

\tech\book\accident.doc

ACCIDENTS WILL HAPPEN

Two types of danger to our health and safety are generated by faulty technological systems; chronic pollution and accidents. Pollution may be chemical or physical (mainly radiation; but also acoustic); accidents may be release of toxins whether chemical or radioactive, explosions, fires, foundering of vessels, crashes of trains, automobiles and aircraft etc. Pollution may affect humans directly such as traffic smog, or indirectly through the food chain as in Minemata disease, or both as at Chernobyl. A major source of technophobia is to be found in the publicity attending upon accidents

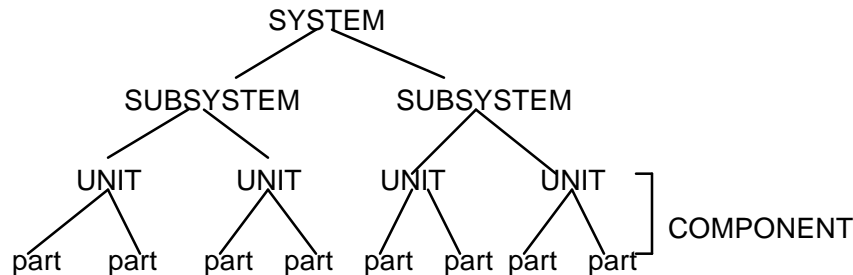


Fig. 145

An accident is defined as a failure in a subsystem, or the system as a whole, that damages more than one unit and in so doing disrupts the ongoing or future output of the system. A disaster is a serious accident with which the public has a high emotional involvement. The first law of safety is that it takes two errors to make an accident. An error is an incorrect belief or action¹. Systems failures are due to unforeseen interactions between failures in subsystems. Many component (part or unit -) failures or even sequences of failures may be anticipated in the normal course of wear and tear. They give rise only to incidents. A problem arises when the entire safety operation is automated because obviously the systems designer cannot anticipate every possible event. Automatic safety devices can only cope with foreseen situations. It is impossible to build flawless software and many events are too dangerous to experiment with by trial and error: the accident at Chernobyl was initiated by just such a dangerous experiment. On the other hand, where there is an intelligent human operator who knows the goals of the system an improvised solution may be found. It will be many years before such intelligence is built into a machine².

The term "accident" has a certain ambivalence about it and a study of its evolution shows how its use was socially constructed during the nineteenth century with the effect, whether consciously intended or not, of suggesting external causes for technological malfunctions. "It was no one's fault; it was an accident!". In other words, the term "accident" should be critically examined ("deconstructed") in the light of the particular context in which it has been used. In many cases it will be found that the malfunction is due either to faulty design or to poor operating practice. Awareness of this is expressed in the popular expression "An accident waiting to happen."

Examples of accidents

Most of the accidents documented in the literature are characterized by both operator error and multiple sub-system failure. Many exhibit the phenomenon of error in the form of an incorrect belief, erroneous perception or "false visualization of the situation" which may

take the form of "misplaced certainty". These impressions have a certain inertia and are not easily changed by conflicting facts -- which tend to be ignored or explained away.

There are many well documented examples of accidents with fatalities ranging from 50 to tens of thousands. Marine accidents are very common, a largish vessel is lost on average every day. We remember the Titanic and closer to home the Ocean Ranger. The loss of the Perintis in the English Channel with a cargo of the biocide Lindane had unknown consequences. Chemical accidents are amongst the worst and the worst of these was at Bhopal in India. The mercury at Minemata, the dioxin at Serveso, the PCBs at Basil Le Grand and at Yusho in Japan, the water poisoning at Camelford in Cornwall are other instances that spring to mind. Chernobyl was the worst nuclear accident, although there have been many others, some kept secret³. Three Mile Island is a good case history because it was short lived and well documented.

Three Mile Island -2.

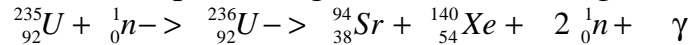
How it works

The purpose of the reactor is to provide a supply of heat for electric power generation using steam turbines. The reactor contains enriched Uranium (proportion of the 235 isotope increased with respect to the 238 isotope) whose controlled fission turns matter into energy and thereby heats the cooling water. The control technology of a nuclear reactor is designed to maintain a chain reaction.

If a chain reaction is to be self-sustaining, it must keep itself supplied with neutrons. Consider the following typical sequence. A neutron plunges into a nucleus of U-235. The nucleus ruptures; as well as two fission-product nuclei it also shoots out three neutrons. One of these three goes out through the surface of the lump of uranium and is lost. Another is absorbed by a nucleus of U-238, which begins its two-stage change into plutonium-239, but does not rupture. This leaves one neutron. If this third neutron now plunges into another U-235 nucleus and ruptures it, the process can continue; otherwise the chain reaction is snuffed out.

At any instant, inside the lump of Uranium, there must be the right number of neutrons of the proper energy to propagate the chain. In effect, for a sustained chain reaction, each neutron which is lost by causing a fission must be replaced by exactly one neutron which does likewise. The system then has a 'reproduction factor' of 1. When this condition is achieved the system is said to be 'critical' and the situation is called 'criticality'. Despite a common misperception to the contrary, 'criticality' is not here used to imply 'danger'. You could say that a nuclear system 'goes critical' just as you could say that a car engine 'starts'. If on average each neutron lost when it causes a fission is replaced by more than one which also causes fission, the reaction 'runs away'....If on average each neutron so lost is replaced by fewer than one which causes fission, the reaction will stop...(Patterson, 1986).

An alternative reaction, producing two neutrons, might be as follows:



The two neutrons could suffer various fates: non-fission capture by U-238, lost at surface of fuel, lost to the structural material of the reactor, captured by the fission products, or start another chain reaction by splitting a U-235 nuclide. The superfix is the nucleon number and the suffix is the proton number according to IUPAC convention. PFM

The slower the neutrons, the more likely they are to be captured. Therefore part of the technology involves moderating their speed. This can be done with various chemicals, including carbon and boron, certain gases or with either ordinary or heavy water. Heavy water is like ordinary "H₂O" except that the hydrogen is replaced by its isotope, deuterium which has a neutron in its nucleus.

The fission of a nucleus generates heat and fast-moving particles whose kinetic energy is turned into heat when they hit something. The next technical problem is therefore to remove the heat so as not to melt the reactor. The whole purpose of the reactor is to produce heat to generate steam to drive a turbine. Hence the removal of heat for a useful purpose kills two birds with one stone.

The essential elements of a reactor are therefore, a supply of fissionable material with the correct spatial arrangement, a moderator to slow the neutrons, a system to remove heat, and control rods to stop it running away.

The pressurized water reactor at TMI#2 consisted of numerous subsystems. (a schematic diagram⁴ will be inserted in later versions of this lecture when copyright has been clarified: Calgary students have access to a hard copy in Reserve Reading)

1. The **core system** is the reactor itself which is cooled by the primary cooling system containing pressurized water whose function it is to cool, to absorb neutrons, to reflect neutrons and to slow neutrons to so-called thermal speeds. The primary coolant passes through a heat exchanger where it gives up its heat to
2. The **steam generating system** which acts as the **secondary cooling** system this has a **main set** of pumps and a **back-up set** for emergencies..
3. A third cooling system passes through the **condenser** of the steam generating system;
4. A fourth, **emergency cooling** system is housed in the auxiliary building and contains borated water that absorbs neutrons.

The Accident

First failure

The accident started in the secondary cooling system at 04:00 on March 28, 1979. As a result of a wrong detailed design of the polisher resin transfer system resin blockage occurred in the transfer line. The operators attempting to clear it hooked up the service instrumentation air system to the higher pressure water system. Water in the air system caused the main the main feedwater pump to trip⁵. A second later the turbine tripped in response to an ASD (Automatic Safety Device). A second ASD now switched on the emergency feed pumps to supply cold water to the heat exchanger (steam generators) and thus keep the radioactive water in the

primary cooling system cool.

Second Failure

Unfortunately someone had closed the valves in this emergency system and so no cool water reached the steam generator. As a result, the primary cooling water began to heat up and expand.

The rising pressure opened the PORV (pressure operated relief valve) through an electromagnetic relay. The pressure also caused the reactor control rods to 'scram' (drop down into the reactor) and successfully stopped the chain reaction fission. Radioactive decay of fissionable products continued, with the emission of more heat. Cooling water from the reactor continued to move out through the PORV and to reduce the pressure.

Third Failure

The reduced pressure sent an electromagnetic signal to the PORV to close. This signal was duly recorded at the console but, unknown to the operators, in fact the PORV did not shut. The instrumentation was poorly designed because it did not record the state of the valve.

Water continued to leave the reactor vessel, filling the drain tank and blowing the rupture disc of a relief valve through which it eventually entered the auxiliary building. There it continued to emit highly radioactive gas into the surrounding countryside for the next few hours.

Human errors

Meanwhile the rising temperature had automatically turned on the emergency cooling system taking borated water to the reactor. But the operators had been warned not to shock the reactor with too much cold water and so they turned off one of the pumps and cut back the throttle on the other.

The resulting rate of emergency water supply was lower than the loss through the jammed PORV. But the operators were convinced that the PORV was closed because the signal to close it had been recorded. They did not look at the temperature in the escape pipe which would have told them it was open, because a label from a removed instrument was hanging in front of the dial. The holding tank showed atmospheric pressure when it was empty and again when the rupture disc broke; no one caught it during the short time it was overpressured. The operators failed to interpret correctly the low pressure recorded in the primary system and the increased vibration.

False visualization

With this mental picture firmly in mind, when the operators got a report of radioactive water in the sump they recorded it as of "unknown origin".

By now the top of the reactor was exposed; very high temperatures and superheated steam were attacking the cladding of the fuel rods and producing hydrogen. The excess of steam was causing the primary coolant pumps to malfunction and so they turned them off. The temperature went off scale and in fact over half the reactor melted. (Ten hours later there was a small hydrogen explosion but the roof stayed on.)

Salvation

At that moment a new shift came on duty. The new supervisor had no preconceived mental picture and reappraised the situation. He closed the block valve leading from the reactor

vessel and thus overrode the jammed PORV. It was 142 minutes from the first malfunction. Had the accident lasted much longer a complete meltdown would have occurred. It is even possible that the radioactive materials would have burnt a hole into the underlying concrete pad and on down to the water table, although the latest calculations indicate that this would not have happened. As it was, the surrounding countryside was saved from a deluge of radioactive iodine only by a system of air filters in the auxiliary building. Another saving factor lay in the basic design of the reactor. The water in the primary cooling system of a PWR (Pressurized Water Reactor) or a CANDU (CANadian Deuterium Uranium) reactor is also the moderator i.e., it slows down the neutrons and gives them a chance to hit their targets to produce a chain reaction. It also reflects neutrons back into the pile. When water is lost accidentally to steam, the moderating and reflecting effect is reduced and the reaction slows down: this is known as having a negative void coefficient. By way of contrast, in the Chernobyl design, the moderator is graphite and moderation is not affected by LOC (Loss of Coolant); the reactor simply gets hotter. This is known as a positive void coefficient.

General Remarks

The persistence of mental pictures formed early in an emergency is a major cause of accidents. This was clearly the case at Three Mile Island. It was the case when an Iranian air bus was destroyed with the loss of 290 lives by US Navy Cruiser Vincennes on July 3rd 1988. The enquiry found that, in the stress of "battle", radar operators in the Vincennes mistakenly convinced themselves that the aircraft they had spotted taking off from the airport in Bandar Abbas was hostile and intended to attack the Vincennes. The ultimate mistake was the erroneous belief that the aircraft was descending as Vincennes captain Will Rogers gave orders to shoot it down.

As soon as a system like the AEGIS system in American warships reaches a certain degree of complexity it becomes, in effect, uncontrollable because of unforeseen interactions (close coupling) between subsystems. In many systems there is a fundamental design error that results in subsystems being too tightly coupled, i.e., too much open to mutual influence. An error in one subsystem produces an unexpected result in another subsystem, usually too rapidly for corrective action to be taken. Thanks to Michael Crichton's "Jurassic Park" everyone now has some understanding of this. His character Ian Malcolm, the mathematician, says that the park's safety system must collapse because it is too precariously complex in its coordination of so many and so intricate fail-safe devices.

"It's chaos theory. But I notice nobody is willing to listen to the consequences of the mathematics. Because they imply very large consequences for human life. Much larger than Heisenberg's principle or Gödel's theorem, which everybody rattles on about... But chaos theory concerns everyday life... We have soothed ourselves into imagining sudden change as something that happens outside the normal order of things. An accident, like a car crash. Or beyond our control, like a fatal illness. We do not conceive a sudden, radical, irrational change as built into the very fabric of existence. Yet it is... Chaos theory proves that unpredictability is built into our daily lives. It is as mundane as the rainstorm we cannot predict. And so the grand vision of science, hundreds of years old- the dream of total control - had died, in our century".⁶

Complex man-machine systems fail for complex reasons in which it is difficult to separate human agency from mechanical malfunction (Pheasant, 1988). As the systems become more complex the possibilities of failure become significantly greater. Automatic safety devices (ASD) can, of course, only cope with the situations for which they have been programmed: not with the unexpected. Software systems are particularly vulnerable. And when a large software system has been programmed by teams of up to 300 programmers, no single person has a total overview. As one commentator noted "The vast majority of systems are deeply flawed from the viewpoint of reliability, safety, security and privacy". The bug in the Pentium microprocessor had no more serious consequences than some bungled calculations and millions of dollars in losses for Intel. But if they had been running diagnostic or dosage calculations for medical treatment, the results might have been different. In the accident at Reactor 4 of the Bruce nuclear station at Kincardine near Owen Sound Ontario, a single letter typed wrongly in a program lay dormant for four years until "a special conjunction of various factors" led to system breakdown and the escape of 1200 L of highly radioactive water.

Military software is particularly liable to bugs. partly because it cannot be tested under realistic conditions unless one can arrange a war. The loss of the Sheffield to an Exocet in the Falkland Islands war has been quoted as an example. It is said that the Exocet transmitted radar beams on a frequency that was used by Sheffield's communication system. She was transmitting a message to London when the Exocet came in undetected. Sheffield's defence system had been designed to protect her from Soviet missiles not from French ones. There was therefore an unexpected interference between two subsystems.

In the next section I discuss what can be done to reduce accidents.

Technological solutions and "fixes".

I. Many technological solutions have been shown to be effective. Some of these would be classified as "fixes" because they are a technological substitute for standards of training and alertness which the industry seems not to be able to attain. Bumping into the ground by aircraft, known as CFIT (controlled flight into terrain) was the most common form of serious flying accident until the introduction in 1975-1976 of the Minimum Safe Altitude Warning (MSAW) and the Ground Proximity Warning System (GPWS) which sounds a horn and shouts "Pull Up". Some studies argue that automation has gone too far and crews have difficulty in maintaining attention. The A320 Airbus is almost fully automated, but four have crashed in the period June 1988- January 1996.

II. There are cases a technological solution is practicable but unprofitable for the corporation. The exploding gas tank of the PINTO could have been fixed for 11\$ per auto. But cost/benefit studies apparently indicated that it would be cheaper to pay out claims for the estimated 180 deaths/a.

III. There are cases where there is no incentive for the operator to find a solution because the victims are external to the system e.g. third party victims such as innocent bystanders or fourth party victims such as those unborn at the time of their parent's involvement. Acid rain

is a good example of the costs being born by third party victims. The dioxin accidents may have fourth party victims.

IV. In certain classes of accident, it is thought that the organizational framework rather than the hardware is at fault. For example in marine accidents which show a continuing high level, the rate per work unit increased 74% over the 1970-80 decade. The loss rate is still about 1 ship per day. There are two major technical problems in marine navigation. One is that one cannot see the bottom, the shore, bridges etc. and the other one is the relative motion of tide, wind, and ship. The major technological fix has been radar. But after the introduction of radar the collision rate did not go down. Speed went up⁷

Collision avoidance systems have been developed as a technological fix. But an analysis of past accidents shows that only 1 in 10 could have been avoided with CAS. The system requires a stable course and in most cases manoeuvring prevented its determination.

The electronic chart display system (ECDIS) recently introduced by Canada Steamship Lines will probably have the same effect. ECDIS is the first full alternative to plotting a ship's progress on a paper chart. Detailed charts are digitized and stored on a colour monitor. Satellite signals allow a skipper to pinpoint a vessel's location to within 10 m and watch on the monitor as its real-time progress along a set course is updated twice every second regardless of weather.... For CSL, the ability to operate in extreme weather, including fog and ice that may idle non-ECDIS Ships, amounts to a competitive advantage which will "have" to be exploited (the "economic imperative").

The error-inducing character of the marine system lies partly in the social organization of the personnel aboard ship, the economic pressures operating, the structure of the industry and insurance, and the unregulated climate in which marine transportation operates. On a ship the captain is the absolute master and yet the complexity of modern technology is such that one man cannot master it. It became clear in the enquiry into the loss of the Ocean Ranger drilling vessel that the Captain did not understand the stabilizing equipment. The technology exists to prevent ships straying ten nautical miles off course as in the case of the tanker EXXON Valdez. The ship was said to have had all the latest navigational aids. But it ran aground.

By contrast, the crew of an aircraft has developed a much more cooperative culture. Their danger arises more from the gender roles of the crew which, by preventing men from showing fear, have on occasions prevented them from showing prudence. The Air Florida crash in 1987 was caused by ice build up on the wings. The flight recorder confirms that the First Officer noticed it but, instead of doing anything, he and the Captain made jokes about it⁸.

To sum up these remarks on accidents it is clear that both human and technological factors are involved. Complexity adds to the probability of system failure generally through unforeseen interactions between subsystems. For a serious accident to occur it is usually necessary for there to be failure in more than one component of the system and some human error.

Selected References

Report of the President's Commission On the Accident at Three Mile Island. *The need for*

change: The legacy of TMI. Washington DC: United States Government Printing Office, 1979.

[TK1344 .P4 U65]

Brooks, G.L. and E. Sidall (1980). *An analysis of the Three Mile Island Accident.* Mississauga ON: Atomic Energy of Canada Ltd.

Review questions

1. Discuss the statement "Most accidents are caused by human error."
2. From the point of view of safety, what is the most important difference in design between a PWR or a CANDU reactor and the reactor at Chernobyl?
3. Describe some hazardous situation known to you and suggest both a technological fix that might make it safe and a behavioural change that might make the fix superfluous. What considerations ought to govern the choice of solution?

¹Pheasant, 1988

²deMarco & Lister

³AP London: "A-accident hushed up, papers say." Globe & Mail 1989, January 3, p.A8. 800 farms were contaminated with high levels of Sr-90 but public was not warned and matter was hushed up until McMillan's papers released in 1986.

⁴See IEEE *Spectrum*, 1979 for Special Report on Three Mile Island.

⁵Atomic Energy of Canada analysis of the accident. (Brooks and Siddall, 1980)

⁶Quotations taken second hand from Stephen Jay Gould, New York Review, 12 August 1993 p.53.

⁷Globe and Mail Report on Business 20 Apr. 1993.

⁸Herald Sunday Magazine 13 Dec 1987 p.4