# Nuclear Power Plant Safety

## by H.J.Otway

*In the last decade nuclear reactors have proven to be a source of electrical energy economically competitive with conventional means of power production. With the resulting increase in orders for nuclear power stations there has been a corresponding increase in public awareness of the safety and environmental aspects of these facilities. This public awareness has been evidenced by the number of articles in the world press, either praising or condemning the trend toward nuclear power.*

*Those opposed express concerns which tend to fall into three major areas: the long-term disposal of radioactive wastes, the effects of routine radioactive and thermal emissions, and the effects and probability of large-scale accidents. This article will limit itself to a discussion of the latter item, consistent with space limitations, based largely upon a summary of material from the USAEC report WASH-1250 [1] "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities".*

**The Possible Effects of Catastrophic Accidents**

In the 1950s it became necessary to determine the amount of liability insurance that would be required by the developing nuclear power industry. Therefore, in 1957, the USAEC published the well-known report WASH-740 [2] which was an attempt to estimate the consequences of a catastrophic reactor accident in a hypothetical 500 MW (thermal) reactor located about 50 km from a city of 1,000,000 people. Its title "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants", and its subtitle "A Study of Possible Consequences if Certain Assumed Accidents, Theoretically Possible but Highly Improbable, Were to Occur in Large Nuclear Power Plants", actually summarizes the contents and intent quite well.

The report itself provides a technically sound estimate of the worst consequences possible in the event of a major accident but, it is important to note, physical mechanisms for accident initiation were not considered. That is, accidents that would release a certain amount of fission products were assumed to occur and then estimates were made for the worst possible outcome in terms of mortalities, injuries and property damage.

The calculations were performed under three different sets of assumptions regarding weather conditions, amount and temperature of fission product release, particle size, etc. The predicted results varied widely, depending upon which set of assumptions was used. For example deaths, depending upon assumptions, were estimated to fall between 0 and 3400; injuries from 0 to 43,000 and property contamination from 18 to 150,000 square miles. The consequences of the "worst-case" accident seem severe indeed but it must be noted that this was based upon 50% gross fission product activity released *to the atmosphere* under adverse weather conditions. The physical mechanisms for initiating such a release were not considered, nor was credit given for the types of engineered protective systems which are incorporated into the nuclear power plants of to-day. An atmospheric release of 50% of all fission products is to-day considered to be much higher than could occur in a real reactor accident.

### Defence in Depth

In 1973 the USAEC published WASH-1250 [1], a review of the current status of the safety and environmental aspects of nuclear power plants. This report, in some respects an up-dating of the WASH-740 material, also presents the basic design philosophy for assuring nuclear power plant safety – *"defence in depth"*. This philosophy defines three levels of safety:

> *The first level is to design and build the plant so it will operate as intended with a high degree of reliability. This level addresses the* prevention *of accidents through intrinsic design features and stresses quality control, redundance, testing, inspection and fail-safe design.*
>
> *The second level follows the first by assuming that, despite efforts to prevent accidents, it is prudent to* anticipate *that one might occur. Therefore reliable protection devices are provided to prevent or minimise the effects of an incident. Such devices include an emergency core cooling system (ECCS) to provide adequate core cooling in event of a loss of coolant accident, engineered limits on the rate of power increase, a fast reactor shutdown (SCRAM) system activated by redundant and independent instrument channels, an independent supply of off-site power.*
>
> *The third level of safety supplements the first two by features which add* design margin *by assuring protection of the public even if seemingly remote and unlikely events occur. This is done by evaluating the design concept under conditions of severe hypothetical accidents, such as the assumed independent failures of redundant protective systems simultaneously with occurrence of the accident they were designed to control. In this respect several Design Basis Accidents (DBA) are considered, the best-known being the loss-of-coolant accident (LOCA) where a large pipe rupture is assumed to abruptly occur. Other third level design features include protection against (among others) seismic events, tornados, floods, component failures.*

It should be mentioned that there has been a controversy surrounding emergency core cooling systems since semi-scale tests in 1969 indicated deficiencies in the evaluation models and computer codes used in their design. These systems have since been extensively studied with the aims of securing basic research information and establishing new design criteria. In the interim, ECC systems must satisfy required performance criteria under conservative assumptions regarding simultaneous component malfunctions. **Table I** compares the conservative assumptions actually used in design with a set of assumptions thought to represent reality better. The rulemaking process on ECCS criteria in the USA appears to be nearing completion; preliminary indications are that nuclear power plants having ECC systems designed under the old criteria will be subject to power deratings averaging about 5% [3].

### Nuclear Risks in Perspective

It is pointed out in WASH-1250 that the evolving methodology of probabilistic safety analysis appears to offer the best approach for putting the risk from nuclear reactor accidents in perspective. This approach allows weighing the consequences of large-scale accidents by their probabilities of occurance.

TABLE I.* PARTIAL COMPARISON OF REALISTIC ASSUMPTIONS WITH CONSERVATIVE ASSUMPTIONS OF LOCA CALCULATIONS

| Realistic Assumptions | Conservative Assumptions |
|---|---|
| Accident Initiation | |
| 1. Crack in large pipe or ruptured smaller pipe resulting in shutdown and repair. | 1. Double-ended or major break of largest pipe. |
| Electrical Systems | |
| 1. Off-site power is available. | 1. Off-site power is not available, and one of multiple emergency diesel generators fails to start. |
| Power | |
| 1. The plant is operated at 100% power or less. | 1. The plant is operated at 102% power (PWR), 105% power (BWR) continuously to account for possible instrument errors. |
| 2. Hottest region of core has expected peaking factor. | 2. Hottest region of core assumed to be at the maximum allowable peaking factor due to abnormal condition. |
| 3. Decay heat follows best estimate prediction. | 3. Decay heat is conservatively above best estimate to account for uncertainties in prediction. |
| ECCS | |
| 1. All components of the ECCS operate when called upon. | 1. The "worst consequence" single active component fails to operate when called upon. |
| 2. Break occurs in system such that some of water from ECCS reaching broken loop is effective. | 2. All water from the ECCS reaching the broken loop is lost to the containment (PWR only). |
| 3. Pumps deliver at higher than design flow rate. | 3. Pumps deliver at design flow rate. |
| ECCS Performance | |
| 1. Reactor coolant pumps continue to run. | 1. Reactor coolant pumps are tripped and coasting down or assumed to have a locked impeller. |
| 2. Some emergency water delivered during the blowdown reaches and remains in pressure vessel. | 2. All emergency water delivered during the blowdown is lost (PWR only). |
| 3. Best estimate heat transfer coefficients used. | 3. Conservative lower heat transfer coefficients used. |
| 4. Fuel rods will have a distribution of temperature. | 4. Attention is focused on the hottest single fuel rod. |

* From Reference 1.

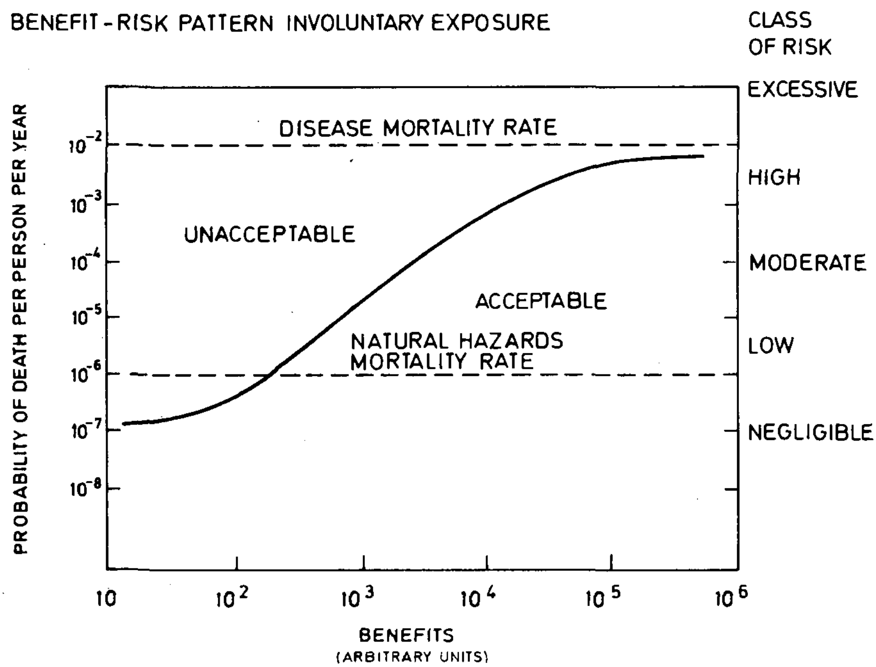
Many of the routine activities of life have an associated possibility of sudden death or injury connected with them. Participation in these activities continues because there is also an associated benefit which seems to outweigh the risks involved. This risk-benefit process is followed on a personal basis even though the assessments of risk and benefit are usually made in a subjective, intuitive way. In fact, there is virtually no such thing as a perfectly "safe" activity, there is always the probability, however small, of an accident occurring. For example, even the necessary acts of eating and breathing have an associated risk; over 1000 people die each year in the U.S.A. due to inhalation or ingestion of objects leading to suffocation. (In risk terms, based upon a population of 200 million, this is expressed as an average risk of $5 \times 10^{-6}$ per person per year:

$$\frac{1000}{200,000,000} = \frac{5}{1,000,000} = 5 \times 10^{-6}/\text{yr})$$

It has been noted [4] that risks below $10^{-6}$ per person/year (1 in 1,000,000) appear not to be of much concern to people and, indeed, people are hardly aware of them. Likewise, Starr [5] has postulated that, in the USA, accident risks higher than $10^{-2}$ per person/year (the US average risk of death from natural causes) appear to be clearly unacceptable. However, as noted earlier, participation in activities involving risk is also related to the magnitude of the benefit expected. **Figure 1** has been proposed as a graphic portrayal of the division between "acceptable" and "unacceptable" risk levels as a function of the benefit derived. The question now is one of estimating the risk presented by nuclear power plant accidents and putting it into perspective.

FIGURE 1*

BENEFIT - RISK PATTERN INVOLUNTARY EXPOSURE




* From Reference 7.

Early work in estimating the probability of large-scale accidents [4,6] summarized in WASH-1250, has indicated that the probability of a catastrophic accident in a nuclear power plant is very small – in the order of $10^{-9}$ to $10^{-10}$ per year. ($10^{-9}$/year means 1 chance in 1,000,000,000 per year of operation). Preliminary results from more thorough study in U.S.A. [3] appear to be in rather close agreement. Results of Refs. 4 and 6 have been interpreted in WASH-1250 to imply an average mortality risk to people living in the vicinity of a nuclear power plant of about $10^{-10}$ per person/year.
In comparison with the relationship of **Figure 1** this risk is seen to be trivial, even if there were no benefit involved – yet there is an obvious benefit provided in the form of electrical energy.

Another way of placing this nuclear risk in perspective is by comparison with other risks common in the U.S.A. **Table II** provides some other average mortality probabilities which may be compared with the value of $10^{-10}$ per person/year estimated for those living near nuclear power plants.

TABLE II.* SOME MORTALITY RISK STATISTICS (USA)

| Hazard | Mortality Risk/person/year |
|---|---|
| Cancer (all types) | $1.6 \times 10^{-3}$ |
| Auto accident | $2.8 \times 10^{-4}$ |
| Drowning | $3.7 \times 10^{-5}$ |
| Poisoning | $1.2 \times 10^{-6}$ |
| Cancer (Medical X-rays) | $1 \times 10^{-5}$ |
| Choking on food | $5 \times 10^{-6}$ |
| Lightning Strike | $8 \times 10^{-7}$ |
| Natural catastrophe | $6 \times 10^{-7}$ |

* From References 1 and 4.

Another study [7] has compared the public health risks from nuclear and fossil-fuelled power plants. The results indicate that the overall risk from the nuclear plant is lower, perhaps by as much as a factor of 10 to 100.

This discussion of risk is only a superficial treatment of a complex and interesting topic; due to space limitation many aspects have not been discussed at all. Dunster [8] has recently published a summary of the cost-benefit philosophy as applied to nuclear power. Those interested are referred to WASH-1250 or to the original references [4-8] for further reading.

**International Aspects**

Action at the international level will assume greater importance as the number of nuclear power plants increases, especially in the more densely populated parts of the world. Predictions of growth made prior to October 1973 [9] indicated that, by 1980, 14% of the electricity would be supplied by nuclear plants and by the year 2000 this figure would be about 50%. This will make the topic of international co-operation and standards of even greater importance.

The IAEA has long been active in providing assistance to Member States in the siting design and operation of nuclear reactors. These activities have been pursued through advisory missions, the publication of codes of practice, guide books, technical reports and in arranging meetings to promote information exchange.

During the early development of nuclear power, there was no well-established body of experience which would allow formulation of internationally acceptable safety criteria, except in a few special cases. Hence, nuclear power plant safety and reliability matters often received an *ad hoc* approach which necessarily entailed a lack of consistency in the criteria used and in the levels of safety required.

It is clear that the continuation of an *ad hoc* approach to safety will prove inadequate in the context of a world-wide nuclear power industry, and the international trade which this implies. As in several other fields, the establishment of internationally acceptable safety standards and appropriate guides for use by regulatory bodies, utilities, designers and constructors, is becoming a necessity.

The IAEA is presently planning the development of a comprehensive set of basic requirements for nuclear power plant safety, and the associated reliability requirements, which would be internationally acceptable, and could serve as a standard frame of reference for nuclear plant safety and reliability analyses.

## REFERENCES

[1] "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities", U.S. Atomic Energy Commission Report WASH-1250, July 1973.
[2] "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants", U.S. Atomic Energy Commission Report WASH-740, March 1957.
[3] "Rasmussen Study, ECCS, Standardization are First Day Topics", news item in Nuclear Industry, January 1974, p.22.
[4] OTWAY, H.J. and ERDMANN, R.C., "Reactor Siting from a Risk Viewpoint", Nuclear Engineering and Design, 13 (1970) pp.365-376. North-Holland Publishing Co.
[5] STARR, C., "Benefit-Cost Relationships in Socio-Technical Systems", presented at the Symposium on Environmental Aspects of Nuclear Power Stations. Organized by IAEA in co-operation with USAEC, UN Headquarters, New York, August 10-14, 1970. IAEA Publication STI/PUB/261 Vienna, 1971, pp.895-917.
[6] OTWAY, H.J., LOHRDING, R.K., and BATTAT, M.E., "A Risk Estimate for an Urban-Sited Reactor", Nuclear Technology, Vol.12, October 1971, pp.173-184.
[7] STARR, C., GREENFIELD, M.A., HAUSKNECHT, D.F., "A Comparison of Public Health Risks: Nuclear vs Oil-Fired Power Plants", Nuclear News 15, October 1972, pp.37-45.
[8] DUNSTER, J., "Costs and Benefits of Nuclear Power", New Scientist, 18 October 1973, pp.192-194.
[9] EKLUND, SIGVARD, "Nuclear Power, Safety and Environment", in this issue of the Bulletin.