No2NuclearPower.org.uk Briefing January 2007

Nuclear Reactor Safety

- A recent simple power failure at a Swedish nuclear plant highlighted our vulnerability to nuclear catastrophe.
- A nuclear chain reaction must be kept under control, and harmful radiation must, as far as possible be contained within the reactor, with radioactive products isolated from humans and carefully managed.
- Nuclear reactions generate high temperatures and fluids used for cooling are often kept under pressure. Together with the intense radioactivity the high temperatures and pressures make operating a reactor a difficult and complex task.
- The risks from operating reactors are increasing and the likelihood of an accident is now higher than ever.
- New reactors start with a higher risk as they are broken in.
- Reactors in mid-life should theoretically be the lowest risk, but operators are under pressure to increase power output and cut back on safety inspections.
- Most of the world's reactors are more than 20 years old and therefore more prone to age related failures.
- Many utilities are attempting to extend the life of their reactors from the 40 years or so they were originally designed for to around 60 years.
- New so-called passively safe reactors have many safety systems replaced by 'natural' processes, such as gravity fed emergency cooling water and air cooling. This can make them more vulnerable to terrorist attack.

Introduction

On 25th July 2006 the main power supply to the Forsmark-1 reactor in Sweden was interrupted. Two of the four backup generators failed to start, but luckily two were sufficient to run part of the plant's cooling system. If they hadn't started there could have been a catastrophic meltdown. (1) A former director of Forsmark commented that: "*it was pure luck there wasn't a meltdown*". For 20 minutes, workers were unable to obtain information about the condition of the reactor and were only able to respond after 21 minutes. (2)

The incident highlighted how frequently incidents have occurred in several countries in different reactor types, and how vulnerable we are to nuclear catastrophe. There have been widespread and frequent problems in the US and Germany (3). And a similar incident took place in the Belgian reactor Tihange 2 on 4th July 2005, where 2 out of 3 power backup systems failed during a test (4). Power blackouts such as happened in the US and Canada in 2003 - forcing more than 20 reactors to close - can very easily lead to a catastrophic reactor meltdown, if backup systems fail. A report by the US Nuclear Regulatory Commission (NRC), revealed that 50% of all meltdown scenarios are initiated by plant blackout (5). The Forsmark fault originated in equipment installed in 1993. The same faulty equipment has also been installed at other nuclear power plants in other countries.

Reactor Design and Operation

Nuclear reactors run on fissile material – usually uranium-235 – which is capable of sustaining a chain reaction thus generating heat. To start a chain reaction inside a reactor you need neutrons. In a lump of uranium there will always be a few stray neutrons. To start up the nuclear chain reaction, the neutron absorbers – or control rods – are withdrawn slowly from the core of the reactor. Stray neutrons can then split the nucleus of uranium-235 so that it undergoes fission and releases more neutrons and so beginning a chain reaction. (6)

But before pulling the control rods out and allowing a self sustaining chain reaction to go-ahead, you need to make sure that radiation is not pouring out of the core. So you need to surround the reactor with enough concrete or some other protective shielding to cut down the radiation outside to as low a level as possible. The fissile material, or fuel, is sealed into casings called ‘cladding’ to support the fuel and to confine the waste fission products that will be produced. Assemblies of sealed fuel called ‘fuel elements’ are interspersed with a ‘moderator’ to slow down the neutrons and a neutron absorber (the control rods) to control the chain reaction.

The nuclear reaction or fission that goes on inside a nuclear reactor gives rise to fission products, that are generally far more radioactive than uranium-235. As a result, the more energy generated from a batch of fuel, the more radioactive the fuel becomes. Severe accidents in nuclear reactors could produce a great deal of harm, if these fission products were to escape. Even if everything goes according to plan the waste produced requires very careful management. (7) Neutrons also make the reactor itself intensely radioactive. This makes reactor maintenance and repair as well as disposal of used reactors far more difficult and costly than with conventional power plants.

Once the chain reaction is going, heat must be removed from the reactor by pumping a heat-absorbing fluid through the core, past the hot fuel elements. The fluid can be a gas, such as carbon dioxide, or a liquid such as water or even molten metal. To avoid problems if there is a leak in the fuel cladding this cooling system is usually a closed circuit, and can also be pressurised – a pressurised gas is denser and can carry more heat per unit volume, but has implications for safety, because a rupture of the cooling circuit might have serious consequences. The heat is used to generate steam in a secondary system which is used to drive turbines to generate electricity.

So with different fuels, moderators, control systems, cooling arrangements, spatial configurations and protective shieldings, there are hundreds of different possible reactor designs.

Reactor Hazards

So the basics of nuclear safety are:-

- It is essential to maintain control over the chain reaction. Operators need to be able to insert control rods (which are neutron absorbers) to stop the reaction at any time.
- Fission products must be contained within the reactor.
- Radiation escaping from the reactor must be kept to a minimum
- The reactor must be kept cool by use of a coolant. Without a coolant, continued production of fission energy would cause the reactor vessel and its contents to get very hot. This would rapidly lead to a melting of the fuel - a "meltdown."
- Coolant circuits must be carefully managed to avoid rupture especially if the coolant is kept under pressure.
- Given the intense heat, special care must be taken with components which might be prone to catching fire – such as the moderator or the fuel cladding.

A major study of reactor hazards by two leading scientists and an international energy specialist, published by Greenpeace in April 2005, concluded that risks from reactors in the West have been significantly increasing over the last few years and the likelihood of accidents occurring is now higher than ever. The authors argue that all operational nuclear reactors have very serious inherent safety flaws, which cannot be eliminated by safety upgrading, and a major accident in a reactor today could be far more severe than Chernobyl, the world's worst nuclear accident, which took place on 26th April 1986.

The study also concludes that:

- New reactor lines are envisaged which are heralded as fundamentally safe, but these have their own specific safety problems;
- De-regulation (liberalisation) has pushed nuclear utilities to decrease safety-related investments and limit staff; increase reactor pressure and operational temperature and the burn-up of the fuel. This accelerates ageing and decreases safety margins. Nuclear regulators are not always able to fully cope with this new regime;
- The average age of the world's reactors is around 21 years and many countries are planning to extend the lifetime of their reactors beyond the original design lifetime. Age-related degradation mechanisms are not well understood and difficult to predict;
- Reactors cannot be sufficiently protected against a terrorist threat. There are several scenario's – aside from a crash of an airliner on the reactor building – which could lead to a major accident; (8)

The changing risk profile

The Union of Concerned Scientists (UCS) described the profile of risk over the lifetime of a reactor as a ‘bathtub’ curve. New reactors start out as a high-risk as they are ‘broken-in’. In the middle of their life, reactors should be in peak health where the risks are at their lowest. Then as reactors get older they enter a ‘wear-out’ phase with a high risk that components will wear out and fail. (9)

There are several examples of disasters, which happened during the ‘break-in’ phase – Fermi, Three Mile Island and Chernobyl. Literally thousands of unexpected safety problems have surfaced at new reactors. UCS say that public interventions in the licensing process for new reactors has in the past led to numerous safety improvements. The global trend of reducing the opportunities for public intervention in the licensing process in order to drive down costs is therefore particularly worrying. Indeed the US Nuclear Regulatory Commission (NRC) says public participation greatly enhances safety, and has documented numerous examples of reactor safety improvements, which have resulted from public participation. Unfortunately the NRC, bowing to industry pressure, has now virtually eliminated public participation from the process. (10)

With regard to new reactors UCS recommend that: (a) they are excluded from any State limited liability schemes for accidents to encourage vendors to design in safety upgrades (and instead take out their own insurance); (b) prototype reactors must be used to verify safety performance before commercial reactors are built; (c) there should be extensive inspection of new reactors during design and construction to verify compliance with regulations; (d) there must be meaningful public participation in the licensing process.

New reactors with teething problems

* Fermi Unit 1 (Michigan) began commercial operation in August 1966. A partial meltdown on October 5, 1966, caused extensive damage to the reactor core.

* Three Mile Island Unit 2 (Pennsylvania) began commercial operation in December 1978. On March 28, 1979, a partial meltdown prompted the evacuation of nearly 150,000 people.

* St. Laurent des Eaux A1 (France) started up in June 1969. Nearly 400 pounds of fuel melted on October 17, 1969, when the online refueling machine malfunctioned.

* Chernobyl Unit 4 started up in August 1984. It suffered the worst nuclear plant disaster in history on April 26, 1986, when two explosions destroyed the facility and ignited a reactor fire that burned for more than a week. Dozens of plant workers were killed and thousands of people permanently relocated.

Liberalization imposes mid-life crisis

In the middle of their life, reactors should be in the peak of health and risks should be at their lowest. Unfortunately the global trends of deregulation and liberalization have increased pressure on operators to maximize power output, and cut back on safety inspections.

Probabilistic Risk Assessments are used to calculate the odds of specific events occurring (such as the breaking of a pipe that carries cooling water to the reactor) and the odds of a plant's numerous safety systems being unable to prevent damage to the reactor core. Nuclear regulators often rely on these risk assessments carried out by plant operators for making regulatory decisions. Yet there are numerous examples of deficient risk assessments, used to justify safety cutbacks, such as the decision in 2001 to allow the Davis-Besse nuclear plant in Ohio to continue operating in an unsafe manner.

Vessel head penetration cracking – Davis-Besse

Pressurised Water Reactors have been widely found to leak cooling water from their control rod drive mechanism nozzles. A cap at the top of the reactor pressure vessel contains the pipes that allow the control rods to be inserted into the reactor core. In the early 1990s cracks began to appear in the reactor vessel heads of some reactors in France. Worldwide investigations were carried out and similar problems were found in reactors in Sweden, Switzerland and the U.S.

In 2001 the US Nuclear Regulatory Commission (NRC) had compelling evidence that there were leaks at the Davis Besse reactor in Ohio, and so drafted an order requiring the plant to shut down to check the nozzles. The owners provided the NRC with a risk assessment arguing that the plant should be allowed to operate until its next outage the following year. When checks were finally done it was discovered that leaks had severely damage the reactor vessel. Only a thin layer of stainless steel was left to contain the cooling water in the reactor. It was lucky that the steel did not crack. (11)

A December 2002 report by the NRC's Office of the Inspector General (OIG) found that the NRC's decision "*was driven in large part by a desire to lessen the financial impact on* [the operator]." (12)

An ageing reactor fleet

At the start of 2005 there were 441 nuclear power reactors, operating in 31 countries. Of these, over 300 were more than 20 years old. Clearly, as with any other sort of equipment, as reactors get older there is an increased risk of age-related failures. All the more worrying then that across the globe there is a general trend towards extending the life of reactors.

At the time of their construction it was usually assumed that reactors would not operate more than forty years. However, now, in order to retain the nuclear share of the market and maximize profits—with, in theory, the large construction and decommissioning costs paid for—life-extension offers an attractive proposition for nuclear operators. In the US between 2000 and 2005 32 reactors, received 20-year extensions to their 40-year life, and applications for 16 more reactors were in the pipeline.

Ageing processes are not always easy to recognize and can increase plant risk considerably. They are difficult to detect because they usually occur on the microscopic level of the inner structure of materials. They frequently become apparent only after a component failure—for example, break of a pipe—has occurred. For a nuclear power plant, whatever the reactor type, the ageing phase will begin after about twenty years of operation. This, however, is a rule-of-thumb number only and ageing phenomena can begin earlier.

Naturally, with Plant Life Extension (PLEX) ageing mechanisms will become increasingly important over the years, contributing significantly to overall plant risk. However, reactors have limited accessibility due to the layout and high radiation levels, so it is not possible to examine all components. Therefore, it is often necessary to rely on model calculations in order to determine the loads and their effects on materials.

UK reactors cracking up

The UK's Nuclear Installations Inspectorate's (NII) have raised serious questions over the safety of Britain's ageing Advanced Gas-cooled Reactors (AGRs), some of which have developed major cracks in their reactor cores. (13) The NII says the operator, British Energy, does not know the extent of the cracks, cannot monitor their deterioration and does not fully understand why cracking has occurred. (14) Continued operation could increase the risk of an accident. It has now demanded that British Energy carry out more frequent checks. The extra inspections might involve reactors closing down more frequently. (15) British Energy is keen to extend the life of its AGRs but the NII says it is faced with "*significant regulatory issues ... for all operating AGR reactors*". (16)

Cracks in boiler tubes were discovered at Hunterston B in August 2006. This lead to investigations at the sister station, Hinkley Point B. By December British Energy revealed that repairs to Hunterston B and Hinkley Point B would not be completed until at least March 2007, and even then they would only run at 70 per cent capacity. The problems will wipe £100m off the company's profits for the year. (17)

New reactors

If there is a burst of new reactor building around the world, the reactors built are likely to be the so-called "Advanced Reactors," or Generation III - three of which are already in operation in Japan. About twenty different designs are reported to be under development. Most are "evolutionary" designs developed from existing reactor types. What is most worrying is that many of these new designs - so-called 'passive' safety systems - rely on a completely different safety philosophy.

The Westinghouse AP1000 design, for example, employs passive safety features, which the industry claims makes it *inherently safe.* But there is nothing *inherently* safe about highly hazardous plant, which has a highly radioactive fuel core. In fact, the suspicion is that the AP1000 design is more about saving money than improving safety. Unlike traditional PWRs, AP1000s do not use a "*large network of safety support systems*" (18)

The European Pressurized Water Reactor (EPR) similarly displays several modifications which constitute a reduction of safety margins.

There are two important principles currently used in nuclear safety: redundancy and diversity. (19) Redundancy requires having more than one item to do the same thing so that if one fails there is a backup. Diversity requires having more than one way of doing the same thing so that if there is a generic failure that applies to all of the same type of equipment, then there is also back up for that. The passive safety concept does not adhere to the redundancy and diversity principles. Instead it relies on gravity and convection, or so-called "passive" safety systems. In the present design of PWRs there are a series of valves and pipes designed to supply an "emergency core cooling system". The AP1000 relies upon natural means, including gravity fed water from tanks, to transfer heat from the fuel. Compared with the original PWR, the design has many safety systems stripped out. It has 50 percent fewer valves, 83 percent less piping, 87 percent less control cable, 35 percent fewer pumps and 50 percent less seismic building volume than a similarly sized conventional plant. These reductions in equipment and bulk quantities lead to major savings in plant costs and construction schedules.

Passive systems attempt to avoid relying on nuclear operators to deal with emergency situations, but it is by no means certain that real nuclear reactors will behave in ways the scaled-up theoretical calculations say they will. There is a trade-off in trying to remove human error. What if the emergency event has not been predicted by designers and requires intelligent intervention by the operators? Reliance on passive safety systems could result in a worsening situation with the plant workers left with no means to do anything about it. (20)

Resistance to terrorist attack

In addition to the risk of accident, nuclear plants are highly vulnerable to deliberate acts of sabotage and terrorist attack. Even the International Atomic Energy Agency (IAEA), which promotes the use of nuclear power, admitted that in the light of the September 11th 2001 attacks in New York that most reactors were only designed to withstand the accidental impact of a small aircraft. (21) One might have expected that new reactors would be designed to be less vulnerable to terrorist attack. With the AP1000 design, the reverse is the case. For final heat dissipation the design relies upon air-cooling, so the structural integrity of the reactor dome has been sacrificed. This means the “secondary containment system”, which is supposed to stop radioactivity escaping in a meltdown, actually has a huge hole in it. A proper containment thickness would put the reactor design back on the drawing board. (22)

References

(1) BBC News 3rd August 2006 http://news.bbc.co.uk/1/hi/world/europe/5241780.stm
(2) CNN Europe 3rd August 2006
http://edition.cnn.com/2006/WORLD/europe/08/03/sweden.nuclear.ap/index.html
Spiegel Online 4th August 2006 http://service.spiegel.de/cache/international/0,1518,430164,00.html
(3) Hirsch, H et al (April 2005) Nuclear Reactor Hazards Report. p.121.
http://www.greenpeace.org/international/press/reports/nuclearreactorhazards
(4) AVN, annual report 2005 p. 23. http://www.avnuclear.be/avn/anrep2005.pdf
(5) Hirsch H et al (April 2005) p.121.
(6) For a fuller explanation of how reactors work see Patterson, W (1986) Nuclear Power Penguin available on-line at http://www.waltpatterson.org/nppenguin.htm
(7) Makhijani, A and Saleska, S (1996) The Nuclear Power Deception, IEER
http://www.ieer.org/reports/npd.html
(8) Summary of Ref 3: Froggatt A, (Nov 2005) Nuclear Power Myth and Reality; Nuclear Reactor Hazards. Nuclear Power Issues Paper No.2 Heinrich Boll Foundation.
http://www.boell.de/en/nav/275.html
(9) Lochbaum, D (May 2004) US Nuclear Plants in the 21st Century: The Risk of a Lifetime, UCS
http://www.ucsusa.org/assets/documents/clean_energy/nuclear04fnl.pdf
Lochbaum, D (August 2000) Nuclear Plant Risk Studies: Failing the Grade UCS
http://www.ucsusa.org/assets/documents/clean_energy/nuc_risk.pdf
Lochbaum, D (June 1998) The Good, the Bad and the Ugly: A report on safety in America’s Nuclear power Industry, UCS
http://www.ucsusa.org/assets/documents/clean_energy/ACFKm1toT.pdf
(10) Lochbaum, D (May 2004) page 8.
(11) Lochbaum, D (May 2004), pages 15 & 16 and Froggatt, A (Nov 2005)
(12) Public Citizen, (2005) Nuclear’s Fatal Flaw: Safety
http://www.citizen.org/documents/JTF-Safety.pdf
(13) Guardian 5th July 2006 http://www.guardian.co.uk/nuclear/article/0,,1812795,00.html
Guardian 5th July 2006 http://www.guardian.co.uk/nuclear/article/0,,1812870,00.html
(14) Greenpeace release 5th July 2006 with links to the documents obtained under FoI and comment by Nuclear Engineer, John Large:
http://www.greenpeace.org.uk/climate/climate.cfm?CFID=5143211&CFTOKEN=91461491&UCIDParam=20060705083925
(15) Guardian 6th July 2006 http://www.guardian.co.uk/science/story/0,,1813609,00.html
(16) New Scientist Article 26th March 2006
http://www.robedwards.com/2005/03/cracks_may_forc.html
(17) Independent 21st Dec 2006 http://news.independent.co.uk/business/news/article2091904.ece
(18) Westinghouse AP1000 Background. http://www.ap1000.westinghousenuclear.com/

(19) Layfield (1987) Sizewell Inquiry report. Para 5.52

(20) See Karlheinz Orth, Siemens AG, quoted in “Outlook On Advanced Reactors,” Nucleonics Week, Mar 30, 1989, pp1-20

(21) Kole, W Security (17th September 2001) Security Tightens at Nuclear Plants, Associated Press

(22) WISE News Communique (1998), “New generation: The AP 600”, (492.4881), May 22, 1998, http://www.antenna.nl/wise/492/4881.html