Refineries and Associated Plant: Three Accident Case Studies

"Optimism and stupidity are nearly synonymous." Hyman G. Rickover.

"Safety doesn't happen by accident." Anonymous (Safety slogan)

"Responsibility is a unique concept... You may share it with others, but your portion is not diminished. You may delegate it, but it is still with you... If responsibility is rightfully yours, no evasion, or ignorance or passing the blame can shift the burden to someone else. Unless you can point your finger at the man who is responsible when something goes wrong, then you have never had anyone really responsible." Hyman G. Rickover.

"*The big accidents are just waiting for the little ones to get out of the way."* Carolyn Merritt.

"It should not be necessary for each generation to rediscover principles of process safety which the generation before discovered. We must learn from the experience of others rather than learn the hard way. We must pass on to the next generation a record of what we have learned." Jesse C. Ducommun

This note presents a brief overview of refineries and their accident record, followed by three accident case studies:

1. A pipeline rupture and fire in Washington State, USA, on 10th June 1999.
2. An accident at the coking plant of the Anacortes refinery, Puget Sound, Washington State, USA, on 25th November 1998.
3. The BP Texas City refinery fire and explosion on 23rd March 2005.

OIL REFINERIES – A VERY BRIEF INTRODUCTION

There are currently about 700 operational oil refineries in the world. A medium-sized refinery can typically process 100000 barrels of oil per day. Jamnagar refinery in Gujarat, India, is currently the biggest refinery in the world; it alone processes more than one per cent of global output. The top 10 biggest refineries in the world are currently as follows:

	Location	Operator	Capacity (barrels per day)
1	Jamnagar, Gujarat, India	Reliance Industries	1,240,000 bpd
2	Paraguana, Venezuela	PDVSA	940,000 bpd
3	Ulsan, South Korea	SK Energy	850,000 bpd
4	Yeosu, South Korea	GS-Caltex (Chevron/GS Holdings)	730,000 bpd
5	Ulsan, South Korea	S Oil (Saudi Aramco/Hanjin Group)	669,000 bpd
6	Jurong Island, Singapore	Exxon Mobil	605,000 bpd
7	Baytown, Texas, USA	Exxon Mobil	572,500 bpd
8	Ras Tanura, Saudi Arabia	Saudi Aramco	550,000 bpd
9	Baton Rouge, Louisiana, USA	Exxon Mobil	503,000 bpd
10	Texas City	BP (sold to Marathon 2012)	467,720 bpd

Refineries are high-technology process plants, and the cost of building a large modern refinery is several billion US dollars. The main processes carried out in simple refineries typically include the following:

Refinery process	**Function**	**Products**
Crude oil storage	*Self-explanatory*	-
Desalter	Removes impurities from crude oil	Clean crude oil
Crude oil distillation column	Separates crude oil into light and heavy components	Naphtha*, jet fuel, diesel, residue
Hydro-treating	Remove sulphur	Desulphurised products
Catalytic reforming, platforming or isomerisation	Converts naphtha to gasoline	Gasoline/petrol
Residual Fluid Catalytic Cracking (RFCC)	Takes residue from distillation column and produces useable product	Gas, LPG, gasoline, diesel, slurry
Thermal conversion and delayed coking plant	Takes heavy oil residue and converts it to coke (batch production only)	Coke
Product storage and blending	*Self-explanatory*	Blended products to meet market needs

*Naphtha is defined as the fraction of hydrocarbons in petroleum boiling between 30 °C and 200 °C

Refineries are undoubtedly very hazardous, high risk facilities. The hazards and risks mainly arise because they process hydrocarbons at high temperature and high pressure:

> A leak of high-pressure gaseous hydrocarbon can, if it ignites immediately, produce a jet fire which can impinge on other process plant and then escalate to become a large conflagration, in a similar fashion to the Piper Alpha accident.
>
> An un-ignited leak of high-pressure gaseous hydrocarbon can quickly generate a large, inflammable cloud which may drift until it finds an ignition source, and it can then yield a vapour cloud explosion.
>
> A spill of liquid hydrocarbon may catch fire and yield a pool fire.

Hence, accidents in refineries can be amongst the most devastating industrial accidents. Marsh Risk Consulting[1] publishes data on major accidents, including refinery accidents, giving the insured losses in each case. (*Total* losses may, of course, exceed *insured* losses.) The following table is a compendium of refinery accident data between 1972 and 2011 from the Marsh reviews for 2001 and 2011, and it shows that at least 53 major refinery accidents occurred during the 40 year period covered. Many of these accidents did cause injuries and deaths, although the table does not list them.

There can be no guarantee of the completeness of these data, in particular because Chinese and pre-1990 Soviet and Eastern European data are not available. It is also noted that data in the period 1972 to 1979 are strangely absent.

[1] http://uk.marsh.com/ProductsServices/MarshRiskConsulting.aspx

However, the point is made; refineries are almost uniquely difficult places to operate safely. If we allow for some credible under-reporting of accidents, and assuming for the purposes of argument that the number of refineries worldwide has remained broadly constant at about 700 over the timescale (production has increased but bigger plants will have replaced smaller ones), with each plant having something like a fifty-year operational life, then we can derive a rough rule-of-thumb as follows: **Any given refinery has about a one in ten chance of suffering a major accident during its operational lifetime.**

Refinery Major Accident Losses, 1972-2011

	Date	Location	Type of accident (**shaded = natural causes**)	Value of Insured Losses (2001 USD) (*** 2011 USD**)
1	21 July 1979	Texas City, Texas	Vapour cloud explosion	$47 million
2	1 Sept 1979	Deer Park, Texas	Explosion	$138 million
3	20 Jan 1980	Borger, Texas	Vapour cloud explosion	$65 million
4	20 Aug 1981	Shuaiba, Kuwait	Fire	$73 million
5	7 Apr 1983	Avon, California	Fire	$73 million
6	23 July 1984	Romeville, Illinois	Explosion	$275 million
7	15 Aug 1984	Las Piedras, Venezuela	Fire	$89 million
8	22 Mar 1987	Grangemouth, UK	Explosion	$107 million
9	5 May 1988	Norco, Louisiana	Vapour cloud explosion	$336 million
10	10 Apr 1989	Richmond, California	Fire	$112 million
11	5 Sept 1989	Martinez, California	Fire	$62 million
12	18 Sept 1989	St Croix, Virgin Islands	Hurricane	$168 million
13	24 Dec 1989	Baton Rouge, Louisiana	Vapour cloud explosion	$89 million
14	1 Apr 1990	Warren, Pennsylvania	Explosion and fire	$30 million
15	3 Nov 1990	Chalmette, Louisiana	Vapour cloud explosion	$25 million
16	30 Nov 1990	Ras Tanura, Saudi Arabia	Fire	$40 million
17	12 Jan 1991	Port Arthur, Texas	Fire	$31 million
18	3 Nov 1991	Beaumont, Texas	Fire	$18 million
19	3 Mar 1991	Lake Charles, Louisiana	Explosion and fire	$28 million
20	13 Apr 1991	Sweeney, Texas	Explosion	$45 million
21	10 Dec 1991	Westphalia, Germany	Explosion and fire	$62 million
22	8 Oct 1992	Wilmington, California	Explosion and fire	$96 million
23	16 Oct 1992	Sodegaura, Japan	Explosion and fire	$196 million
24	9 Nov 1992	La Mede, France	Vapour cloud explosion	$318 million
25	2 Aug 1993	Baton Rouge, Louisiana	Fire	$78 million
26	25 Feb 1994	Kawasaki, Japan	Fire	$41 million
27	24 July 1994	Pembroke, UK	Fire	$91 million
28	16 Oct 1995	Rouseville, Pennsylvania	Fire	$46 million
29	24 Oct 1995	Cilacap, Indonesia	Explosion and fire	$38 million
30	27 Jan 1997	Martinez, California	Explosion and fire	$22 million
31	14 Sept 1997	Visakhapatam, India	Explosion and fire	$64 million
32	9 June 1998	St John, New Brunswick	Explosion and fire	$66 million
33	26 Sept 1998	Pascagoula, Mississippi	Hurricane	$357 million
34	6 Oct 1998	Berre l'Etang, France	Fire	$23 million
35	19 Feb 1999	Thessaloniki, Greece	Explosion and fire	$40 million
36	25 Mar 1999	Richmond, California	Explosion	$79 million
37	17 Aug 1999	Korfez, Turkey	Earthquake	$210 million
38	2 Dec 1999	Sri Racha, Thailand	Explosion	$37 million
39	25 June 2000	Mina Al-Ahmadi, Kuwait	Explosion and fire	$433 million
40	9 Apr 2001	Aruba, Caribbean	Fire	$134 million
41	16 Apr 2001	Killingholme, UK	Explosion and fire	$82 million
42	23 Apr 2001	Carson City, California	Fire	$124 million
43	28 Apr 2001	Lemont, Illinois	Fire	$36 million
44	21 Sept 2001	Lake Charles, Louisiana	Fire	$52 million
45	22 Nov 2002	Mohammedia, Morocco	Explosion and fire	$190 million*
46	6 Jan 2003	Fort McMurray, Alberta	Explosion and fire	$170 million*
47	4 Jan 2005	Fort McKay, Alberta	Explosion and fire	$150 million*
48	23 Mar 2005	Texas City, Texas	Explosion and fire	$250 million*
49	12 Oct 2006	Mazeikiu, Lithuania	Explosion and fire	$170 million*
50	16 Aug 2007	Pascagoula, Mississippi	Explosion and fire	$230 million*
51	18 Feb 2008	Big Spring, Texas	Explosion and fire	$410 million*
52	12 Sept 2008	Galveston, Texas	Hurricane^	$540 million*
53	6 Jan 2011	Fort McKay, Alberta	Explosion and fire	$600 million*

^This refers to Hurricane Ike, which affected six refineries in the Galveston area. The loss data relate to the worst affected single refinery.

CASE STUDY 1: PIPELINE RUPTURE AND FIRE, WASHINGTON STATE, USA, 10TH JUNE 1999

This accident involved the rupture of a buried gasoline (petrol) pipeline.[2] The basic facts are simple yet tragic. The buried pipeline was 16 inches in diameter (40 centimetres), and the rupture released about 237000 gallons (more than a million litres) of gasoline into a river creek flowing through Whatcom Falls Park in Bellingham, Washington. The park is a woodland area in an otherwise mostly residential suburb, a few miles south of the US-Canadian border.

The gasoline from the pipe flowed down the river creek for about 90 minutes before finding a source of ignition and catching fire. One and a half miles of the river creek burned, and two ten-year old boys and an eighteen-year old man were killed, with a further eight people injured. Property damage was estimated at $45 million.

The NTSB report, although very detailed, does not name any of the actors in the long sequence of events which led to the accident, probably because legal action was still pending.

As stated above, the facts are simple and tragic. The accident was undoubtedly unusual – a massive fire in a public park on a Thursday afternoon in summer. The surprising things about this accident in the current context are, however, as follows: the number of missed opportunities to prevent the accident; the number of different people and organisational entities that failed in their responsibilities; and the length of time between the first failings and the eventual accident.

The pipeline was owned and operated by the Olympic Pipeline Company, but operation was subcontracted to another company, Equilon, although the 2002 NTSB report says that Equilon disputed this assertion - Equilon said it was not responsible for pipeline operations and that it only loaned employees to Olympic.

[2] US National Transportation Safety Board, “Pipeline rupture and subsequent fire in Bellingham, Washington, June 10, 1999”, NTSB/PAR-02/02, 8 October 2002

Fig 1: Whatcomb Falls Park, June 1999, after the fire in the river creek (NTSB)

The Olympic pipeline system consisted of a network of some 400 miles of pipelines transporting refined petroleum products from refineries in northwest Washington State to various locations as far as Portland, Oregon. The pipeline system included a length of pipeline between Ferndale and Bayview, which passed through Whatcom Falls Park; this was a section of a longer pipeline used for transferring gasoline from a refinery at Cherry Point in northern Washington southwards towards a large storage depot at Renton near Seattle.

The section of pipeline in Whatcom Falls Park where the accident occurred was installed in 1964, but was re-routed in 1966 because of the construction of a water treatment plant (owned by Bellingham city council) that is situated in the middle of the park. The pipeline was made of 0.312 inches thick steel. It was hydrostatically tested to 1820 pounds per square inch (124 bar). Maximum operating pressure was eighty per cent of the hydrostatic test pressure.

As part of further improvements to the water treatment plant in the early 1990's, Bellingham city council personnel were required to confirm the exact location of the gasoline pipeline using a process called 'potholing'. This consisted of, first, the rough location of the pipeline with a magnetic detector, then probing with a steel bar, and finally by hand excavation. Olympic's own personnel were present when the council crew carried out this work on different occasions in 1993.

Bellingham council placed contracts with two companies (IMCO General Construction Inc and Barrett Consulting Group, subsequently known as Earth Tech) to implement the modifications at the water treatment plant.

The arrangements were supposed to be that Olympic personnel would be present whenever excavation happened within "ten to fifteen" feet of the pipeline, and that all excavation within two feet of the pipeline would be only by hand; that is, no mechanical diggers were to be used close to the pipeline. Olympic inspectors also made unannounced visits to the work site on a regular basis, more than once per week.

However, the NTSB report concluded that excavation around the Olympic pipeline occurred in August 1994, without Olympic inspectors being present, in order to lay a new water pipeline which crossed over the gasoline pipeline. A subcontractor to IMCO told the accident investigators that he heard the gasoline pipeline being struck by a backhoe - a powered mechanical excavator - during the project, probably on 11th August 1994, when an Olympic representative was not present, and that IMCO personnel decided not to notify Barrett or Olympic. The subcontractor said that IMCO personnel coated the damaged area of pipeline with a mastic coating before backfilling over it. A labourer working for IMCO also recalled IMCO hitting the pipeline. All other IMCO employees denied this account.

Next, Olympic had placed a contract with Tuboscope Linalog Inc to carry out 5-yearly remote inspections of the pipeline along its entire length using a magnetic flux inspection tool which determines steel thickness of the pipeline wall. (Such a device is called a 'pig' in the oil industry – it is passed along the pipeline and records data which can be analysed later off-line.) An inspection in 1991 showed no defects in the area of the later failure. An inspection on 18th March 1996, however, did show anomalies in that area. These anomalies were assessed by Tuboscope and judged to be small enough not to matter; however, the assessment methodology they used was developed by the American Society of Mechanical Engineers (ASME) specifically for corrosion damage and not mechanical damage. For mechanical damage, the geometry of the defect may be much more precisely defined, and the resolution of magnetic flux inspection may underestimate the severity of the damage.

A separate incident on an Olympic pipeline led, on 17th September 1996, to the Washington Department of Ecology ordering Olympic to carry out further remote inspection work, including the use of a diverse (mechanical) measurement technique called 'caliper tools'. This led, on 15th January 1997, to another inspection of the pipeline done by a different company, Enduro, using the caliper tool inspection technique that was specifically aimed at identifying mechanical damage. Near the site of the future pipeline rupture, a 0.45 inch "sharp defect" was reported at the same point where Tuboscope had detected an anomaly. The "sharp defect" at the future rupture site was reported as being 23 per cent of wall thickness.

In May 1997, Olympic began exposing locations where anomalies had been measured that might be more than 20 per cent of pipewall thickness.

The future rupture site was declared by an employee of Olympic's construction supervisor to be "too wet" to permit excavation at that time. This was reported to a junior engineer in Olympic, who says

he was told they would “go back and try again when the area was dry”. Tragically, no further action was taken before the accident.

(After the accident, inspection of the failed section of pipeline showed “numerous gouges and dents”. The pipeline was about 10 feet (3 metres) underground at the failure location. The failed section of pipe had a tear-like fracture some 27 inches (68 centimetres) long with a maximum separation of 7 inches (17 centimetres).)

Meanwhile, several miles away at Bayview, in December 1998, Olympic completed construction of a new terminal with a storage capacity of 500000 barrels (82 million litres). The contractor was Jacobs Engineering Inc. The gasoline flowed southwards along the pipeline, through Whatcom Falls Park, to the new terminal.

The new Bayview Terminal had a design operating pressure of 740 pounds per square inch (50 atmospheres or 50 bar) and the accident pipeline was designed for much higher pressures, so it was necessary to install pressure-reduction equipment where the pipeline joined the new terminal. There were three layers of control and safety devices: (i) a control valve to throttle the incoming flow, (ii) a pilot-operated spring-loaded relief valve, and (iii) three motor-operated isolation valves. This triple-barrier approach is sound design – a control system, backed-up by two protection systems (the relief valve and the isolation valves). In the event of a problem with the control valve, the relief valve should operate quickly, and only in the event of a fault with the relief valve should the isolation valves ever have been required to operate.

The three safety-critical motor-operated isolation valves operated as follows: two isolated the pipeline from the new terminal, and the third opened the pipeline into a receiver vessel to divert the source of high pressure.

During commissioning of the new terminal, on the night of 16th-17th December 1998, it was discovered that the pilot-operated spring-loaded relief valve had been wrongly specified – it opened at 100 pounds per square inch (6.9 bar) instead of the intended 700 pounds per square inch (48 bar). The springs in the pilot valve were replaced with spares, but the replacement springs were actually identical. Furthermore, in the process of replacing the springs, the pilot-operated spring-loaded relief valve was actually rendered unreliable. Finally, to make things even worse, no proper re-testing was carried out to see if the valve was working properly and at its correct relief pressure.

There still should have been opportunities to diagnose and rectify the problems with the relief valve: After the new Bayview Terminal went into service on 17th December 1998, there were operational difficulties. Pressure control continued to be a problem, and the motor-operated isolation valves operated 41 times because of high-pressure within the terminal. Each time this happened, a pressure pulse was sent back along the pipeline towards the future accident site. Some of these pressure pulses exceeded 1300 psig. Because the isolation valves were classified as “safety devices”, the closure of these valves should have triggered management concerns – their closures clearly implied that something was wrong with both the pressure control valve and the relief valve. However, no concerted effort was made to find out what was wrong to cause the isolation valves to keep operating, or to find out why with the relief valve was not opening.

The final stage in the sequence of events happened on the day of the accident, 10th June 1999.

The Olympic pipeline was controlled using a Supervisory Control and Data Acquisition (SCADA) system – in other words, a computerised control system. This system used plant sensors and actuators connected to two DEC VAX computers, with one primary computer, and one backup. The computers received data from the sensors and the actuators every 3 to 7 seconds. As is normal for systems like this, the operators used screens with pre-programmed formats on which the data was displayed, and the operator could interact with the system by mouse click. The system also recorded and stored all data and commands made.

Among its other functions, the SCADA system sent control signals to the control valve which throttled flow incoming from the north.

At about 1500 hours on the afternoon of the accident, 10th June 1999, the SCADA system's response time slowed significantly following an upload of plant data records into the SCADA historical database. This data upload was done by the computer system administrator. The SCADA system's problems grew more pronounced over a period of about 20 minutes, and for a while the system became completely unresponsive; it was unable to send control signals to any of the equipment on the pipeline system. This meant that the pressure control valve and the isolation valves were not operational.

Although the SCADA fault that caused the system to be unresponsive could not be replicated or explained subsequently, the computer system administrator had been carrying out development work on the live system at the time. This is extremely bad practice. Olympic personnel were using the *operational* pipeline SCADA system as the test bed to develop improvements to its database; normal good practice should be to first test changes on a separate off-line system.

Finally, at the same time as the computer system administrator's on-line development work caused the SCADA system to stop working, the pipeline system controller switched delivery points, which led to a significant pressure pulse through the system.

This pressure pulse went through the system; the SCADA system was unresponsive, so the isolating valves did not operate; and the pipe ruptured at 1528 hours, at the point where a defect remained from the 1994 excavation work.

So, the complete timeline of missed opportunities and mistakes that led to this accident can be summarised as follows:

1. The pipeline was damaged during excavation work carried out IMCO probably on 11th August 1994. This damage was not reported to Olympic.
2. A magnetic inspection carried out on 18th March 1996 did show anomalies in the region of the eventual pipe rupture. The anomalies were assessed to be insignificant, but the assessment technique was intended for corrosion damage and not mechanical damage.

3. Another inspection was carried out on 15th January 1997 using a different inspection technique. A "sharp defect" was reported near the eventual failure site. However, the ground was too wet to allow excavation and it was agreed to excavate later when it was drier. No subsequent excavation took place.
4. A new gasoline terminal was installed some miles downstream and commissioned on 17th December 1997. The pressure relief valve was not set up properly so it did not function, and it was not tested so the improper set-up was not revealed.
5. Because the relief valve was not opening when required, there were 41 separate occasions when the isolation valves operated because of overpressure. None of these was investigated.
6. On the day of the accident, 10th June 1999, the computer system administrator had doing software development work on the live SCADA system which controlled the entire pipeline system, including the isolation valves. For reasons unknown, this development work caused the whole SCADA control system to become unresponsive. This occurred at the same time as the pipeline system controller was switching delivery points, which led to a pressure pulse going through the system.

The result of all the above was that a pressure pulse occurred, but the relief valve had never worked, and the control system was unresponsive, so the isolation valves did not operate. The pipeline pressure rose and the pipe ruptured at the defect caused by the excavation damage in August 1994, allowing one million litres of gasoline to flow down a river creek on a summer afternoon, where it caught fire and killed three people.

The key question for determining the root causes of accidents is "To when would I have to travel back in a time machine to prevent this accident happening?" By this rule, all of the above six points count as root causes.

Probable cause of the accident was ascribed to:

1. Damage done to the pipe by IMCO General Construction Inc during the 1999 water treatment plant modification project.
2. Olympic Pipeline Company's inadequate evaluation of on-line pipeline inspection results.
3. Olympic Pipeline Company's failure to test, under approximate operating conditions, all safety devices associated with the new Bayview Terminal.
4. Olympic Pipeline Company's failure to investigate and correct the conditions leading to the repeated unintended closing of the Bayview inlet isolation valve.
5. Olympic Pipeline Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline, which led to the system becoming non-responsive at a critical time during pipeline operations.

This was a long and sorry tale of many people, over five years, all of whom failed to carry out their duties properly. It is difficult from the report to be sure exactly how many people were involved in unsafe acts and poor decisions, but there must have been at least twelve individuals involved. Mostly, their failings were simply laziness, indifference, or cynicism. There was no evidence to suggest time pressure, or financial pressure. It was just that people *couldn't be bothered*. No-one cared about what they were doing, and as a result two ten-year old boys and an eighteen-year old man were killed.

Maybe I am being too harsh. Perhaps the people involved simply didn't recognise that this sort of accident could happen. Maybe, instead, all those involved thought the only risk was that there might be a pipeline leak – and not a gross rupture - and that the worst that could happen was a little localised environmental damage, instead of fatalities. After all, this was a very unusual accident; it just so happened that the pipeline rupture was large, and that it ruptured near a river creek, and that the gasoline was able to flow un-ignited for over an hour, so that the size of the area affected (when it eventually did find an ignition source) included one and a half miles of the river creek. In which case, their blame can be ascribed to ignorance, or at least lack of imagination, and not indifference.

However, I am reminded of the legal principle that *Ignorantia juris non excusat* – 'Ignorance of the law is no excuse'. In safety, there should perhaps be a principle that 'Inability to imagine the consequences of your actions (or inactions) is no excuse'.

CASE STUDY 2: EQUILON ANACORTES REFINERY COKING PLANT ACCIDENT, 25TH NOVEMBER 1998

This accident was an unusual, multiple fatality refinery accident, which was actually relatively minor in terms of financial losses so it does not even appear on the above table of refinery accidents .

It is an unusual accident because if doesn't involve hydrocarbon liquids or gases under pressure. The accident occurred at one of the coking drums, where coke is produced from long-chain hydrocarbon residues in a thermal cracking process.

It is also unusual as an example of 'group-think', where a number of experienced people in a slightly unusual situation persuaded themselves to do something that, with hindsight, seems to be completely crazy.

The delayed coking unit is where heavy oil residues are converted into coke which can then be used, say, as fuel for electricity generation. The heavy oil residues are passed through a furnace – a 'thermal conversion unit' where the long chain molecules are 'cracked' - and into large coke drums where the coke formation actually takes place. The term 'delayed' is used to indicate the coke formation does not take place in the furnace (which would lead to a plant shutdown) but, instead, the coke crystallises in the large coke drums after the furnace.

The coke drums are filled and emptied daily in a batch process, although the rest of the refinery operates more-or-less continuously. Like most plants of this sort, the Anacortes refinery had two large coke drums, Drums A and B, stainless steel drums each about 20 metres tall and each with

adequate capacity for one day's coke production. The process conditions in the operational coke drum are 450 to 500 degrees C and 20 to 30 bar pressure. Only one coke drum is on-line at any time; the other is off-line, being emptied or standing by. Vapour passes from the top of the operational coke drum to a fractionating column, where the gaseous products are separated into the desired fractions. The residue remains in the coke drum to crack further until only the coke is left.

This description of the accident is taken from two sources: a NASA presentation which is available on-line, and a file on the historylink website.[3]

A powerful storm hit western Washington State on 23rd November 1998. It caused widespread damage and also interrupted the electricity supplies to the Equilon Anacortes refinery in Puget Sound for about two hours. This meant, in particular, that the delayed coking unit had to be re-started. Drum A was about one hour into a routine charging cycle when the power interruption occurred.

Under normal conditions, at the end of the cycle, the drum would be cooled with steam first and then water. Once the temperature was low enough, a Permit to Work would be issued and the top of the vessel would be unbolted and removed. The mass of coke in the vessel is then cut up using high-pressure hoses; the coke and water then can be discharged out of the bottom the vessel.

In this case, however, because of the power interruption, the Charge Line at the bottom of the vessel, through which the coke would normally flow out of the drum at the end of the cycle, was clogged with coke that had formed during the power cut. This meant that the operators were unable to put steam or water into the drum to cool the coke. There were some 46000 gallons (about 200 m^3) of hot coke remaining in the drum.

[3] See nsc.nasa.gov/SFCS/SystemFailureCaseStudyFile/Download/115 and also http://www.historylink.org/_content/printer_friendly/pf_output.cfm?file_id=5618

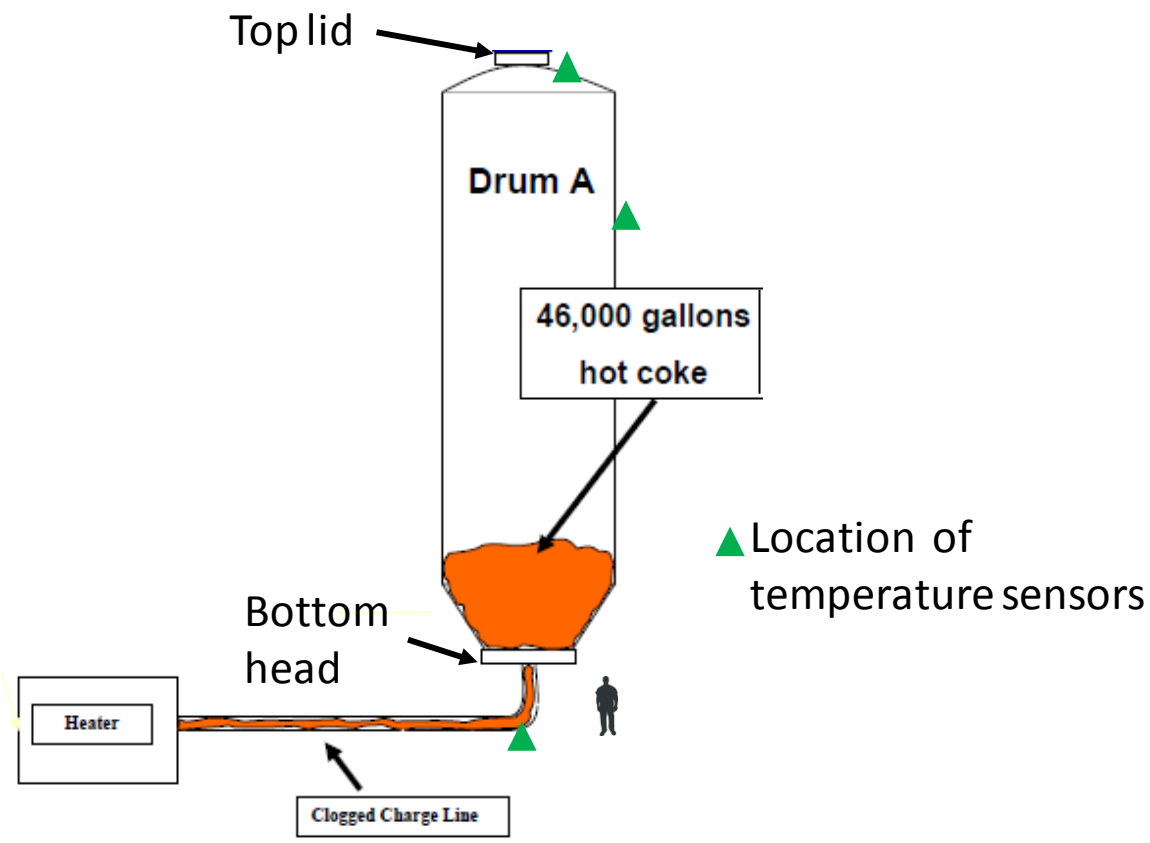

Fig 2: Drum A in the coking plant at Equilon Anacortes refinery, 25th November 1998. Six people standing under the bottom head when it was unbolted and removed were killed by hot coke and burning heavy oil residue.

Electric power was restored and at about 1000 hours on 24th November steam was also available. The operators made attempts to clear the clogged charge line. They believed - although there was no evidence to confirm this had happened – that steam had made its way into Drum A. Instead, it is likely that pressure relief valves were actually diverting the steam into a blowdown system.

At the afternoon meeting to discuss the instructions to the nightshift, it was agreed to tell nightshift that the drum was cooling without the need for water, and that dayshift would remove the head from the drum the following day, Wednesday 25th November.

There were no credible indications of the temperature of the coke inside the vessel. The only temperature sensors were on the outside of the drum. Although the operators believed that steam had passed into the drum, no steam had actually been admitted to the drum. Furthermore, no attempt had been made to put water into the drum. Nevertheless, on the morning of 25th November, the foreman and operators reviewed the drum temperature sensors and concluded that the drum contents had cooled sufficiently. It appears that Equilon plant management were also involved in the decision to go ahead, and a Permit to Work was issued for a specialist contractor, Western Plant Services, to open up the drum. Wearing oxygen masks, workers removed the top lid from the drum safely.

At about 1330 hours, only 37 hours after the loss of power which interrupted the normal coke batch production sequence, and without any further effort to determine the temperature of the coke (even after removing the top lid from the drum), the bolts holding the bottom head in place were removed and a hydraulic lift began to lower the head from the bottom of the coking drum. Six men were standing directly under the drum; they expected to find a congealed mass of crude oil residue, but the unit was far hotter than anyone thought.

Hot heavy oil broke through the crust of cooled residue and poured from the drum. The oil was above its auto-ignition temperature so, when exposed to air, it burst into flames engulfing the two refinery workers operating the hydraulic lift and pouring onto four more workers below. Witnesses said they heard an explosion, and saw a large plume of black smoke rise up from the refinery followed immediately by a ball of fire several stories high. The blast was felt several blocks from the refinery. A few minutes later, a site emergency was declared.

The six workers killed in the explosion were two Equilon employees and four Western Plant Services employees. They died from smoke inhalation and burns.

Later analysis showed that, without effective steam or water cooling, it would have taken about 200 days for the 200 m^3 of coke in the drum to cool to a safe temperature.

The Washington State Department of Labor and Industries set up an investigation that lasted eight months. Their report criticised the Equilon plant managers for allowing the coking drum to be opened when it had only air-cooled for some 37 hours, instead of the normal steam- and water-cooling process.

Equilon subsequently installed a remotely-controlled system for removing the drum lids, and installed a gas-fired back-up system to maintain steam supplies in the event of a power failure.

On 19th January 2001, a $45 million settlement was reached between Equilon and the families of the six men, and Equilon accepted responsibility for the accident.

What should have happened? First, the situation was very significantly different from the normal plant operating procedures, so this should have triggered all sorts of concerns for the managers and operators.

- Some attempt to measure the temperature of the material in the drum could perhaps have been made, possibly by lowering a temperature measurement device in form the top of the vessel. Specialist contractors would almost certainly have been needed to do this.
- Specialist advisers might have proposed some further ways to cool the drum.
- The plant managers should also have contacted specialist technical support, who would have tried to calculate temperatures inside the drum.

All these steps would undoubtedly have required off-site specialist assistance, and the off-site experts would undoubtedly have taken a long time, possibly as much as several weeks. During that time the coking plant could only been used at best at half-capacity, using the other drum.

What did happen? It seems to me that there are two possibilities:

1. By a process of 'group-think' the plant managers and operators somehow convinced themselves that there was no problem, that the coke drum would not contain dangerously hot oil and coke. Possibly they all felt commercial pressure to make the plant operational again, which might have affected their judgment.
2. The managers and operators were completely unaware of the nature of the hazard posed by an extremely hot mixture of heavy oil residue and coke being exposed to the air.

This is an example of the "Ignorance v. Stupidity" question. Here option 1 is "stupid" and option 2 is "ignorant".

I think option 2 is difficult to believe. These were people with many, many years of collective experience. In this example, it appears to me that the collective knowledge of the decision-makers means they must have known about the hazard of the hot oil residue-coke mixture, so ignorance is simply not credible. So, somehow, a group of experienced people persuaded themselves that it would be okay to do something really stupid.

This bizarre accident happened because the plant managers somehow convinced themselves that the situation was safe, despite operating well outside their approved operating procedures.

CASE STUDY 3: THE BP TEXAS CITY ACCIDENT, 23rd MARCH 2005

The Texas City refinery explosion and fire on 23rd March 2005 killed 15 people and injured a further 180. The accident had a financial cost exceeding $1.5 billion, making it the most expensive refinery accident in history. A highly-critical report was published by the US Chemical Safety and Hazard Investigation Board[4], who also produced an excellent 55-minute video[5] about the accident.

A further independent report was commissioned by BP itself, chaired by James Baker[6]. James Baker had a very long and distinguished career in US politics and government. He had been Chief of Staff in President Reagan's first administration 1981-1985, Secretary of the Treasury in Reagan's second administration 1985-1989, and Secretary of State and then Chief of Staff again in the administration of President George HW Bush 1989-1993. Baker's report was highly critical of the safety culture and the management of safety within BP, as we shall see. BP's ploy of asking Baker to chair the independent report into the Texas City accident was intended to show, very publicly indeed and especially for a US audience, that they were going to learn their lessons and change their ways.

[4] US Chemical Safety and Hazard Investigation Board, Investigation Report 2005-04-I-TX, March 2007
[5] *Anatomy of a Disaster*, http://www.csb.gov/videoroom/detail.aspx?vid=16&F=0&CID=1&pg=1&F_All=y
[6] The Report of the BP US Refineries Independent Safety Review Panel (The Baker Report), January 2007

The Texas City accident and the public reports of management shortcomings were followed by much public breast-beating by BP, with BP representatives giving presentations about all that had been wrong at Texas City, and how things were going to change radically within the worldwide BP organisation to make things better – in effect they were saying "*mea culpa, maxima mea culpa*" and repenting their sins. Technical presentations were given in public seminars in various locations, including one I attended in Aberdeen, the centre for UK North Sea oil activity, where I was running the office of a safety management consultancy.

BP TEXAS CITY REFINERY – PRELUDE TO THE ACCIDENT

The Texas City refinery had operated since 1934. The refinery had been owned by Amoco until it merged with BP in 1998. Under Amoco's ownership, at least three opportunities had been missed to carry our modifications that would have prevented the accident:

1991: The Amoco refining planning department proposed eliminating blowdown systems that vented to the atmosphere, but funding for this plan was not available.

1993: A project was proposed to eliminate atmospheric blowdown systems but funding was not approved.

1997: Despite Amoco's process safety standard prohibiting new atmospheric blowdown systems and calling for the phasing out of existing ones, Amoco replaced the 1950s-era blowdown drum/vent stack that served the raffinate splitter tower with an identical system, instead of upgrading to recommended alternatives that were safer.

Accident time-lines almost always read like comedies of errors, instead of the tragedies that they are. When the events are laid out in chronological order, it is hard not to read the stages of the accident unfolding without thinking "They did WHAT?"I have put my comments on the timeline below in italics.

With hindsight, in the years preceding the March 2005 accident, there had been a number of significant indicators that all was not well regarding plant safety at Texas City. In the preceding 30 years, 23 people had been killed in separate accidents on the plant. *This number seems incredibly high - it should have attracted attention from both senior management and from safety regulators.*

Budget cuts of 25% were made at all refineries after the BP-Amoco merger in 1998 without any apparent review for their effects on process safety.

Mergers and acquisitions create difficult problems for the management of safety. Responsibilities and reporting routes change. Management communications based on personal relationships can be disrupted. The expectations of the new people in charge may not be clear. The balance between the needs of safety and the needs of production – in which safety should always come first - may become upset, either because plant operators misperceive the expectations of their new senior management, or else because senior management fail to communicate their requirements clearly to their new staff. Senior managers such as VP's and Directors may be unsure of their new CEO – is he really concerned about safety, or is he just paying lip-service? If it comes to a tough decision about

safety versus production and revenue, senior managers may be thinking, "Where will the new CEO stand?" I know this is a sweeping generalisation, but CEO's as a breed can be quite intimidating people, and it can be difficult to get to know them.

Further down the corporate food-chain, middle managers may be anxious about their new senior managers, because downsizing normally follows acquisition and they may be worried about their jobs. There may be issues of different company cultures – for example, the way in which things are done and the way in which concerns are communicated – that can affect safety.

There may even be new paradigms introduced about safety; for example, there was a vogue in the late 1990's for the rate of industrial safety accidents (that is, accidents arising from 'slips, trips and falls' in the workplace) to be used by senior management as a surrogate Key Performance Indicator (KPI) for the safety of a hazardous industrial process, that is, the risk of a major process accident such as a fire or explosion. *Clearly, these are two almost entirely different issues.*

So, at Texas City, a KPI for Lost Time Accidents was used as a surrogate measure of process safety – and then the Lost Time Accident rate was, somehow, declared to be a record low in 2004 - the very same year that they had three fatal accidents. *Who was kidding who?*

BP's own reports during the years immediately before the accident reported multiple safety system deficiencies, and included the following comments and statements (as detailed in the report by the US Chemical Safety and Hazard Investigation Board):

2002: "Infrastructure at Texas City was in compete decline."

"Serious concerns about potential for major site incident."

There were 80 hydrocarbon releases at Texas City in a two-year period.

A further proposal to replace the blowdown drum/vent system was cut from the budget.

2003: "Current condition of infrastructure and assets is poor at Texas City".

Maintenance spending was limited by a "chequebook mentality".

2004: "Widespread tolerance of non-compliance with basic HSE rules"

"Poor implementation of safety management systems."

"Production and budget compliance gets recognised and rewarded above anything else."

There was a high leadership turnover rate.

The refinery had three major accidents in 2004, including 3 fatalities and $30m damage, but its lowest ever rate of Lost Time Accidents (LTAs). *These two facts, juxtaposed like that, do not ring true – but that is what we are told. The only possible reconciliation is that there was significant under-reporting of Lost Time Accidents. A 'punitive culture' with regards to incident reporting was one of the contributory factors cited in the investigation reports.*

2005: The isomerisation unit splitter tower high level alarm had been reported as not functioning several times in the two years prior to accident – but maintenance work orders were closed without repairs being carried out.

One month before the accident, an internal BP memo said, "I truly believe we are on the verge of something bigger happening."

THE ACCIDENT AT BP TEXAS CITY

On the morning of 23rd March 2005, there were lots of contractors on site for maintenance projects. Mostly, they were housed in temporary trailers near hazardous plant, including the Isomerisation Unit[7]. Start-up of the Isomerisation Unit had commenced during night-shift.

At 0215, operators started to introduce raffinate[8] into the Raffinate Splitter Tower, which is used to distil and separate gasoline components. The tower was more than 30 metres tall. A single instrument (shown as LT) was available for liquid level indication at the bottom of tower which had a maximum indicated level 9 feet (about 3 metres). Above this level the instrument just indicated '9 feet'. However, operators routinely filled above level this during start-ups to avoid the possibility of low level causing furnace damage.

At 0309, a High Level Alarm (shown as LAH) actuated. Another alarm, designated 'Hi-hi', failed to actuate.

At 0330, the level indication showed its maximum - 9 feet - and feed was stopped by operators. (The actual level was probably about 13 feet at that point.)

At 0500, the Lead Operator in the satellite Control Room for the Isomerisation Unit gave a briefing to the Central Control Room and left to go home early.

At 0600, a new Central Control Room operator arrived to start his thirtieth consecutive day doing 12 hour shifts, because of staff shortages.

(Thirty consecutive twelve-hour days would obviously be exhausting. In the European Union it would also be illegal under the Working Time Directive, enacted in 2003.)

The shift log left by the nightshift was unclear about the level in the Raffinate Splitter Tower and the general state of start-up. All that was recorded was "ISOM (*Isomerisation Unit*): brought in some raff to unit".

At 0715, the Day Supervisor arrived late, so he missed the shift handover.

At 0951, the start-up was resumed. The day shift put more feed put into the already over-filled splitter tower. An Auto-level control valve on the raffinate feed to the Splitter Tower was left closed because of 'conflicting instructions'. *So the Splitter Tower just kept filling up higher and higher.....*

[7] The Isomerisation Unit's function is to improve the octane rating of the raw gasoline.
[8] The word 'raffinate' means a product in the refining process. In this case the raffinate was naphtha or raw gasoline from the crude distillation column.

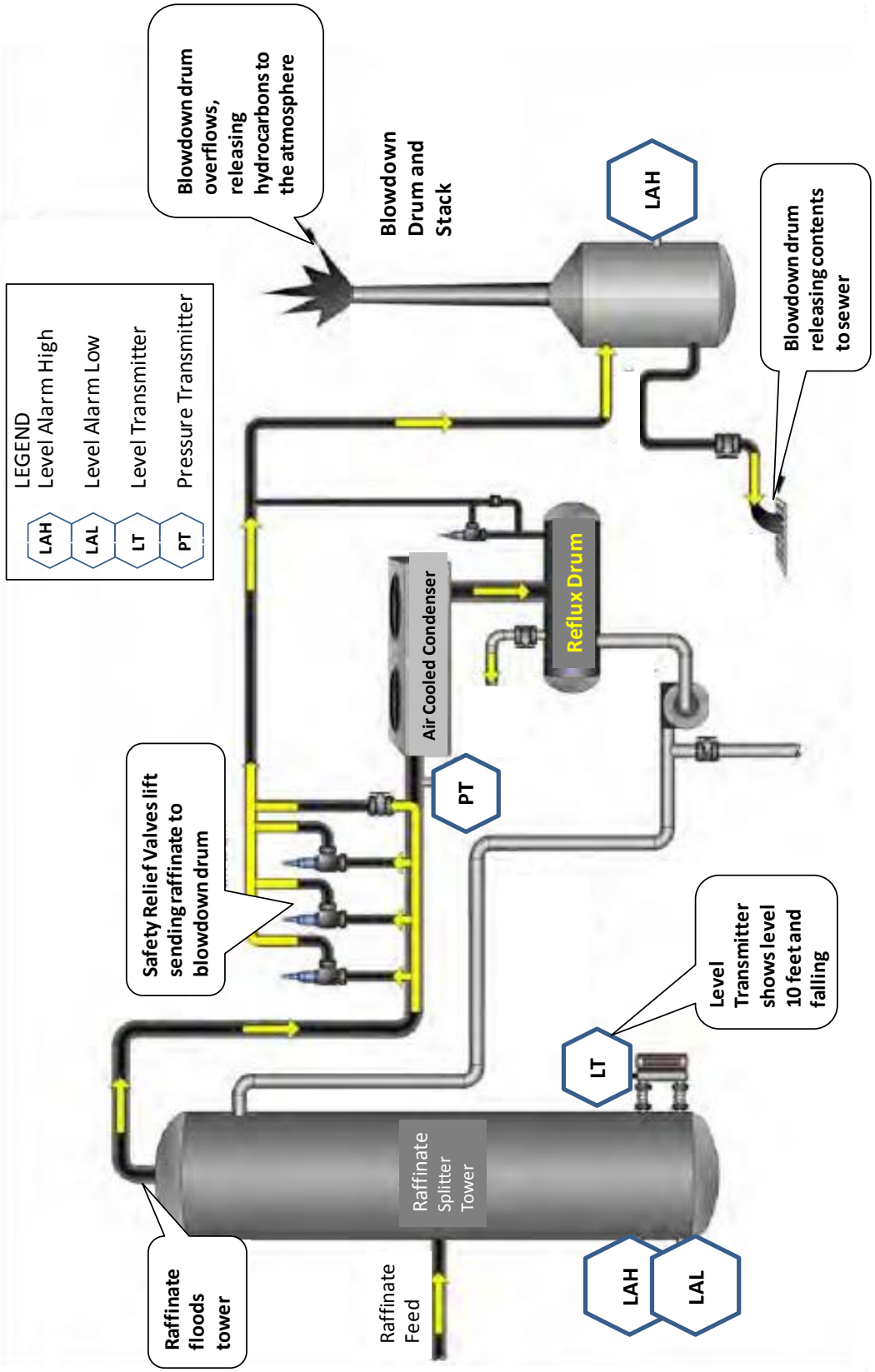

Fig 3: Schematic diagram of the Isomerisation Unit, BP Texas City (adapted from the US Chemical Safety and Hazard Investigation Board report)

At 1000, the Furnace under the Raffinate Splitter Tower was lit to start feed heating. Raffinate feed was still going on, although the only level instrument still showed its maximum of about 9 feet.

At 1050, the Day Supervisor left the site to deal with a family medical emergency. This left no supervisor in the Central Control Room, contrary to the operating rules. A single control room operator, very tired from thirty consecutive 12-hour shifts, was now running three operating units, including the Isomeration unit as it went through its start-up procedure.

(In 1999, after the BP-Amoco merger, a second operator position had been eliminated.)

By about 1200, the level in the Splitter Tower level reached 98 feet (15 times its normal level) but the level instrument showed 8.4 feet and gradually falling. Screen displays in the Control Room did not show 'flowrate in' and 'flowrate out' on same screen (so the control room operator had to toggle between two separate displays, if this was checked at all), nor was there any computer calculation of the total amount of liquid in the tower.

At about 1200, maintenance contractors left their temporary trailers near the Isomerisation Unit for a lunch to celebrate one month without lost-time injury.

(The irony of this stretches belief. It also says something about the working environment at Texas City refinery that a mere one month *without a lost-time injury was considered sufficient to merit a celebratory lunch. Also, I do not understand how this is consistent with the claim of 'zero Lost Time Accidents' in 2004, unless the celebratory lunch was something that had happened every month for a long time.....)*

At 1241, an alarm appeared in the Control Room to say there was high pressure at the top of the Splitter Tower. *(This was caused by compression of gases as the liquid raffinate level rose. The Splitter Tower - a distillation column - was now almost completely full of liquid raffinate.)* The Control Room operator got plant operators to respond to this alarm as follows:

- A plant operator opened a manual valve to vent gases into the relief system (which vented unflared gas into atmosphere via the Blowdown Drum).
- A plant operator also turned off two burners in the furnace at the bottom of the Splitter Tower (thinking this would reduce the pressure).
- A plant operator opened a valve to allow liquid to go from the bottom of the Splitter Tower to storage tanks. This liquid was very hot and flowed through a heat exchanger with liquid entering the Splitter Tower, raising temperature of liquid entering tower by about 141 degrees Fahrenheit (about 90 degrees Centigrade).

At 1300, the contract workers returned from their celebratory lunch to their temporary trailers which were located near the Blowdown Drum.

At 1314, the hot feed raffinate caused boiling, so the level rose until the Splitter Tower was filled completely. Hot liquid gasoline then spilled into the vapour line, which caused pressure relief valves in the vapour line to open (*see Figure 3*). 52000 gallons (236000 litres) of liquid gasoline thereby vented to the blowdown drum, where it overflowed and drained into a process sewer, setting off

control room alarms. The high-level alarm in the Blowdown Drum (shown as LAH) failed to actuate. A geyser of liquid and vapour gasoline erupted from the vent above the Blowdown Drum, and the hot gasoline formed a large vapour cloud, which was ignited by a running truck engine nearby. An explosion and fire ensued, causing 15 deaths and 180 injuries. The temporary trailers housing the contractors were destroyed in the blast.

To recap: The accident involved the Splitter Tower becoming completely filled with hot liquid raffinate (naphtha or gasoline), when it should have been less than one-tenth full. Hot raffinate then overflowed into the Blowdown Drum and out through its vent. The Splitter Tower had been receiving raffinate feed for several hours without any apparent concern that it might be overfilling. The level instrumentation at the bottom of the tower never recorded any values above about 9 feet. After the overflow, the Blowdown Drum level alarm failed to work.

The Control Room Day Supervisor had missed the handover from nightshift. He then had to go home because of a family medical emergency. The only remaining Control Room operator was on his thirtieth consecutive 12 hour shift.

Some of the extremely damning root causes and contributory factors noted in the Accident Reports are listed in the following table.

	Root cause or contributory factor
1	There was a lack of open event reporting – a "punitive culture".
2	There was de-centralised management which impaired learning from incidents elsewhere.
3	There was a failure to investigate near-misses in previous Isomerisation Unit start-ups.
4	There was a lack of modern design for key safety systems (e.g. level instrumentation, blowdown system).
5	There were occupied trailers near the Isomeration Unit. This neglected industry siting guidelines, and personnel inside the trailers were not advised of start-up operations. BP's own Management of Change guidelines were not heeded in considering the positions of the trailers.
6	There was serious worker fatigue and no fatigue prevention policy.
7	Inadequate training: the training programme had been down-sized.
8	There was lack of procedural adherence and, in any case, the procedures were out-of-date.
9	There was "no accurate and functional measure of level in tower" which led to incorrect decisions.
10	There was poor communication during shift handover.
11	There was a lack of robust, enforceable, external independent auditing.
12	There was tolerance of serious deviations from safe operating practices, and apparent complacency toward serious process safety risks.
13	Restructuring following the BP-Amoco merger had resulted in a significant loss of people, expertise and experience.

There was a very significant recommendation which should apply to all hazardous process plant: "All hazardous chemical operations should be required to review the safety impact of major organisational changes." When the organisation is changed - as happens in all companies on a regular basis – the implications for safety have to be considered carefully.

The Baker Report was aimed, in particular, at "the effectiveness of BP's corporate oversight of safety management systems at its five US refineries and its corporate safety culture." Amongst its findings were the following:

> It is imperative that BP's leadership set the process safety "tone at the top" of the organization and establish appropriate expectations regarding process safety performance

> BP has emphasized personal safety in recent years and has achieved significant improvement in personal safety performance, but BP did not emphasize process safety.
>
> BP has not established a positive, trusting, and open environment with effective lines of communication between management and the workforce.....
>
> BP's corporate management.....have overloaded personnel at BP's US refineries.
>
> BP tended to have a short-term focus, and its decentralized management system and entrepreneurial culture have delegated substantial discretion to US refinery plant managers without clearly defining process safety expectations, responsibilities, or accountabilities.
>
> BP's system for ensuring an appropriate level of process safety awareness, knowledge, and competence in the organization relating to its five U.S. refineries has not been effective in a number of respects.
>
> BP.....has sometimes failed to address promptly and track to completion process safety deficiencies identified during hazard assessments, audits, inspections, and incident investigations.

The Chemical Safety and Hazards Investigation Board drew lessons in Safety System Deficiencies, Incident Investigation Deficiencies, Maintenance, Management of Change and Safety Culture. From the accident, the CSHIB drew eight Key Lessons for operators of hazardous plant. These are absolutely generic in nature – they apply to any hazardous plant:

1. Track KPIs for monitoring safety performance
2. Maintain adequate resources for safe operation and maintenance
3. Nurture and maintain a proper safety culture
4. Non-essential personnel should be remote from hazardous process areas
5. Equipment and procedures should be kept up-to-date
6. Manage organisational changes to ensure safety is not compromised
7. Analyse and correct the underlying causes of human errors
8. Directors must exercise their duties regarding safety standards

To paraphrase: The accident happened because the plant was not maintained adequately, the operators were over-stretched and didn't adequately understand the plant they were operating, and the management were not paying enough attention.

After repairs and a further period of operation, BP sold the Texas City refinery to Marathon Oil in October 2012. By that time, of course, BP had suffered another massive accident in the United States – the blowout at Macondo/*Deepwater Horizon*.