Chemical Engineering 4N04
Process Safety Introduction

- Summary of Topics to be covered
- Quick look at how safe/unsafe the industry has been
- Summary of Some Past Accidents

Chemical Engineering 4N04
Process Safety Topics

- Introduction
  - Safety record of industry
  - Some infamous industrial accidents
- The Safety Hierarchy
- Pressure relief and subsequent processing
- Hazards and Operability Studies (HAZOP)
- Workshop on BP Texas City Accident

Measures of risk/safety used by governments and industries

- **FAR: Fatal Accident Rate - This is the number of fatalities occurring during 1000 working lifetimes (10^8 hours). This is used in the U.K.**

- **Fatality Rate = FAR*(hours worked) /10^8 (fatalities/y)**

- **OSHA Incidence Rate - This is the number of illnesses and injuries for 100 work-years. This is used in the USA.**

Typical data comparing various occupations

FAR Data for typical Activities

Activity	FAR
Chemical Industry	4
Steel Industry	8
Coal Mining	40
Construction	67
Uranium	70
Asbestos (old data?)	620
Staying home	3
Traveling by automobile	57
Cigarette smoking	???

What is the fatality rate/year for the chemical industry?

What is FAR for cigarette smoking?

Question: What is the fatality rate (/year) in the chemical industry?

$(4)\ (8\ \text{hr/day})\ (5\ \text{day/week})\ (45\ \text{weeks/year}) / 10^8$

$= 7.2 \times 10^{-5}$ fatalities/year

FAR	**Chemical Industry**	**4**
FAR	**Cigarette smoking**	**40**

Trevor Kletz, "Eliminating Potential Process Hazards", Chem. Eng., April 1, 1985

What is the Basis or Goal for Engineering Design?

- One standard used is to maintain the risk for involuntary activities less (much less?) than typical risks such as “staying home”

  Remember that many risks exist
  (total risk is sum)

- We must consider the inaccuracies of the estimates

- We must consider people outside of the manufacturing site.

What is the Basis or Goal for Engineering Design?

- **People usually distinguish between voluntary and involuntary risk. They often accept higher risk for voluntary activities (rock climbing).**
- **People consider the number of fatalities per accident**

Fatalities = (frequency) (fatalities/accident)

.001 = (.001) (1) **fatalities/time period**

.001 = (.00000001)(100,000) **fatalities/time period**

We need to consider frequency and consequence

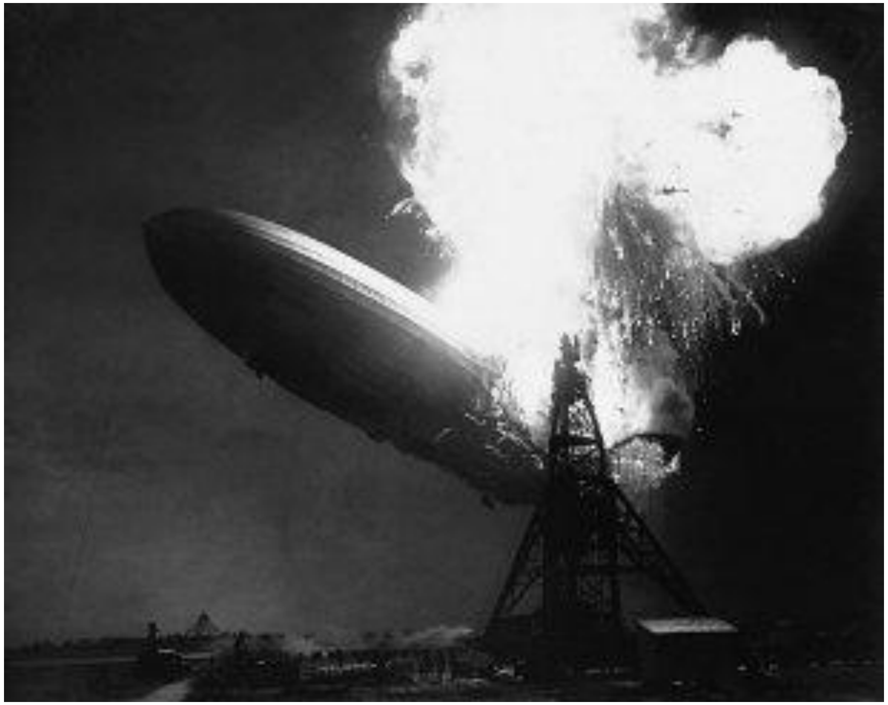
Why should we study past accidents in technological systems?

"Those who do not learn from history are doomed to repeat it" - George Santayana

Legislation and engineering standards are often based on key events.

We are not smarter than those who committed these great errors; will we be better prepared?

We have learned how to manage technology from previous bad experiences, haven't we?



Hindenberg hydrogen-filled dirigible

From: http://www.otr.com/hindenburg.html

The Challenger space shuttle minutes before its destruction

From: http://www4.ncsu.edu/~jherkert/mds322.html

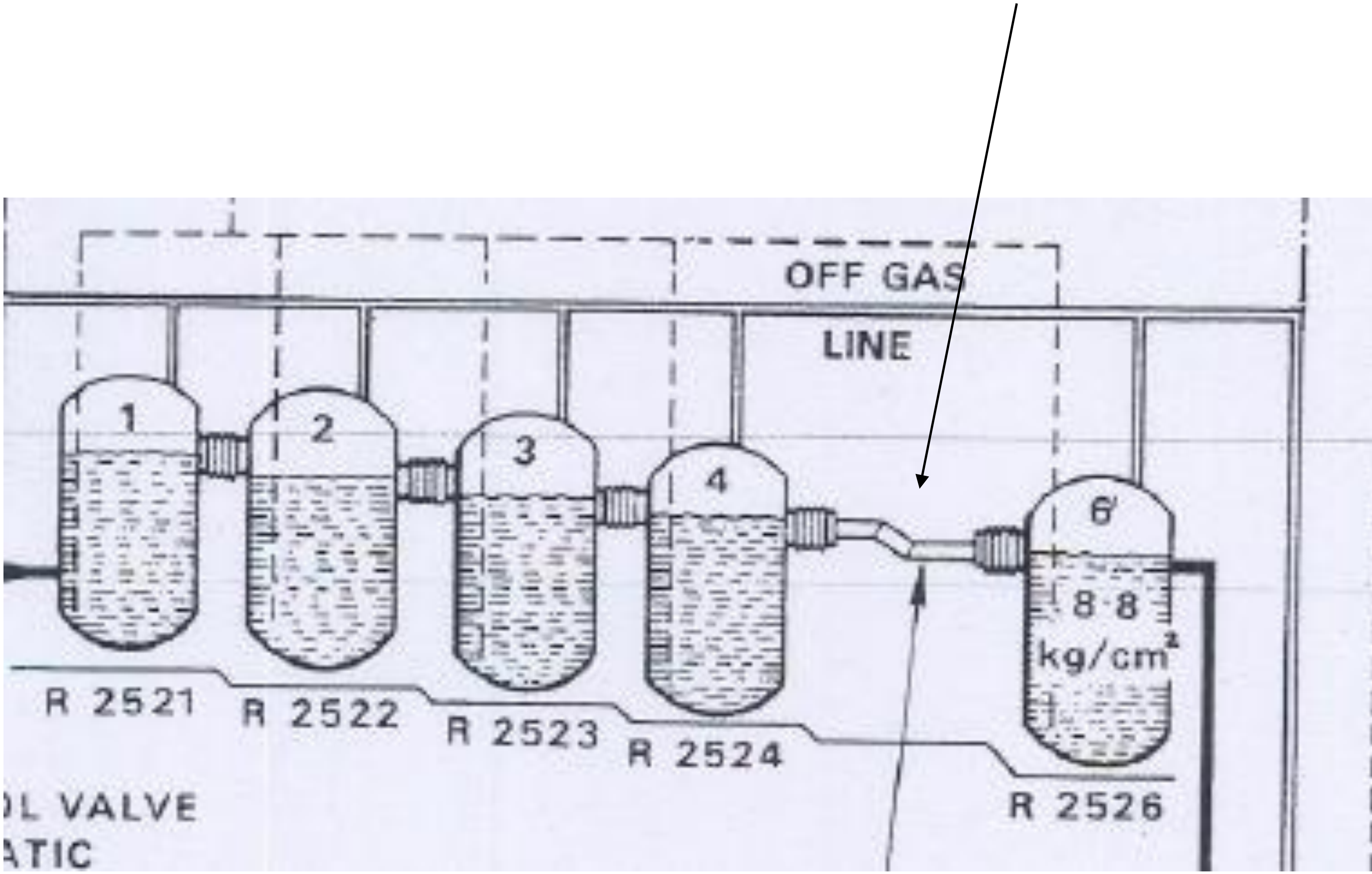
Large chemical companies with lots of experience know how to build and operate plants safely, don't they?

Flixborough in the UK. (1974)

A person without proper education designed a piping change. After some time in operation, the pipe failed and a large cloud of hydrocarbons were released to the atmosphere, where they exploded.

http://www.acutech-consulting.com/acusafe/Incidents/Flixborough1974/Flixborough1974-1.jpg

Process modification without proper engineering analysis



http://www.patricklagadec.net/uk/pdf/Flixborough.pdf

Flixborough Accident Summary

At about 16:53 hours on Saturday 1 June 1974 the Nypro (UK) site at Flixborough was severely damaged by a large explosion. **Twenty-eight workers were killed and a further 36 suffered injuries.** It is recognised that the number of casualties would have been more if the incident had occurred on a weekday, as the main office block was not occupied. Offsite consequences resulted in fifty-three reported injuries. Property in the surrounding area was damaged to a varying degree.

Prior to the explosion, on 27 March 1974, it was discovered that a vertical crack in reactor No.5 was leaking cyclohexane. The plant was subsequently shutdown for an investigation. The investigation that followed identified a serious problem with the reactor and the decision was taken to remove it and install a bypass assembly to connect reactors No.4 and No.6 so that the plant could continue production.

During the late afternoon on 1 June 1974 a 20 inch bypass system ruptured, which may have been caused by a fire on a nearby 8 inch pipe. This resulted in the escape of a large quantity of cyclohexane. The cyclohexane formed a flammable mixture and subsequently found a source of ignition. At about 16:53 hours there was a massive vapour cloud explosion which caused extensive damage and started numerous fires on the site.

Eighteen fatalities occurred in the control room as a result of the windows shattering and the collapse of the roof. No one escaped from the control room. The fires burned for several days and after ten days those that still raged were hampering the rescue work.

Taken from http://www.hse.gov.uk/hid/land/comah/level3/5A591F6.HTM

Plants with safety systems cannot be operated in an unsafe manner, can they?

The Chernobyl (Soviet Union) accident in 1986 was the result of a flawed reactor design that was operated with inadequately trained personnel and without proper regard for safety.

http://www.cc.gla.ac.uk/courses/science/shc/shcl17.htm

"On 25 April, prior to a routine shut-down, the reactor crew at Chernobyl-4 began preparing for a test to determine how long turbines would spin and supply power following a loss of main electrical power supply. ***Similar tests had already been carried out at Chernobyl and other plants***, despite the fact that these reactors were known to be very unstable at low power settings.

A series of operator actions, including the ***disabling of automatic shutdown mechanisms***, preceded the attempted test early on 26 April. As flow of coolant water diminished, power output increased. When the operator moved to shut down the reactor from its unstable condition arising from previous errors, a peculiarity of the design caused a dramatic power surge.

The fuel elements ruptured and the resultant explosive force of steam lifted off the cover plate of the reactor, releasing fission products to the atmosphere. A second explosion threw out fragments of burning fuel and graphite from the core and allowed air to rush in, causing the graphite moderator to burst into flames.

The accident destroyed the Chernobyl-4 reactor and **killed 30 people, including 28 from radiation exposure. A further 209 on site were treated for acute radiation poisoning** and among these, 134 cases were confirmed (all of whom recovered). Nobody off-site suffered from acute radiation effects. However, large areas of Belarus, Ukraine, Russia and beyond were contaminated in varying degrees. "

From http://www.world-nuclear.org/info/chernobyl/inf07.htm

Plants have equipment to contain dangerous materials, so no problem?

In **Bhopal, India (1984)**, a large amount of toxic gas was released that killed at least 3500 people immediately. The plant was designed to hold a large inventory of hazardous material and had **four processes to prevent a release** - all failed.

http://www4.ncsu.edu/~jherkert/mds322.html#GRID

The Bhopal crisis was triggered by a technological accident: 45 tons (100,800 lb) of methyl isocyanate (MIC) gas escaped from two underground storage tanks at a Union Carbide pesticide plant. The accident occurred between 10 p.m. (2 December) and 1.30 a.m. (3 December) when the plant was on second shift and the surrounding population was asleep in slum "hutments" that are densely packed together in this part of Bhopal (fig. 5.1).

Leaked gases were trapped under a nocturnal temperature inversion in a shallow bubble that blanketed the city within five miles of the plant. **Next morning, over 2,000 people were dead and 300,000 were injured. Another 1,500 people died in subsequent months owing to injuries caused by the accident.** At least 7,000 animals perished but damage to the natural environment remains largely unassessed (Prasad and Pandey 1985).

The accident that is discussed here began when a large volume of water entered the MIC storage tanks and triggered a violent exothermic chain reaction. Normally, water and MIC were kept separated, even when supply pipes were flushed with water during routine cleaning. However, on this occasion metal barriers known as slip blinds were not inserted and the cleaning water passed directly into the MIC tanks (table 5.1b).

Four safety devices that were meant to keep toxic gases from escaping into the atmosphere failed to function: **lack of coolant in the MIC tank refrigerator prevented it from operating properly; the vent gas scrubber could not neutralize the gases because it lacked sodium hydroxide; a pipe leading to the flare tower had been dismantled for repairs, so the flare could not be used to burn escaping gases; finally, water sprays could not be used to douse the gases because they lacked sufficient pressure to reach the height from which the gases were spewing**.

From: http://www.unu.edu/unupress/unupbooks/uu21le/uu21le0c.htm#introduction

I don’t have to worry about safety in a pharmaceutical plant, do I?

A **mixture of dust and air** caused the violent explosion of West Pharmaceutical Services in Kinston, N.C., USA in 2003, the federal Bureau of Alcohol, Tobacco and Firearms said. Investigators are still looking for what sparked the explosion.

The blast left a once-busy Kinston employer of 255 a lifeless gray skeleton. The smell of burning rubber and charred metal still stain the air at the site.

The fiery eruption rocked Kinston and was felt for miles around. It left four dead and nine in critical condition.

Local authorities are well informed and prepared for an emergency, aren't they?

Seveso (1976)

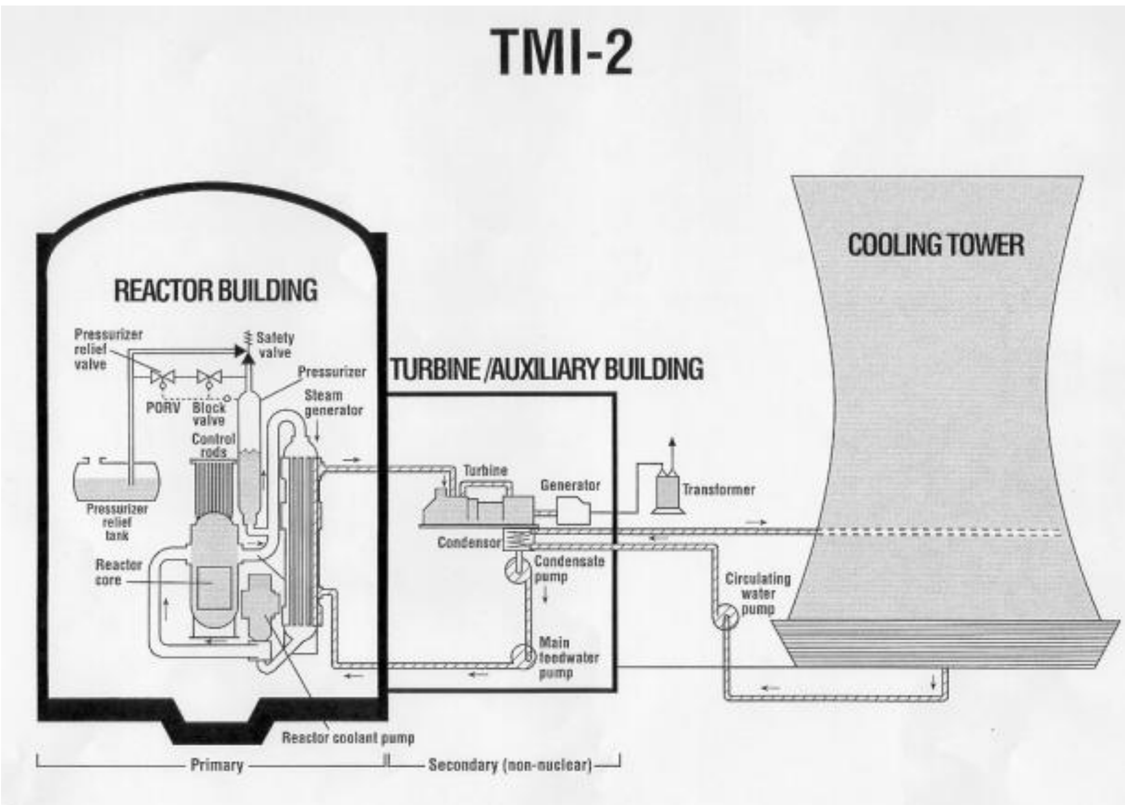
http://www.tlchm.bris.ac.uk/motm/245t/245tc/seveso.htm

Around midday on Saturday 10 July 1976, an explosion occurred in a TCP (2,4,5-trichlorophenol) reactor of the ICMESA chemical plant on the outskirts of Meda, a small town about 20 kilometres north of Milan, Italy.[1] A toxic cloud containing TCDD (2,3,7,8-tetrachlorodibenzo-*p*-dioxin), then widely believed to be one of the most toxic man-made chemicals (Mocarelli et al. 1991), was accidentally released into the atmosphere. The dioxin cloud contaminated a densely populated area about six kilometres long and one kilometre wide, lying downwind from the site (fig. 4.1). This event became internationally known as the Seveso disaster

One of the most remarkable features of the Seveso experience was that neither the residents nor the local and regional authorities suspected that the ICMESA plant was a source of risk. They did not even know much about the type of production processes and chemical substances that occurred there.

From: http://www.unu.edu/unupress/unupbooks/uu21le/uu21le09.htm#4%20seveso:%20a%20paradoxical%20classic%20disaster

Since we monitor the plant using sensors, it can never become dangerous, can it?



http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html#tmiview

The nuclear power plant in **Pennsylvania, USA,** experienced equipment failures that could have been contained. However, the sensors and valves did not provide the behavior expected by the personnel.

In a short time, major damage to the plant occurred.

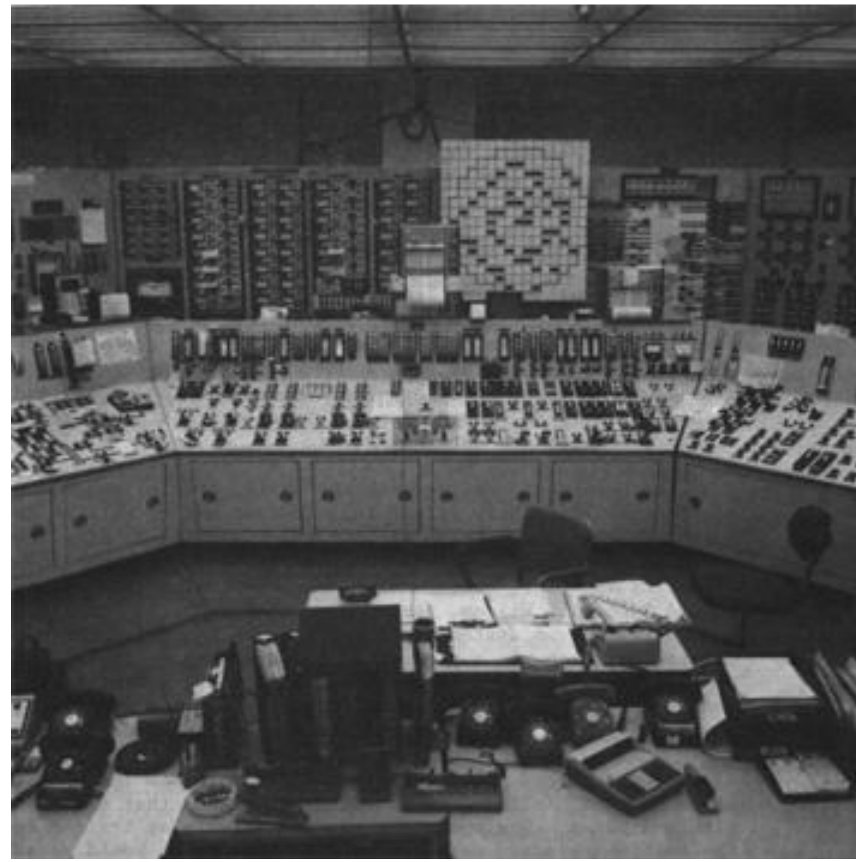
(1979)

You have worked ½ of your shift and things are pretty quiet. An alarm sounds to inform you that the main cooling pumps have shutdown and the control rods have been lowered in the reactor to reduce heating. While not desirable, you are not worried, because the backup pumps have started to provide cooling to the reactor. This happens occasionally.

You observe that the safety valve opened and then closed after a short time, which is reasonable to relieve steam pressure due to the short-term overheating.

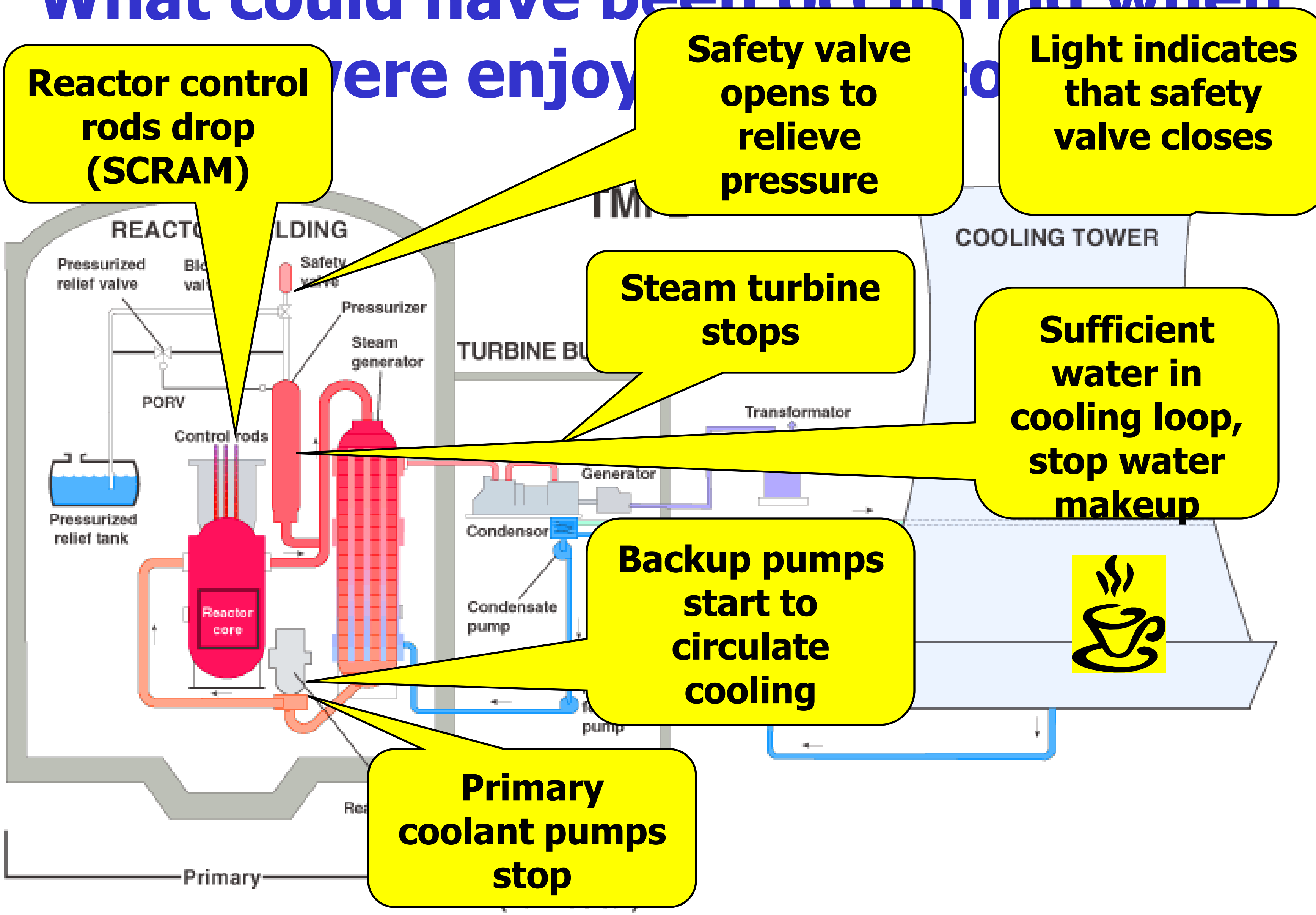
The cooling water level surrounding the reactor is appropriately high, so you turn off the emergency makeup water pumps.

Things are getting back to normal, so time to enjoy that cup of coffee and get back to the discussion of the Penn State basketball team.



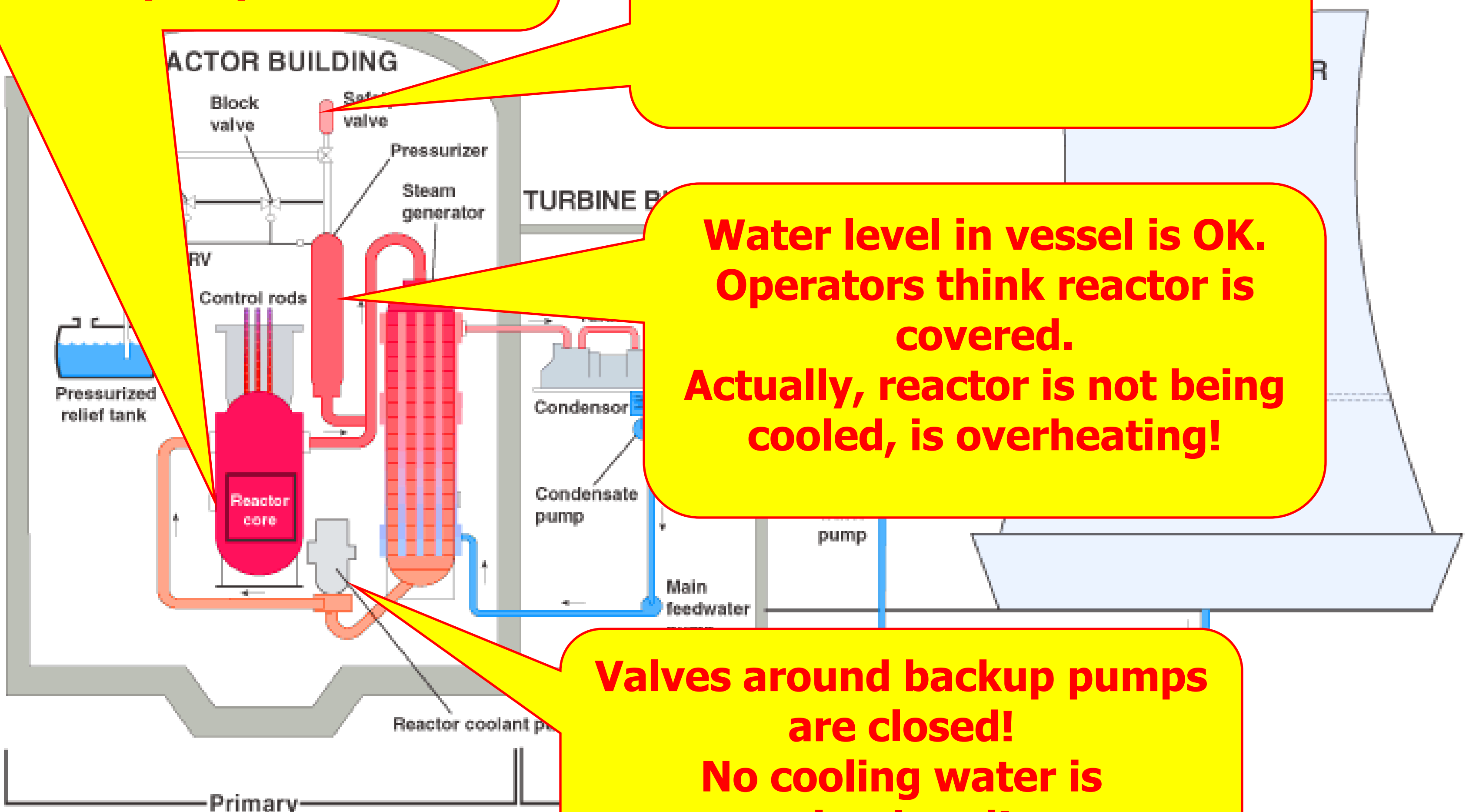
http://www.animatedsoftware.com/hotwords/control_room/control_room.htm

What could have been occurring when … ere enjoy … co



http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

What actually occurred when you were ...ing your coffee?



Since operators think water is OK, they shutoff emergency water makeup pumps!

Safety valves remained open! Water continues to escape!

Water level in vessel is OK. Operators think reactor is covered.
Actually, reactor is not being cooled, is overheating!

Valves around backup pumps are closed!
No cooling water is circulated!

We would like to become famous for our engineering achievements, but …. not this way!!

Three Mile Island Nuclear Power Plant

The accident began about 4:00 a.m. on March 28, 1979, when the plant experienced a failure in the secondary, non-nuclear section of the plant. The **main feedwater pumps stopped running**, caused by either a mechanical or electrical failure, which prevented the steam generators from removing heat. First the turbine, then the reactor automatically shut down. Immediately, the pressure in the primary system (the nuclear portion of the plant) began to increase. In order to prevent that pressure from becoming excessive, **the pressurizer relief valve (a valve located at the top of the pressurizer) opened. The valve should have closed when the pressure decreased by a certain amount, but it did not**. **Signals available to the operator failed to show that the valve was still open**. As a result, the stuck-open valve caused the pressure to continue to decrease in the system.

The emergency feedwater system (backup to main feedwater) was tested 42 hours prior to the accident. As part of the test, a valve is closed and then reopened at the end of the test. But this time, through either an administrative or human error, **the valve was not reopened** - - preventing the emergency feedwater system from functioning. The valve was discovered closed about eight minutes into the accident. Once it was reopened, the emergency feedwater system began to work correctly, allowing cooling water to flow into the steam generators.

Because of these voids, the water in the system was redistributed and the pressurizer became full of water. The **level indicator**, which tells the operator the amount of coolant capable of heat removal, **incorrectly indicated the system was full of water**. Thus, the operator stopped adding water. He was unaware that, because of the stuck valve, the indicator can, and in this instance did, provide false readings.

Because adequate cooling was not available, the nuclear fuel overheated to the point where some of the zirconium cladding (the long metal tubes or jackets which hold the nuclear fuel pellets) reacted with the water and generated hydrogen. This hydrogen was released into the reactor containment building. By March 30, two days after the start of the chain of events, some hydrogen remained within the primary coolant system in the vessel surrounding the reactor, forming a "hydrogen bubble" above the reactor core. From:http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

After we have experienced a serious accident, we will vastly improve safety, won’t we?

BP Texas City (2005)

BP Deepwater Horizon (2010)

Haramachi power plant in Minami Soma, Fukushima showing damage from earthquake and tsunami in March 2011

http://www.nydailynews.com/news/world/2011/03/14/2011-03-14_the_battered_now_face_nuke_fears.html

Haramachi power plant in Minami Soma, Fukushima showing damage from earthquake and tsunami in March 2011

An official from the **International Atomic Energy Agency (IAEA) said in December 2008 that safety rules were out of date and strong earthquakes would pose a "serious problem" for nuclear power stations.** The Japanese government pledged to upgrade safety at all of its nuclear plants, but will now face inevitable questions over whether it did enough. While it responded to the warnings by building an emergency response centre at the Fukushima plant, it was only designed to withstand magnitude 7.0 tremors. Friday's devastating earthquake was a magnitude 9.0 shock.(http://www.telegraph.co.uk/news/worldnews/wikileaks/8384059/Japan-earthquake-Japan-warned-over-nuclear-plants-WikiLeaks-cables-show.html)

Three hundred technicians have been battling inside a danger zone to salvage the six-reactor Fukushima plant since it was hit by an earthquake and tsunami that also killed 7,508 people and left 11,700 more missing in northeast Japan. The unprecedented multiple crisis will cost the world's third largest economy nearly $200 billion in Japan's biggest reconstruction push since post-World War II. It has also set back nuclear power plans the world over. Encouragingly for Japanese transfixed on the work at Fukushima, the situation at the most critical reactor -- No. 3 which contains highly toxic plutonium -- appeared to come back from the brink after fire trucks doused it for hours.(http://www.newsdaily.com/stories/tre72a0ss-us-japan-quake/)

Recent entries on US Chemical Safety Board Internet Site

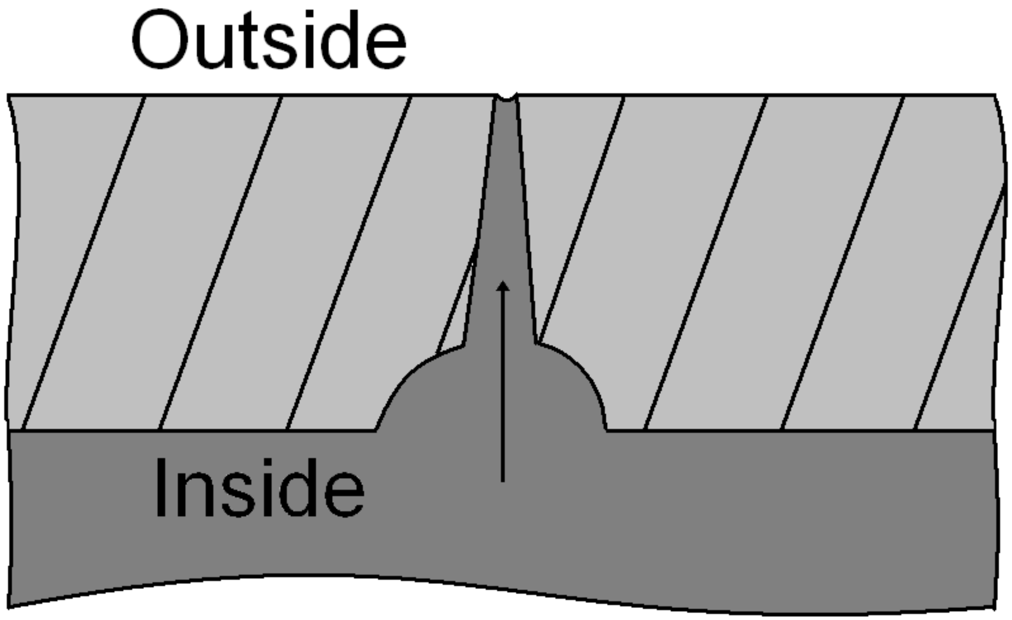
Laboratory explosion at Texas Tech University; student seriously injured. **Don’t let this happen to you!**

Specifically, the CSB found:

- The physical hazards of the energetic materials research work were not effectively assessed and controlled at Texas Tech;
- Texas Tech's laboratory safety management program was modeled after OSHA's Occupational Exposure to Hazardous Chemicals in Laboratories Standard (29 CFR 1910.1450); yet, the **Standard was created not to address physical hazards of chemicals, but rather health hazards as a result of chemical exposures**;
- Comprehensive hazard evaluation guidance for research laboratories does not exist;
- Previous Texas Tech laboratory incidents with preventative lessons were not always documented, tracked, and formally communicated at the university;
- The research-granting agency, DHS, prescribed no safety provisions specific to the research work being conducted at Texas Tech at the time of the incident, missing an opportunity for safety influence; and
- Safety accountability and oversight by the principal investigators, the department, and university administration at Texas Tech were insufficient.

http://www.csb.gov/assets/document/CSB_Study_TTU_FINAL.pdf

Dupont release of Phosgene leading to death of plant operator



http://www.csb.gov/investigations/detail.aspx?SID=92

On January 23, there was a release of highly toxic phosgene, exposing a veteran operator at the DuPont facility in Belle, West Virginia and resulting in his death one day later. DuPont officials told the CSB that a braided steel hose connected to a one-ton capacity phosgene tank suddenly ruptured, releasing phosgene into the air. An operator who was exposed to the chemical was transported to the hospital, where he died the following day. The phosgene release followed two other accidents at the same plant in the same week, including an ongoing release of chloromethane from the plant's F3455 unit, which went undetected for several days, and a release from a spent sulfuric acid unit.

Key Findings

1. An internal DuPont investigation report from a prior oleum leak recommended including all piping in a PM thickness monitoring program. The CSB found no evidence that the piping in the January 23, 2010, incident was included in the program.
2. The general wall thinning rate estimate for the oleum service was conservative. However, highly localized corrosion attack cannot be predicted by this method.
3. Corrosion caused a small leak in the oleum pipe under the insulation