Safety Culture and Major Accidents

Mark Hailwood, Zsuzsanna Gyenes

1 Event: Macondo (2010)

1.1 Brief Description:

On the evening of 20 April 2010, a ‘well control event’ allowed hydrocarbons to escape from the Macondo well onto Transocean’s Deepwater Horizon oil rig in the Gulf of Mexico.
Eleven people were killed and 17 were injured in the resulting explosions and fire, which burned for 36 hours until the rig sank. Hydrocarbons continued to flow from the reservoir through the wellbore and the blowout preventer (BOP) for 87 days, causing a significant spill.
The following month, US President Barack Obama announced the creation of the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling: an independent, nonpartisan entity, directed to provide a thorough analysis and impartial judgment. The Commission reported in January 2011. It found the immediate cause of the blowout to be ‘a failure to contain hydrocarbon pressures in the well’.

1.2 Indication of defective safety culture:

Numerous investigations explored the causes of the explosion and record-setting spill. Notably, the U.S. government's September 2011 report pointed to defective cement on the well, faulting mostly BP, but also rig operator Transocean and contractor Halliburton. Earlier in 2011, a White House commission likewise blamed BP and its partners for a series of cost-cutting decisions and an insufficient safety system, but also concluded that the spill resulted from "systemic" root causes and "absent significant reform in both industry practices and government policies, might well recur".

- Managers misread pressure data and gave their approval for rig workers to replace drilling fluid in the well with seawater, which was not heavy enough to prevent gas that had been leaking into the well from firing up the pipe to the rig, causing the explosion.
- The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling released a final report on 5 January 2011. The panel found that BP, Halliburton, and Transocean had attempted to work more cheaply and thus helped to trigger the explosion and ensuing leakage.
- The accident „exhibits the costs of a culture of complacency”.
- „[A]ny successful oil and gas industry safety institute would require in the first instance strong board-level support from CEOs and boards of directors of member companies for a rigorous inspection and auditing function. Such audits would need to be aimed at assessing companies‟ safety cultures (from design, training, and operations through incident investigation and management of improvements) and encouraging learning about and implementation of enhanced practices.‟

2 Event: Chernobyl (1986)

2.1 Brief Description:

On Monday, April 28, 1986, at 1:24 an experiment to check the use of the turbine during rundown as an emergency power supply for the reactor went catastrophically wrong. There was a power surge in the reactor, the coolant tubes burst, and a series of explosions rent the concrete containment. The graphite caught fire and burnt, sending out a plume of radioactive material. Emergency measures to put out the fire and stop the release were not effective until May 6.

2.2 Indication of defective safety culture:

- Management of Change – similar to Flixborough in this respect.
- No indication that a risk assessment preceded the test.
- High demand to increase production that put pressure on the experimenting team.
- When eventually the test began, the key decision makers and experts who could have challenged the judgement of the onsite teams had left for the weekend.
- Even though the test was planned, the permission was given to run it using the automatic system and not in manual mode. The test procedure was altered on an ad hoc basis and so critical safety devices were disabled.
- In principle, employees at all levels should be equally comfortable stopping each other when at-risk behavior is observed and recognizing each other when safe behavior is observed. However, in this case the operators knew that switching off the reactor emergency core cooling system was directly against regulations. Violation of procedures.
- Due to a chain of operator errors within the test, not following the regulations, the reactor could not be shutdown which initiated a chain of further events that led to ignition and explosion.
- The reactor was operated with boiling of the coolant water in the core and at the same time with little or no sub cooling at the pump intakes and at the core inlet. Such a mode of operation in itself could have led to a destructive accident of the kind that did ultimately occur, in view of the characteristics of positive reactivity feedback of the reactor. Failure to recognize the need to avoid such a situation points to the flaws in operating a nuclear power plant without a thorough and searching safety analysis, and with a staff untutored in die findings of such a safety analysis and not steeped in safety culture.
- Operation of the reactor with almost all control and safety rods withdrawn to positions where they would be ineffective in achieving a quick reduction in reactivity if 19 shutdown were suddenly needed. Awareness of the necessity of avoiding such a situation should be second nature to any responsible operating staff and to any designers responsible for the elaboration of operating instructions for the plant.

3 Event: Bhopal (1984)

3.1 Brief Description:

Early in the morning of December 3, 1984, a relief valve lifted on a storage tank containing highly toxic methyl isocyanate (MIC) at the Union Carbide India Ltd (UCIL) works at Bhopal, India. A cloud of MIC gas was released onto housing, including shantytowns, adjoining the site.
Close on 2000 people died within a short period and tens of thousands were injured.

3.2 Indication of defective safety culture:

- The UCIL facility in Bhopal was not profitable and was being run down.
- Important safety equipment had either been removed or was not operational.
- This incident also raises questions on application of Industry standards in countries where Local Authorities are not applying much scrutiny.
- The plant was not maintained to a high standard consistent with the handling of a dangerous material such as MIC.
- Between 1979 and 1982, the Bhopal plant underwent three Union Carbide audits. According to Union Carbide the most recent audit had been in 1982 when an “operational Safety Survey” was conducted. It found that there were major safety concerns in the MIC production unit that could lead to serious personnel exposures. Union Carbide asserts that none of these recommendations would have had an impact on the December 3, 1984 release, and that all of the issues had been addressed well before it occurred. Nevertheless it is reported elsewhere that, at the post incident trial, it was not clear as to whether the local

company or its US parent had the responsibility for implementing survey recommendations.

- Two and a half years after the disaster Union Carbide Corporation (UCC) filed a court document in India detailing the findings of the consulting firm Arthur D. Little contracted by the corporation, which came to the conclusion that the cause of the MIC release could only have been the result of sabotage, thus absolving UCC from much of the blame. This investigation has in the meantime been shown to be incomplete and at least four different scenarios are considered possible.

4 Event: Herald of Free Enterprise (1987)

4.1 Brief Description:

On the day the ferry capsized, the Herald of Free Enterprise was working the route between Dover and the Belgian port of Zeebrugge. This was not its normal route and the linkspan at Zeebrugge had not been designed specifically for the Spirit class vessels: it used a single deck, preventing the simultaneous loading of both E and G decks, and the ramp could not be raised high enough to reach E deck. To compensate for this, the vessel's bow ballast tanks were filled. However, the ship's natural trim was not restored after loading. Had the Herald survived, she would have been modified to obviate this procedure.

Before dropping moorings, it was normal practice for the assistant boatswain to close the doors. However, the assistant boatswain, Mark Stanley, had returned to his cabin for a short break after cleaning the car deck upon arrival, and was still asleep when the harbour-stations call sounded and the ship dropped her moorings The first officer, Leslie Sabel, was required to stay on deck to make sure the doors were closed Sabel said he thought he saw Stanley approaching. He was seriously injured in the disaster and the court concluded that his evidence was inaccurate It is believed that under pressure to get to his harbour station on the bridge, he had left G deck with the bow doors open in the expectation that Stanley would arrive shortly The court also described the attitude of boatswain Terence Ayling, believed to have been the last person on G deck, as most unfortunate. Asked why he did not close the doors given there was no one else there to do it, he said it was not his duty. However the court praised his work in the rescue.

Captain David Lewry assumed that the doors had been closed since he could not see them from the wheelhouse owing to the ship's design, and had no indicator lights in the wheelhouse.

4.2 Indication of defective safety culture:

- The first officer had conflicting requirements: on deck to make sure the doors were closed and harbour-station on the bridge. The bosun (senior crewman supervises the other members of the ship's deck department) did not consider it his duty to check the doors.
- The safety critical task, i.e. closing the bow doors did not have an adequate assurance mechanism –assumptions were made that the doors would be closed.
- Request for CCTV or other equipment – no answer from the management.
- Furthermore, on several previous occasions ships had left harbour with their doors open and several Captains had asked for indicator lights to be installed but their requests had been ignored and even ridiculed by the company's management. A hazard analysis should have revealed this problem but no such analysis were completed.
- Responsibility for safety within the management structure was not clear despite the Department of Transport's recommendation in 1986 that "every company operating ships should designate a person ashore with responsibility for monitoring the technical and safety aspects of the operation of ships". There was no system for auditing the operation of the ships within the company.

5 Event: Challenger (1986)

5.1 Brief Description:

The Space Shuttle Challenger disaster occurred on January 28, 1986, when the NASA Space Shuttle orbiter Challenger (OV-099) (mission STS-51-L) broke apart 73 seconds into its flight, leading to the deaths of its seven crew members, which included five NASA astronauts and two Payload Specialists. The spacecraft disintegrated over the Atlantic Ocean, off the coast of Cape Canaveral, Florida at 11:38 EST (16:38 UTC). Disintegration of the vehicle began after an O-ring seal in its right solid rocket booster (SRB) failed at lift-off. The O-ring failure caused a breach in the SRB joint it sealed, allowing pressurized burning gas from within the solid rocket motor to reach the outside and impinge upon the adjacent SRB aft field joint attachment hardware and external fuel tank. This led to the separation of the right-hand SRB's aft field joint attachment and the structural failure of the external tank. Aerodynamic forces broke up the orbiter.

The disaster resulted in a 32-month hiatus in the shuttle program and the formation of the Rogers Commission, a special commission appointed by United States President Ronald Reagan to investigate the accident.

5.2 Indication of defective safety culture:

- The Rogers Commission found NASA's organizational culture and decision-making processes had been key contributing factors to the accident.
- NASA managers had known contractor Morton Thiokol's design of the SRBs contained a potentially catastrophic flaw in the O-rings since 1977, but failed to address it properly.
- They also disregarded warnings (an example of "go fever") from engineers about the dangers of launching, posed by the low temperatures of that morning, and failed to adequately report these technical concerns to their superiors.
- NASA did not know of Thiokol's earlier concerns about the effects of the cold on the O-rings, and did not understand that Rockwell International, the shuttle's prime contractor, viewed the large amount of ice present on the pad as a constraint to launch.

6 Event: Buncefield (2005)

6.1 Brief Description:

In the early hours of Sunday December 11, 2005, the Buncefield Oil Storage Depot in Hempstead, Hertfordshire, United Kingdom, had a series of explosions with at least one very large explosion. Buncefield site was collectively operated by a number of different companies. However, the incident was initiated in one of the tanks of Hertfordshire Oil Storage Ltd., which was a COMAH site housing about 200,000 metric tons of gasoline inventory. The initiating event of the incident was the overfilling of the tank and the subsequent release of cold gasoline with vapour cloud being ignited to cause a major explosion. The main explosion is speculated to have occurred around 6:01 a.m. The explosion and subsequently its resulting fire engulfed about 23 large atmospheric storage tanks, a major portion of the entire tank farm

6.2 Indication of defective safety culture:

- Systems for managing the filling of industrial tanks of petrol were both deficient and not fully implemented.
- An increase in the volume of fuel passing through the site put unsustainable pressure on those responsible for managing its receipt and storage, a task they lacked information about and struggled to monitor. The pressure was made worse by a lack of necessary engineering support and other expertise.

- A culture developed where keeping operations going was more important than safe processes, which did not get the attention, resources or priority status they required.
- Inadequate arrangements for containment of fuel and fire-water to protect the environment.

7 Event: Columbia (2003)

7.1 Brief Description:

The Space Shuttle Columbia disaster occurred on February 1, 2003, when Columbia disintegrated over Texas and Louisiana as it re-entered Earth's atmosphere, killing all seven crew members. During the launch of STS-107, Columbia's 28th mission, a piece of foam insulation broke off from the Space Shuttle external tank and struck the left wing. A few previous shuttle launches had seen minor damage from foam shedding but some engineers suspected that the damage to Columbia was more serious. NASA managers limited the investigation, reasoning that the crew could not have fixed the problem if it had been confirmed.
When Columbia re-entered the atmosphere of Earth, the damage allowed hot atmospheric gases to penetrate and destroy the internal wing structure, which caused the spacecraft to become unstable and slowly break apart.
Following protocols established after the loss of Challenger, an independent investigating board was created immediately after the accident; the Columbia Accident Investigation Board, or CAIB. On August 26, the CAIB issued its report on the accident.

7.2 Indication of defective safety culture:

The report was highly critical of NASA's decision-making and risk-assessment processes. It concluded the organizational structure and processes were sufficiently flawed and that a compromise of safety was expected no matter who was in the key decision-making positions. An example was the position of Shuttle Program Manager, where one individual was responsible for achieving safe, timely launches and acceptable costs, which are often conflicting goals.
The CAIB report found that NASA had accepted deviations from design criteria as normal when they happened on several flights and did not lead to mission-compromising consequences. One of those was the conflict between a design specification stating that the thermal protection system was not designed to withstand significant impacts and the common occurrence of impact damage to it during flight. The board made recommendations for significant changes in processes and organizational culture.

8 Event: Enschede (2000)

8.1 Brief Description:

On May 13 about 100 tonnes of fireworks and other explosives detonated after a fire in the factory of S.E. Fireworks, situated in the middle of the working class housing estate of Mekkelholt in the northern Dutch city of Enschede. The blast was felt up to 30 kilometres away. Over 2,000 members of the community, most of whom had been unaware of the existence of the factory, had to be evacuated, and hundreds of homes were destroyed. Investigations into the cause of the explosion have brought to light a multitude of facts testifying to the negligence of the factory owners and the authorities.

8.2 Indication of defective safety culture:

- The decision what to do when hazardous materials are involved in a fire may be very complex. It is important to agree on tactical response long before an incident, with all parties that will respond.

- Its real causes flow from the fact that the firm responsible was able to stockpile, apparently unhindered, large quantities of dangerous materials stacked closely together. Furthermore it seems the firm was allowed to carry on its business regardless of the most basic safety standards. After a big extension of the stored explosives, safety measures were not implemented to keep up with this scale of development.

9 Event: Texas City (2005)

9.1 Brief Description:

On March 23, 2005, a massive explosion occurred at the BP Texas City Refinery, in Texas City, Texas, USA. This accident resulted in 15 fatalities and 180 injuries and was considered as one of the most catastrophic industrial accidents in U.S. history. The explosion happened at approximately 1:20 p.m. during the startup of a hydrocarbon isomerization unit when a distillation tower flooded with hydrocarbons, caused over pressurization and relief devices to open resulting in a geyser-like release of flammable liquid from the vent stack that was not equipped with a flare. Most victims at the time of the incident were located in office trailers located near to the blowdown vessel. In addition to casualties, houses and building located as far as three quarters mile away from the refinery were significantly damaged. The financial losses from this accident exceed $1.5 billion

9.2 Indication of defective safety culture:

- Andrew Hopkins: culture of BP, and of Texas City in particular was a culture of blindness to major risk.
- Leadership issues – only good news flowed upwards. Lack of practice of mindful leadership. For example, they failed to learn lessons from past accidents.
- Disciplining the workers – not only were there external legal processes that blamed BP, there were also internal processes in which BP blamed its own employees from top to bottom of the organization. Soon after the accident, six workers were terminated “for not fulfilling accountabilities”. The one person who largely escaped the formal accountability processes following the accident was the CEO.
- Diluted message/response to/from the top. Ineffective implementation of process safety policies and procedures, no effective management of change.
- No process safety goals = underreporting of incidents and near misses.
- Compliance audits were regulatory oriented not performance oriented.
- Reliance on low injury rate as sole safety KPI
- BP takeover of AMOCO, lack of oversight, cultural mismatch; budget cuts – inadequate staffing of the control room.
- Miscommunication problem – at a management meeting held on the morning the start-up was scheduled to take place, the decision was made *not* to proceed, because the storage tanks that received the heavy liquid were full. However, operators were not told of this decision and went ahead with the startup, as originally planned. Further to this, at shift handover the operators log book was brief and uninformative and there was no oral communication either.

10 Event: Tolouse (2001)

10.1 Brief Description:

At 10.17 a.m. on 21 September 2001 a severe explosion occurred in Shed 221, a temporary storage of downgraded ammonium nitrates at the AZF industrial site in Toulouse, France. The detonation, felt several kilometer away, corresponded to a magnitude of 3.4 on the Richter scale. Significant dust fallout from the installations and a 7 m deep crater (65x45m) were observed outside the plant.

10.2 Indication of defective safety culture:

- The safety report of the AZF factory did not take into account the downgraded ammonium nitrates store since it was considered as less dangerous (because of the smaller quantity stored). The safety report did not describe each possible accident scenario.
- On the AZF industrial site, 25 subcontracting companies worked continuously (100 subcontractors every day versus 250 employees for a total of 469 employees). Three different subcontracting companies worked in the warehouse (the downgraded AN was picked up, unloaded and removed by them) and the maintenance of this warehouse was carried out by another subcontractor. Cidecos-conseil, a consulting company, hired by AZF, carried out an organisational investigation. They consider that the subcontracting was a "determining factor" of the accident. One consequence of the operational subcontracting of the warehouse is a disengagement of AZF employees for its operational management; AZF has lost the control (in INERIS interviews, inadequate communication has been identified) of some activities carried out by the subcontractors.

11 Event: Seveso (1976)

11.1 Brief Description:

At 12.37 pm on Saturday July 9, 1976, a bursting disk ruptured on a chemical reactor at the works of the Icmesa Chemical Company at Meda near Seveso, a town of about 17,000 inhabitants some 15 miles from Milan. A white cloud drifted from the works and material from it settled out downwind. Among the substances deposited was a very small amount of TCDD, one of the most toxic chemicals known. There followed a period of great confusion due to lack of communication between the company and the authorities and the latter's inexperience in dealing with this kind of situation. Over the next few days in the contaminated area, animals died and people fell ill. A partial and delayed evacuation was carried out. In the immediate aftermath, there were no deaths directly attributable to TCDD, but a number of pregnant women who had been exposed had abortions.

11.2 Indication of defective safety culture:

- The operators did not observe the standard operation method.
- The reactor was constructed without any knowledge of the possibility of a runaway reaction, so no countermeasures for preventing an abnormal temperature rise were taken. Furthermore, in the design of the safety equipment, no consideration was given to the protection of the environment.
- The recommendation and later the order for evacuation of the local inhabitants were delayed. It took the company five days to recognize the existence of dioxin, and furthermore, as the company spent more time on reconfirmation, they did not inform the local government of the existence of dioxin until 10 days after the accident.

12 Event: Piper Alpha (1986)

12.1 Brief Description:

At 10.00 p.m. on July 6, 1988, an explosion occurred in the gas compression module of the Piper Alpha oil production platform in the North Sea. A large pool fire took hold in the adjacent oil separation module, and a massive plume of black smoke enveloped the platform at and above the production deck, including the accommodation. The pool fire extended to the deck below, where after 20 min it burned through a gas riser from the pipeline connection between the Piper and Tartan platforms. The gas from the riser burned as a huge jet flame. Most of those on board were trapped in the accommodation. The lifeboats were inaccessible due to the smoke. Some 62 men escaped, mainly by climbing down knotted ropes or by jumping from a height, but 167 died, the majority in the quarters.

The Cullen Inquiry was set up in November 1988 to establish the cause of the disaster. It released its report Public Inquiry into the Piper Alpha Disaster (short: Cullen Report) in November 1990.

12.2 Indication of defective safety culture:

- Conversion of the platform from oil to oil and gas production meant that the safety concept of separating the most dangerous operations from personnel areas was broken (Gas compression was next to the control room).
- Fire pumps were in manual mode whenever divers were in the water (ca. 12 hrs a day in summer). Despite an earlier audit recommending automatic mode unless divers were in the vicinity of the seawater intakes.
- Poor management of change and permit to work practice meant that an attempt was made to restart a pump which was being overhauled and had had the safety valve removed – Permits were poorly managed.
- Two years previously Occidental (the operator) management ordered a study, the results of which warned of the dangers of these gas lines. Because of their length and diameter, it would have taken several hours to reduce their pressure, so that it would not have been possible to fight a fire fuelled by them. Although the management admitted how devastating a gas explosion would be, Claymore and Tartan (gas production platforms feeding into Piper Alpha) were not switched off with the first emergency call.
- The Cullen Inquiry was critical of Piper Alpha's operator, Occidental, which was found guilty of having inadequate maintenance and safety procedures

13 Event: Ghislenghien (2004)

13.1 Brief Description:

On July 30, 2004 a high-pressure natural gas pipeline operated at a pressure of 70 bar ruptured following recent third party damage. Twenty-four people died as a result and 150 survivors were hospitalised, most with severe burns.

It is thought that damage to the pipeline occurred during the final stages of a car park construction project. This work had been notified to the Pipeline operator, Fluxys, and one of their operatives had regularly attended the site through the course of the project. Damage to the pipeline probably occurred as a mechanical soil stabiliser was driven over it or nearby. This resulted in several evenly spaced (but not full depth) gouges in the steel wall of the pipeline. Two weeks after the completion of the car park gas pressure was increased in the pipeline, which then ruptured with the fault centred on a 350 mm long gouge. Other contributing factors to the accident may have been a reduced cover over the pipeline as a result of levelling, the way information was passed down the sub-contracting chain to workers and the frequency and adequacy of supervision by the pipeline operator at the site.

13.2 Indication of defective safety culture:

- Inadequate assurance of the protective safety zones parallel to the high pressure pipeline.
- Inadequate understanding of the potential for damage during the construction and the consequences for the pipeline integrity.