents' described by Atherton & Gil against the issues listed by van Wijk, Taylor & May. Our analysis, which was inevitably somewhat subjective, is presented in Attachment A and summarised below in Table 1. Not surprisingly we found far more issues than individual incidents, an average of 3.3 issues per incident; this is in line with the 'swiss cheese' model showing multiple layers of protection, any one of which would have prevented the occurrence of injury or damage had it been in place.

We concluded that the issues listed by van Wijk, Taylor & May can indeed be applied to the incidents described by Atherton & Gil, so it is essential that cross-sector peer review should be designed to look for evidence of as many as possible of them.

In addition to the issues listed above, we considered whether there was a lack of understanding by operations personnel of design limitations of equipment or of inherent hazards of the materials being handled. We also considered whether the incident was initiated at a time when the facility or equipment was deliberately being operated in a non-standard manner (such as startup, shutdown, testing, or unavailability of normally-available equipment); it is unlikely that a cross-sector peer review would happen to coincide with non-standard operations, but smart reviewers could ask searching questions about how people would respond to such situations. Our results were:

At first sight, this might imply that cross-sector peer review would be ineffective in identifying the causes of more than two thirds of major process incidents, either because the incidents occurred during non-standard operating conditions which are most unlikely to have been observed during a review, or because a significant factor was unawareness of design or hazard issues by the operations staff observed and interviewed by the reviewers. However remember that an average of 3.6 issues were identified in each incident; if we apply the 'Swiss Cheese Model' shown in Figure 1, we see that if any one barrier had been in place then the incident would have been prevented or at least its consequences made less severe.

APPLICABILITY OF CROSS-SECTOR PEER REVIEW

We now discuss whether cross-sector peer review does or could address each of the issues listed in Tables 1 and 2. We identify them as:

☑ No further action, issue already addressed.

Table 1. Analysis of issues in the 42 incidents described by Atherton & Gil (For further details see Attachment A)

Issue (as listed by van Wijk et al. [2008])	Number of occurrences	Percent occurrences
Leadership issues	13	31%
Operational attitudes and behaviours (operational "culture")	13	31%
Impact of the business environment (often commercial and budgetary pressures)	16	38%
Oversight and scrutiny	24	57%
Competence and training (at all levels)	21	50%
Risk assessment and risk management	26	62%
Organisational learning	23	55%
Communication issues	16	38%
TOTAL	**152**	**3.6 issues per incident**

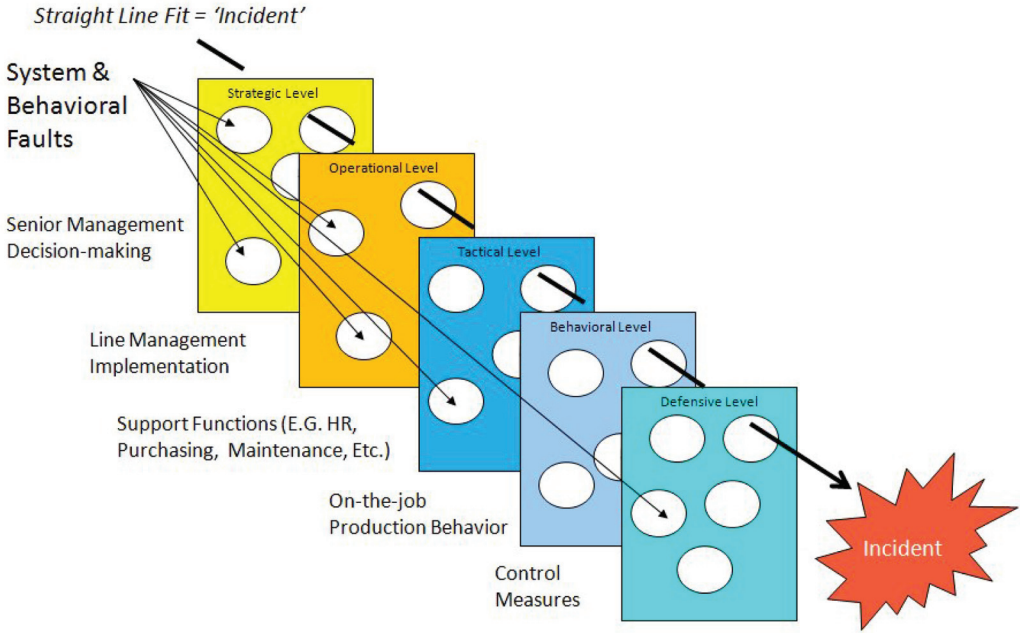

Figure 1. 'Swiss Cheese' model of accident causation (figure kindly provided by Dominic Cooper, B-Safe Management Solutions Inc.)

? Some development needed, issue addressed in the pilot studies but not explicitly discussed in the reports.
☒ Cannot effectively be addressed in cross-sector peer review.

LEADERSHIP ISSUES

✓ This topic was covered in both pilot studies and was addressed both by observing leaders in the workplace or meetings, and in discussions with them and with the workforce.

OPERATIONAL ATTITUDES AND BEHAVIOURS

? In both pilot studies we observed workers and had extensive discussions with them, so were able to assess the operational attitudes and behaviours, although they were not explicitly listed in our reports.

IMPACT OF THE BUSINESS ENVIRONMENT

✓ This topic was covered in both pilot studies through discussion with leaders and the workforce, including questions like, 'If money and resources were no restriction, how would you like to improve safety?'

OVERSIGHT AND SCRUTINY

✓ This topic was covered in both pilot studies under 'Managing change' and questions about the programme of audit and follow-up.

COMPETENCE AND TRAINING

✓ Operations and maintenance staff: this topic was covered explicitly in both pilot studies.
? Design staff: not covered in the pilot studies. It could be covered to a certain extent in a cross-sector peer review,

Table 2. Further analysis of the 42 incidents described by Atherton & Gil

Issue	Number of occurrences	Percent occurrences
Non-standard operating conditions	4	10%
Design or hazard issues apparently not understood by operations	14	33%
Non-standard operating conditions AND design or hazard issues apparently not understood by operations	12	29%
TOTAL	**30**	**71%**

for example assessing adherence to codes and standards, use of incident databases to identify risks in similar facilities, however see 'Design issues' below.

? Asset inspection staff: This topic was covered explicitly in pilot study 2 under 'Asset management'. However there have been a number of process safety incidents where pipework or vessels have failed with catastrophic consequences. For example:
  - Plants containing very cold (cryogenic) material are designed with special steels in the low temperature sections; there have been instances where the incorrect steel was installed at construction (or subsequently replaced) and was not picked up by the materials control systems and post-installation inspections. Similar issues have arisen due to faulty welding.
  - Plants have suffered severe localised corrosion at liquid-liquid or liquid-gas interfaces, with this corrosion not being picked up by routine inspections that did not test pipework at the specific interface.

  For both the above cases we consider that a technical peer review, conducted by specialist inspectors from similar plants, would be most effective in ensuring that the inspectors being reviewed were using best current inspection practices and inspection equipment. Inspection peer reviews of a facility being constructed would deliver best value for money if conducted at appropriate points during the construction phase, as any identified inspection deficiencies could be corrected without needing to re-inspect a large proportion of the facility, some of which might not be readily accessible at later phases of construction.

RISK ASSESSMENT AND RISK MANAGEMENT

✓ This topic was covered explicitly in pilot study 1 under 'Identifying and managing risk'.

ORGANISATIONAL LEARNING

✓ This topic was covered explicitly in pilot study 1 under 'Incident investigation & learning from experience'.

COMMUNICATION ISSUES

✓ This topic was covered explicitly in pilot study 1 under 'Communication'.

DESIGN ISSUES

☒ In the pilot studies, some information was gathered on this subject when managers and workers complained about inadequacies in their facilities. However, in several of the incidents described by Atherton & Gil, it was clear that operating and maintenance teams were unaware of certain design deficiencies until after the incident had occurred, although staff in other facilities had known about them. This is another case where we consider that a technical peer review, conducted by specialist designers of similar plants, would be most effective in ensuring that the designers being reviewed were using best design practices. Such design peer reviews would deliver best value for money if conducted at appropriate points during the design process, as any identified deficiencies could be corrected at minimal cost. If a design peer review were conducted after a facility had been constructed, it might not be possible to rectify any identified design deficiencies but other mitigation measures could be considered through procedures, instrumentation or mechanical improvements.

NON-STANDARD OPERATING CONDITIONS

? This is a difficult issue for any safety management system because, by their nature, non-standard operating conditions are almost impossible to observe, either because they are unscheduled or because, in a scheduled non-standard activity such as a turnaround, staff are expected to be so busy that observers would be an intrusion. Several ways are suggested to address this issue:
  - When assessing 'Competence and training' in a peer review, discuss what training is given to staff in dealing with non-standard conditions and emergencies, including drills, responding to incident scenarios, use of process simulators, etc.
  - Reviewing incident reports, both near hits and ones with adverse consequences, to assess the competence of staff in handling non-standard operating conditions. Similarly reviewing any startup / shutdown reports.

CONCLUSIONS

Cross-sector peer review has been shown to be a powerful tool for improving both occupational safety and process safety. We have suggested how some of the limitations for process safety might be addressed and have suggested alternative means for the ones which are outside its scope.

But without a 'regulatory' driven peer review, major operators of safety-critical installations will convince themselves that they know best and attempt a different solution. If a company is at the top of cultural safety it considers itself immune to accidents and if it is at the bottom it does not want its peers to know (it affects share price in the short term even though recent tragedies show the long term impact in lives, costs and degraded performance). How many more deaths does it take before someone will take notice? Our next challenge is to lobby regulators to get involved in cross-sector peer review.

ACKNOWLEDGEMENTS

I am grateful to my colleagues in the Cross-Sector Peer Review Working Party of the Institution of Occupational Safety and Health, Hazardous Industries Group, for their advice and assistance in the Peer Review Stage 1 Pilot.

I am also grateful to John Atherton and Frederic Gil for their excellent book, and to Dick Taylor for a copy of the paper by himself and his colleagues.

ATTACHMENT A: ANALYSIS OF CAUSES OF MAJOR PROCESS INCIDENTS

Incident	Situation	Leadership	Operations culture	Business pressures
Blind Operations				
Tenerife KLM/PanAm 747s colllided on runway, 1977; 583 fatalities	Airport overloaded by diverted planes; fog			KLM running close to permitted crew hours, high cost/ inconvenience to suspend flight away from destination
Paris MD83/Shorts 330 collided on CDG runway, 2000; 1 fatality	Construction work closed normal taxiways; flashing yellow lights; extended hours due to sporting event			
Three Mile Island nuclear reactor overheated and released radioactivity, 1979; large scale evacuations, nuclear power development halted for decades	Normal ops then cooling water pumps failed and relief valve stuck open			
Design				
Bhopal MIC storage tank ruptured and released toxic gases, 1984; ~2,000 fatalities, 50,000 disabled	Storage tank fridge system shutdown 6 months earlier but alarms not reset; scrubber and flare both shut down for maintenance	Encouraged cost savings	Tolerated deviations from design conditions	Cost savings by not purchasing refrigerant
NASA *Challenger* Space Shuttle exploded at launch, 1986; 7 fatalities, shuttle programme halted	Normal launch procedure but very low ambient temperature		Complacency following 17 successful missions	Political pressure to go ahead with launch
K-Boat WW1 submarines numerous sinkings, 1914–1918; ~140 fatalities	Development during WW1 with U-Boats sinking many ships	Obsession with submarines matching surface ships' 21 knots speed led to steam driven design; low value on human life due to collective mindset to defeat enemy by whatever means		
TWA800 747 centre wing tank exploded in midair, 1996; 230 fatalities	Normal flight			Very high cost of rewiring aircraft once aging wiring identified but screening could have been added

Oversight	Competence	Risk assessment & management	Learning	Communication	#
	Controllers did not prepare revised procedure when overload became apparent (Management of Change – MoC)	Situation not anticipated		PanAm crew had difficulty understanding controller	N
	Controller refamiliarising himself with CDG, made wrong assumption about Shorts position		Previous near hits not yet acted upon	French/English languages so Shorts crew did not understand MD83 communications; poor system for updating ATC info slips	N U
	Back-up emergency cooling water system had not been reinstated following recent test	Situation not anticipated in HAZOP		Operators on duty overwhelmed by alarm overload	
No overriding Engineering Authority; previous Union Carbide audits may not have been addressed		Lack of intrinsic safety in design (large intermediate storage); no risk assessment of degraded plant condition	Unreliable pressure gauges always ignored	Supervisor did not act on workers' reports of burning sensations	N U
Engineering Manager persuaded to overrule engineers concerns about low temperatures overruled for political reasons			O' ring erosion not taken seriously		N U
No overriding Engineering Authority	Views of experienced submariners ignored during development	No clear analysis of 'fleet sub' strategy, need to dive quickly, heat retention in boiler room, crew unable to move between bow and stern sections when submerged	Numerous incidents ignored, when operating submarines along with surface ships	No communications between exercise mgt and minesweepers	
New technical standards not applied retrospectively			Tests and other aircraft accidents had shown that fuel-air explosion in CWT would destroy aircraft; poor aging of wiring led to changes for new aircraft		

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Hindenburg airship destroyed by fire when landing, 1937; 36 fatalities, ended airship development	Thunderstorm during normal landing	Propaganda value of putting airship into service as soon as possible		Helium not available (US Helium Control Act) so hydrogen used – probably did not cause the fire but propagatec it more quickly
External Causes				
Mexico City LPG terminal fires and BLEVEs, 1984; 600 fatalities	Normal operations receiving LPG from pipelines			
Earthquake damaged Turpas Refinery, Turkey, 1999; no fatalities but tank farm destroyed by fire	Process units shut down safely after earthquake but CDU concrete stack collapsed causing major fire, fire mains damaged, fire escalated to tank farm			
Inspection and Maintenance				
Betelgeuse oil tanker fire and explosion, Bantry Bay, 1979; 50 fatalities	Discharging crude oil, normal ballasting operations to control stresses on hull structure	Failure to invest in essential ship repairs and upgrades (ballasting stress computer and inert gas blanketing)	Jetty dispatcher not at his post when fire started hence delay in starting fire pumps	Cost pressures to keep ship commercially viable vs modern larger tankers
Erika oil tanker sinking during heavy storm, 1999; no fatalities but 10,000 tonnes of oil spilled causing significant pollution	Normal voyage but listed in heavy weather, crew attempted to correct list but deck cracked and ship broke into two			Cost pressures
Canadian Pacific TS236 ran out of fuel over Atlantic, pilots managed to glide aircraft to safe landing, 2001 no casualties	Normal flight, sudden imbalance in fuel due to loss of fuel, later found caused by abrasion of fuel line from hydraulic line			

Oversight	Competence	Risk assessment & management	Learning	Communication	#
No tests on flammability of new doping formulation on envelope fabric		Lightning strikes not identified as problem	60 out of 161 rigid airships destroyed either by fire or structural failure		U
Pipeline pressure relief not uprated for increasing flow from supply refineries; additional tankage installed at closer spacing than international codes; local housing allowed to be built in close proximity		None conducted	Local safety committee inspections had revealed critical failings but may not have been acted on		
Lack of comprehensive earthquake design		Knock on effects of earthquake not identified on power supplies, fire mains etc			
Owned and operated by international oil company, but not clear that robust engineering authority in place		No recognition that calculation for ship ballasting was invalid due to corrosion. Apparently no recognition of implications of changing jetty firewater pumps from auto to manual operation due to leaks, also foam system	Ship: inspection revealed severe internal corrosion but cathodic protection not renewed nor ballast tanks coated with protective material; sister ship being broken up		U
Numerous changes in ownership, ship's name and classification society so discontinuities in maintenance and inspection Classification society did not get info on sister ships			Numerous structural faults identified and repaired, should have indicated ship was reaching end of life. All 8 sister ships have suffered serious structural failure		
	Maintenance technicians replaced hydraulic pump on engine with slightly different pump, did not fit bracket to locate hydraulic lines clear of fuel lines (MoC)				U

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Fire on HMS Glasgow while being fitted out, 1976; 8 fatalities	Fit out in shipyard		Short cut practices in use of oxygen for welding in confined spaces; several trades working simultaneously in small space	
HF release at Marathon Oil Refinery, Texas City, 1987; no fatalities but 4,000 residents evacuated	Turnaround: lifting heavy equipment over plant, load slipped and fractured live piping			
Explosion and fire at Texaco oil refinery, Milford Haven, 1994; $76 million damage	Normal operations until lightning caused fire in one process unit. During restart, flare KO pot overfilled and ruptured	Senior personnel took over operating roles rather than taking process overview	Attempting to restart during extreme upset conditions rather than shutting down. Blast-resistant control room compromised by open door because AC faulty	
Total La Mede FCCU explosion, 1992; 6 fatalities	Normal operations until corrosion hole in bypass line released large vapour cloud, which exploded causing major plant damage and collapsing roof of control room			
Knowledge and Training				
Elf Feyzin LPG BLEVE, 1966; 18 fatalities	Routine sampling of propane sphere led to valves icing up and uncontrolled release which ignited/exploded, eventually fire-engulfed sphere ruptured causing BLEVE		Using drain line as sample point as installed sample points were inoperable (MoC)	
Ammonium Nitrate explosions – Oppau 1921, Texas City 1947, Toulouse 2001; more than 1,000 fatalities	Oppau: using blasting powder to break up storage piles of AN. Texas City: fire on ship carrying mixed cargo of combustibles and AN. Toulouse: fire in warehouse used as temporary store for off-spec AN		Oppau: blasting powder had been frequently been used without incident. Toulouse: possible poor housekeeping	
Dust explosion at Courrieres mine, France, 1906; 1,099 fatalities				

Oversight	Competence	Risk assessment & management	Learning	Communication	#
	Workers did not recognise danger signals from coloui of cigarette lighter flame or speed of cigarettes burning		Shipyard's knowledge of oxygen hazard and procedures not emphasised to contracting company		U
		Failure to assess lifting risks and prepare Method Statements			N
Tolerance of corroded flare line and defective instruments	Operators overwhelmed by alarm overload and poor heat/mass balance info from display screens	HAZOP not applied to specific KO pot		Knowledge of how to reinstate high rate liquid disposal system had been lost	N U
Tolerance of inadequate inspection regime in an aging plant			Industry knowledge of major FCCU incidents had not resulted in high quality inspection regime, nor of removing or reinforcing control room which was not blast-resistant		U
Tolerance of being able to use only 1 of 2 firewater pumps due to pressure restrictions on fire main. Reliance on 'active' fire protection (firewater sprays) rather than 'passive' (fire protection coatings.			In 1966 the hazards may not have been widely recognised of LPG drain or sample valves getting stuck open due to icing up, and of LPG vessel rupture below design pressure due to steel being weakened by fire engulfment.		U
Tolerance of large inventories of AN coupled with low separation distances.					U
			Methane gas explosions were well known (hence mandatory safety lamps in some countries), but dust explosions were not identified until after this disaster.		U

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Lack of Hazid (HAZard IDentification)				
Sinking of SS *Titanic* in Atlantic, 1912; over 1,500 fatalities	Maiden voyage, travelling at full speed through floating pack ice, unable to avoid iceberg spotted by lookout, severe damage to many watertight compartments, sank 3 hours later	Managing Director applied pressure for fast journey and bypassed captain in discussing tactics directly with chief engineer. Insisted on engines being restarted before full damage review		Competing with other shipping companies on lucrative cross-Atlantic routes for upper class and business class passengers
Esso Longford gas plant explosion, 1998; two fatalities and major disruption to gas supplies in Victoria, Australia	Normal disposal route for condensate build up not available, temperature should have been increased but not done, process upsets caused extreme cold, when equipment warmed up without depressurising brittle facture occurred and resulting cloud of gas and oil exploded		Royal Commission concluded that Exxon's complex Operations Integrity Management System (OIMS) was difficult to understand and divorced from reality of operations. Large number of alarms active at any one time	
BP Grangemouth hydrocracker explosion, 1987; 1 fatality	Preparing unit for startup, gas breakthrough from 155 bar High Pressure Separator (HPS) into 10 barg Low Pressure Separator (LPS) which disintegrated.		HPS low level alarms ignored. Did not report earlier incident when gas heard passing from HPS to LPS causing relief valve to open, level control valve closed by operator	
Reactive chemicals – Rohm & Haas UK 1976, 3 injuries; Bartlo US, 1997, 3 fatalities; Napp US, 1995, 5 fatalities	Rohm & Haas: Road tanker with contaminated product parked up over weekend, contents polymerised and ruptured tanker. Bartlo: Bags of reactive chemical stored against hot pipe and thermally decomposed, releasing smoke and flammable gases which exploded after firefighters on site. Napp: Cooling water leaked through seal into blender containing reactive chemical, smells and smoke seen, then exploded			

Oversight	Competence	Risk assessment & management	Learning	Communication	#
Chief designer accepted design change to terminate watertight bulkheads 2 levels below weather deck to allow greater freedom of movement, and to reduce lifeboats from 64 to 16 as Titanic was 'unsinkable'.	Very experienced captain had record of several serious incidents – 3 groundings, 1 collision and 1 near-collision.	Design changes not evaluated.		Nearest ship did not respond to distress rockets; more distant ship put itself at risk by racing through ice field.	U
Two years earlier, technical experts had been relocated away from plant to head office in Melbourne, had they been on site would have helped understand potential for brittle fracture (MoC).	Supervisors and operators did not know the dangers of operating process equipment at extremely low temperatures.	HAZOP had been planned for 1995 but not carried out. Modifications to condensate system had recognised carry over potential but impact on downstream vessels not assessed.			N U
No action taken on audit findings of operational problems with leve detection. Tolerance that low level trip was disabled due to spurious trips	Control room operator on duty not trained in procedure to warm up pipework for startup by manual opening of HPS level control valve	Built before the days of HAZOP, but gas breakthrough identified as hazard and protected against by 2 low level switches to shut HPS level control valve. No assessment of decision to disable low level trip (MoC)			N U
	Because of lack of risk knowledge, operators were inevitably unaware of precautions to be taken	General lack of understanding about reactive chemical hazards, potential for major incident grossly underestimated or completely ignored, minimal or no risk assessments	Much information on reactive chemicals available from literature and in reports by regulators, but apparently not used by these three companies		U

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Management of Change				
Chernobyl nuclear reactor explosion, 1986; 30 immediate fatalities, 135,000 people evacuated, concern about delayed fatalities	Experiment to test procedure during power failure to keep coolant circulating while standby generators are starting. Normal emergency systems bypassed. Eventually explosion of CO and H2 blew off roof of reactor building	Key decision makers and experts who could have challenged judgement of onsite teams, had left for the weekend before the test commenced		Design has inherent safety problem but overwhelming commercial benefits of this design appear to have outweighed safety concerns
DSM Nypro explosion at Flixborough UK, 1974; 28 fatalities (would have been many more if explosion occurred during working week)	Crack detected in Reactor 5 of 6, decision to remove Reactor 5 and connect Reactors 4 & 6 using temporary piping. After 2 months operation, plant shutdown to repair leak. On restart, temporary piping ruptured and clouc of cyclohexane exploded, destroying plant including control room	Pending reorganisation, had appointed as acting Maintenance Manager the Laboratory Manager who did not have necessary engineering knowledge and experience		
Not Learning From Near Misses				
NASA *Columbia* Space Shuttle destroyed on reentry, 2003; 7 fatalities	On routine launch, insulation foam became detached and damaged protective heat resistant tiles on wing. On re-entry, wing overheated and failed, causing Columbia to lose aerodynamic control and break up	Over previous decade had lost 40% of budget and workforce, handing over much of operational responsibilities to a single contractor. Leadership increasingly driven by schedule and delivery	"Can do" attitude, nobody prepared to challenge management. Foam separation became an accepted part of every flight, leading to a routine repair activity to replace damaged tiles. Lack of effective checks and balances	Pressure to keep Space Shuttle programme on schedule, particularly to complete International Space Station
Capsize of *Herald of Free Enterprise*, 1987; 193 fatalities (would have been many more had vessel not been turned rapidly so it capsized onto sandbank rather than sinking completely)	Routine departure from port, sailed with bow doors open (the responsible junior officer was asleep in his cabin), vehicle deck flooded and vessel capsized	Emphasis on rapid sea crossings and quick port turnarounds. Subsequent evidence of overloading and carrying excess passengers		Competition from other ferry operators (this was before Channel Tunnel)

Oversight	Competence	Risk assessment & management	Learning	Communication	#
	During the experiment, engineers and operators disabled critical safety devices and continued operation of the reactor outside its safe operating envelope	No formal risk assessment of the experiment (MoC)			N U
Nobody at senior management level in the plant with technical knowledge to ensure that the proper technical standards and sound engineering practice was applied to all engineering work	No expert input into design of temporary piping	No risk assessment of the change – but if there was no mechanical expertise on the hazards of the temporary piping then it may not have been identified (MoC)		Maintenance Engineer recommended 3 week shutdown to repair Reactor 5 but overruled by acting Maintenance Manager	N U
Engineering Authority did not ensure proper investigation of potential major problem identified after launch. No independent safety programme		Foam separation detected from detailed examination of launch photos and videos, so Damage Assessment Team created. No adverse effects noticed by crew or ground support. Engineers challeged to prove that safety issue existed, but denied satellite means to determine extent	Foam separation occurred on every flight but not investigated in detail until after Columbia lost. Chemical Accidents Investigation Board concluded after Columbia was lost that NASA was not an organisation having the characteristics of a learning organisation	NASA engineers made 3 requests to Department of Defense for satellite imagery to examine for damage to Columbia, cancelled by managers as request not made through official channels	U
Roll On-Roll Off (RO-RO) ferries must have watertight hull, with back up from watertight bulkheads on cargo deck which is costly and reduces carrying capacity – not done. Shore based managers did not define roles and responsibilities of officers, preferring to let them 'evolve'		Suggestions had been made by various ships officers to fit remote indication of bow and stern door status – but not followed up	Ships had sailed on 5 previous occasions with bow or stern doors open – but shore management had not advised ships' Masters	No requirement for positive confirmation that doors closed from junior officer to bridge	

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Air France Concorde crash, Paris, 2000; 113 fatalities	Normal takeoff, after reaching lift-off speed a tyre blew out and punctured fuel tank. Escaping fuel ignited and plane crashed into nearby hotel. Subsequently piece of metal found on runway, having come from plane which took off immediately before Concorde - this metal is believed to have destroyed the tyre which failed			Concorde returned to service 15 months after the Paris crash, following safety modifications, but was no longer commercially viable and was retired in 2003
Operating Practices				
R101 airship crash, 1930; 48 fatalities (6 survivors)	During inaugural flight from UK to India, R101 experienced high winds, which damaged the hydrogen gas bags and led to the airship going into a steep dive, hitting the ground and bursting into flames	Intense political pressure to start inaugural flight taking Secretary of State for Air to India, prevented proper flight trials		Modifications made to gas bags and supporting wires in an attempt to increase useful lift from uneconomic 35 te to design lift of 60 te. These caused chafing of the bags so padding added
Explosion and fire on Tosco hydrocracker, US, 1997; 1 fatality	Unit had been in startup mode for previous 10 days. Reactor temperature excursion increased to the point where temperature above 760C caused reactor effluent pipe to fail			Reluctance to depressure, further extending an already protracted start up
BP Texas City ISOM unit explosion, US, 2005; 15 fatalities	Plant startup, blowdown drum overfilled so hydrocarbon liquid ejected from vent and then exploded causing major damage to nearby trailer park installed to service major turnaround on nearby unit, killing many occupants	BP subsequently commissioned an independent safety review led by ex-Secretary of State James Baker [Baker, 2007]. This seriously criticised BP's corporate safety culture; process safety management systems; and performance evaluation, corrective action and corporate oversight. 10 significant recommendations were made	Training deficiencies identified in 2003 and 2004, but Training Co-ordinator spent only 5% of his time on training	Although blowdown drum design philosophy was dated and had been superceded, opportunity not taken to replace it when major flare sytems were installed in 1995 and 2002

Oversight	Competence	Risk assessment & management	Learning	Communication	#
	The flight crew were all experienced personnel - but in this case there was nothing they could have done to extinguish the fire at the height and speed they were able to achieve		There had been 5 previous occurrences of damage to Concorde fuel tanks associated with a tyre burst, but none had escalated to an ignited fuel leak. After this incident, a design change was made to protection the fuel tanks against disintegrating tyres and wheels		
	The finest technical brains were used to design the airship – but the final decision to take off on the inaugural flight was made purely on programme considerations		The fact that so many airships had crashed over the years should have alerted the authorities to the high risks involved, but a perception of invulnerability seems to have developed among the most senior people involved	Little sharing of technical concerns with the highest levels of management, or government, erring on the side of telling them what it was thought they wanted to hear	
Tolerance of unreliable instrumentation, with quench and emergency depressuring systems on manual	Operators had not received consistent instructions on when to initiate depressuring manually	Original process hazards analysis had not addressed the inherent hazard of extreme exothermic conditions. Instrument field panel was installec close to reactors without MoC review			N U
Site Engineering Authority had no designated experienced engineers, not automatically involved in MoC, and no interface with Process Safety Committee	Confusion over which of 2 different startup procedures to use. 11 major deviations from Safe Operating Procedures	Major Accident Risk assessment for Texas City in 2003 did not consider possibility of column overfill/ overflow and consequent impact of liquid in relief systems. MoC required temporary buildings to be at least 100 m from process unit – in fact nearest trailer was only 45 m away from blowdown drum	At least 19 incidents over 15 years of hydrocarbon vapour releases from blowdown drum vent, but corrective actions focussed on training and procedures rather than operating philosophy	No local supervision after shift supervisor left site 3 hours earlier for personal reasons	N U

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Permit to Work Systems				
Motiva refinery explosion, 2001, US; 1 fatality	Walkways being repaired over 6 sulphuric acid tanks, cutting equipment ignited flammable gas escaping from corrosion hole in tank			
Phillips Pasadena explosion, 1989, US; 23 fatalities	During routine maintenance work to clear blockage in polyethylene reactor, major release occurred due to air hoses to open/close critical valve being connected in reverse position			
Piper Alpha platform destroyed, UK North Sea, 1988; 167 fatalities	Starting standby pump without realising relief valve had been removed for maintenance, explosion blew down firewall, automatic seawater deluge had not been reinstated after divers near pump inlets had stopped work, fire caused gas risers to fail catastrophically		Don't shut down platforms unless authorised by onshore managers	
Shell oil depot explosion, Lyon France, 1987; 2 fatalities	Initiating fire thought to be started by welding work to construct a new tank			
BP Grangemouth flare line fire, UK, 1987; 2 fatalities	During shutdown, as valve on 30" flare main was being removed, large quantity of hydrocarbon escaped and resulting cloud ignited		Accepted difficulty of working from high small scaffolding while wearing air-line breathing apparatus	

Oversight	Competence	Risk assessment & management	Learning	Communication	#
Tolerance of severe corrosion on acid tanks, with inert gas to the tank that exploded being routed through a rubber hose as the original nozzle had fallen off due to the corrosion		No Job Safety Analysis for this work, although it was well known that spent acid always contains entrained hydrocarbons		Operator lodged an Unsafe Condition Report about the nitrogen supply via hose one month earlier, but no positive action taken	N
Local managemen had put in place a procedure in direct violation of company's corporate process safety rules and industry standards, which require a double block and bleed valve or a line blind		No risk assessment known	Company safety audits by Phillips personnel and outside companies had identified unsafe conditions but had largely been ignored		
Tolerance of ineffective 'permit to work' system, lack of lock out/tag out system, no protection for gas risers			Independent audit had recommended deluge system to protect risers, with automatic shutdown valve at sea level, but not mentioned at board meeting that reviewed audit report. Regular safety audits were not performed well, few problems identified, major problems sometimes ignored	Connected platforms did not shut off gas flow for over an hour, unable to contact shore based managers for approval due to damaged communications system which were routed via *Piper Alpha*	N U
		No risk assessment known		Law required local authority to take control of emergency so plant personnel had to leave depot reducing technical information available to emergency services	N
	After Operations Supervisor refused to issue work permit because necessary job preparation had not been completed and he was busy elsewhere on the shutdown, a Junior Operations Supervisor checked the flare main drain well away from the valve being removed, without realising that liquid could be lying in lower point closer to the valve	Decision to do the job that day appeared to be taken by shutdown engineers and planners with no discussion on safety aspects			N U

(*Continued*)

Attachment A. Continued

Incident	Situation	Leadership	Operations culture	Business pressures
Emergency Response				
Seveso toxic cloud release, Italy, 1976; no fatalities but population evacuated, major cleanup, local food banned and animals destroyed	Plant shutdown for weekend (as normal), leaving reactor full of material at elevated temperature, uncontrolled exothermic reaction overpressured reactor so bursting disc relieved			
Sandoz warehouse fire, 1986, Switzerland; no fatalities but large quantity of chemicals and contaminated firewater entered Rive Rhine	Fire broke out in unsprinklered warehouse, 10,000 to 15,000 m^3 of firewater completely overwhelmed 50 m^3 water treatment system			
Tacoa power station boil over, 1982, Venezuela; 160 fatalities	Operators transferred fuel oil between tanks on hill above power plant. Seeing product temperature was 88C not 65C, heat tracing cut off. While operators were manually gauging tank, explosion blew off tank roof and started fire. 4 hours later, massive boilover caused fireball and wave of burning liquid. Boil over occurs when hot residues from surface of burning tank sink to water layer and vaporise it with resulting steam explosion			
Human Factors				
Exxon Valdez oil tanker spill, 1976, Alaska; no fatalities but major environmental pollution and cleanup	During routine journey, ship ran aground and holed cargo tanks	Company did not monitor captain after alcohol rehabilitation programme		Crew levels had been reduced, resulting in fatigue
Flash Airlines Boeing 737 crash, 2004, Egypt; 148 fatalities	Aircraft took off normally but then dived into sea 9 miles from the runway			

Unless indicated otherwise, the author extracted all the data below from Atherton & Gil [2008], who had also assigned the subheadings.

Oversight	Competence	Risk assessment & management	Learning	Communication	#
	Clear failure to leave plant in safe state for weekend	Company initially denied knowledge of toxic substances involved, causing 9 day delay in authorities evacuating population	5 major incidents had previously occurred worldwide on similar plants, all since shutdown except for 1 which was rebuilt with significantly increased protection		U
		No consideration had been given to potential water pollution			U
Fire protection systems vulnerable to damage in emergency; tanks located on hill above power plant; poor access for firefighting			6 previous boilovers had occurred worldwide several hours after tank fire started, apparently not known to firefighters		U
	Captain left bridge in command of junior officer and helmsman, contrary to Federal pilot regulations. At least 2 officers should have been on duty in congested waters				
	Investigators concluded that Captain became disoriented and co-pilot who was aware of problem failed to take over control			Co-pilot tried to explain problem to Captain rather than taking over control	

N = non-standard operation; U = lack of understanding

REFERENCES

Atherton, John and Gil, Frederic, 2008, 'Incidents that define process safety', ISBN 978-0-470-12204-4, Center for Chemical Process Safety of the American Institute of Chemical Engineers and John Wiley & Sons, Inc.

Baker, James A. et al. 'The Report of the BP U.S. Refineries Independent Safety Review Panel', 2007, free download from www.bp.com by searching for baker_panel_report.

BP, 'Deepwater Horizon Accident Investigation Report', report of an internal BP incident investigation team, 2010, free download from www.bp.com by searching for deepwater horizon report.

Buncefield Major Incident Investigation Board, 2008, The Buncefield Incident 11 December 2005 – Final Report Volumes 1, 2a and 2b, free download from http://www.buncefieldinvestigation.gov.uk/reports/index.htm

Eves, David, 2010, 'Disasters: learning the lessons for a safer world', ISBN 978-0-901357-46-5, IOSH Services Limited, UK.

Kletz, Trevor, 2009, 'What Went Wrong – Case Studies of Process Plant Disasters and How They Could Have Been Avoided', Fifth Edition, ISBN 978-1-85617-531-9, Elsevier Inc.

Sellers, J.G., Mason, D.J. and Hemming, K., 2009, 'Accelerating learning through cross-sector peer reviews', Hazards XXI, IChemE Symposium series no. 155, Institution of Chemical Engineers, Rugby UK.

Van Wijk, Lorenzo G.A., Taylor, Richard H., May, John H.R., 2008, 'Cultural and Organisational Factors Leading to Major Events', TOPSAFE conference, Dubrovnik, Croatia.