Safer Nuclear Energy for the Future

byDan Meneley PhD, PEng
Atomic Energy of Canada Limited (Engineer Emeritus)
Presented at the 28th International Summer College on Physics and Contemporary Needs
30th June to 12 July 2003
Nathiagali, Pakistan

Introduction

The first question that arises under this heading is "Why?" Why do we need safer plants? Nuclear fission reactors have been used in power production for about 50 years. Over 400 power plants are operating in the world. A totally new energy supply has reached maturity thanks to the efforts of thousands of dedicated and brilliant people. Safety has been a paramount consideration since the beginning. Why do we now need even safer plants?

Two reasons are apparent. First, many people in the world are uncomfortable about the potential for disastrous accidents during operation. Though these fears may seem to be greatly exaggerated, their importance cannot be denied – they have had a profound negative influence on nuclear energy planning and installation over the past 40 years. They must be considered very seriously in the future.

Second, the future need for nuclear generating capacity is expected to be very large. As fossil fuel prices escalate the use of these fuels will become less and less affordable, so nuclear plants gradually will be substituted for them. Horizontal diversification into hydrogen production, transportation fuel production and many other energy-related products is likely. The world installed capacity some 50 years from today may be equivalent to at least 1000 units, each of 1000 MW output, or about 2 ½ times today's capacity. The following 50 years might see a further 10-fold increase. In such a world, each of these nuclear plants must achieve an even higher level of public protection than exists today.

I. Safety Perspectives

The content of these four lectures reflects my own opinions, and in no way represents nor reflects the policies of Atomic Energy of Canada Limited. These opinions are the result of my interactions with this technology, and the people who have developed it, over the past forty years. The topic of safety is very broad. In this space I can present only a few poor words as an attempt to convey my own view of some important aspects of safety improvement.

It is common to assume that what we need to satisfy the people is a set of safer "technical fixes" that (we assume) will solve the problems of nuclear energy. A slightly different perspective is presented in these lectures. The technical examples given here relate mostly to the CANDU-PHWR system, simply because it is the system with which I am most familiar. Most of the lessons can be applied, however, to any nuclear plant concept.

I.1 Do You Feel Safe?

Given any situation (such as an aircraft in flight) an individual either feels safe or does not feel safe. This is hardly an objective concept. However, engineers work in the real world, and this world is governed by people who are guided mostly by this innate feeling, and not by the commonly used term "the cold, hard, facts." When you tell a new acquaintance about your work, and you confess that you have spent half a lifetime working on nuclear power development, the most common first reply is "This is scary, isn't it?" After the next half hour of explanation that it really is not scary, most people are reassured – but not comforted. Most are still afraid. Such reassurance might serve as a convincing factor when everything is going well, but it quickly breaks down, and the fear takes over, when an accident occurs such as an aircraft crash or power plant accident)In my opinion, safety cannot be properly addressed only in rational terms like reliability, defence in depth, and so on. To be successful, proponents must address the underlying fear of nuclear energy, as well.

The task of the safety engineer is to give most people a well-justified, safe feeling about the nuclear energy supply system.

I.2 Objectives of Nuclear Safety

Three objectives are apparent: protection of the public, protection of the operating staff, and protection of the plant itself. Public protection is, naturally, the central issue considered during design and licensing proceedings. Protection of the plant is clearly in the interest of the owner. The owner's desire for investment protection lines up very well with the regulator's interest as well as the public interest. Protection of the operating staff also aligns very well with the need to control all releases of radioactive material.

The plant owners first must recognize that the plant they own is "fragile"[2] and can suffer severe and expensive damage even in cases where the public remains well protected. This is a fact, but not a fact that features in many sales brochures published by nuclear plant vendors. The people who own and operate the plant clearly have an interest in its safe operation. If the plant is damaged the first consequence falls on their staff and their financial investment. Economic assessments should, but most often do not, include the actuarial risk of losses (both production and material losses) during plant operation.

The safety regulator is in a position where he/she is charged as the auditor of the owner's safe performance. The regulator acts on behalf of the people – and so obviously has a central interest in safety. Issuance of an operating licence is an explicit delegation of responsibility to operate the plant within the defined bounds. Commensurate authority also is delegated to the licensee. Responsibility, of course, also remains in full force with the regulatory agency. It cannot be reduced by delegation. Authority to operate confers on the operating organization the ultimate responsibility for safety[3].

I.3 The Human Side of Safety

A well-designed plant can be operated poorly and as a result might produce a major accident, while a poorly designed plant can be operated with care by competent operating staff, and as a result might be very safe. Lapses in care, knowledge, or attention are a consistent pattern in most major accidents, and it appears that the real standards of operational safety are determined largely by the philosophy of senior management

Close ties exist between the individuals running the plant and its achieved safe record of operation. These people are in the front line of safety. (Plants all have excellent radiation safety records until they begin to operate.). In all industries, post-facto review of accidents always reveals lapses by some humans – politicians, managers, designers, operating personnel, regulators, etc. It appears that a distinction can be made between safe and unsafe facilities, by examining the attitudes of senior management. These attitudes are infused throughout the organization and eventually result in failures. Poor management is the real root cause of most accidents. Regulatory oversight at the management level may be the most effective strategy to sustain safe operation.

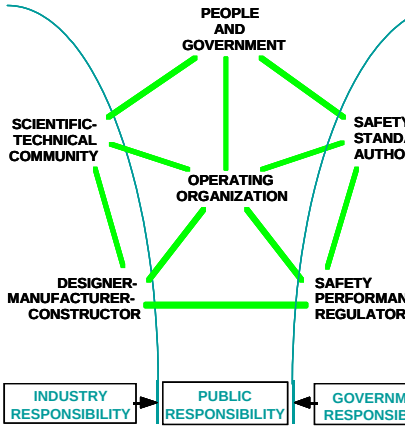

Figure 1 – Safety Management System

I.4 Idealized Safety Management System

The diagram is intended only to represent primary working relationships and responsibilities. It is not an organization chart.

The base triangle shows the designer/builder at one apex and the regulatory staff at the other apex – and both supporting the operating organization that carries the primary responsibility for public safety. The authority for action by regulatory staff flows from the government-appointed Safety Standards Authority. The government establishes Safety Standards on behalf of the people. (International standards have no force within a country – but may be adopted by the government in some cases.) The scientific-technical community provides technical authority for safety. The government registers some members of this community under various education statutes. These statutes sometimes include the establishment of self-regulating engineering associations. Together, these two organizations carry technical responsibility for safe plant designs. Finally, the operating organization is supported and is delegated the authority to operate the plant within the bounds defined by technical and regulatory requirements. Engineering support for operations continues through the whole life of the plant.

I.5 Future Design Opportunities

Given today's advanced capability for automatic control and operation, the panel operator's cognitive ability will, in the future, be mostly reserved for analytical tasks and trouble-shooting. The panel operator's tasks will consist mostly in monitoring of automatic operation, monitoring of the state of plant systems, and initiating manual corrective actions as and when required. Extensive engineering support will be made available to the operating staff.

In addition to the well-developed nuclear safety design principles, the idea of "accident management" has been introduced to limit maximum consequences following any accident. In

the future, plant designs can be chosen to further limit these consequences. This design direction is illustrated by the design concepts used in the most recent CANDU-PHWR plants, and well as those from other reactor vendors. Even today, German law requires designers to prove that no rapid evacuation of the population will ever be required following any accident in a new LWR plant in Germany.

I.6 Limits of SafetyThe common assumption in nuclear plant safety analysis is that accident consequences are inversely proportional to their frequency of occurrence. Plant designs that rest on this assumption are vulnerable to criticism, in that they are capable of producing disastrously large consequences, albeit at some very low probability. Furthermore, recent evidence[5,6,7] indicates that unexpected events occur at an approximately constant rate in mature, tightly coupled, complex systems such as nuclear power plants.

James Reason[8] concludes that unexpected events are likely to be initiated at the human-machine interface. Given this and the possibility of large post-accident consequences, easily could explain the unease that many people feel in the presence of a nuclear plant. Their rational selves might be reassured by the knowledge that the plant is in good hands and has been designed for a high level of safety, but this reassurance is unlikely to be strong enough to comfort their fears. Another approach should be considered.

I.7 The Next Steps

In the near-term future, the following general design approaches should be examined, aimed toward safer plant operation in the future. First, designers should utilize concepts that reduce the operators' workload. This step is a logical part of an approach that recognizes human performance as the main determinant of operational safety. Continuing a long-standing trend, designers are encouraged to use concepts that minimize the <u>likelihood</u> of plant damage. Further, features such as a large low-pressure heat sink inside containment can delay challenges to containment after shutdown. This principle follows the invocation "delay, delay, delay -- decay, decay, decay"; both heat production rates and residual radiation levels decay very rapidly following reactor shutdown. A delayed release from containment is very much less likely to be disastrous than is an early release.

In all instances, designers are encouraged to utilize design concepts that reduce the <u>maximum</u> consequences of any accident, regardless of its probability. This design perspective is intended to improve the "comfort" level of nuclear power plants.

<u>II Past Design Evolution</u>

During the past 50 years several (approximately 20) different power reactor concepts have been developed, at least up to the stage of a large prototype. Most of these prototypes have been decommissioned for one or the other set of reasons: technical, economic, performance, social, and so on. Three successful concepts can be considered to be "mature" at this time – the PWR, the BWR, and the CANDU-PHWR. The largest number of units installed in the world is of the PWR type.

II.1 Operating Experience

Many thousands of minor failures have, as expected, occurred in operating power plants over the past decades. Nearly all of these have been safely protected against by the several systems of defence built into these designs, without any damage to the fuel. (A good measure of successful termination of a failure event, in solid-fuel reactors of this type, is the absence of fuel failures. If this is achieved, release of large quantities of fission products to the environment is essentially impossible.)

Two major failure events resulting in fuel failures have occurred in recent years -- the Three Mile Island Unit 2 accident in 1979 and the Chernobyl Unit 4 accident in 1986.

Three Mile Island Unit 2 was a modern US pressurized water reactor, built to the standards of that day. Errors committed by designers, operators, and regulators led to a partial meltdown of the fuel that threatened the integrity of the pressure vessel. The result was zero environmental or health effects, but large financial losses. Many factors contributed to this complex event, but "unjustified self-confidence" can be seen as its root cause. The plant has not operated since.

Chernobyl Unit 4 was one of a nearly mature group of similar plants built by the USSR. These plants had a moderately long history of successful operation. Errors were committed by government, designers, regulators, managers, and operators that led directly to the death of about 40 people from combined effects of radiation and of an extraordinary fire that was one result of the event. In addition to health effects, the accident incurred a huge cost, equivalent to over 10 billion US dollars. Environmental consequences are still seen, nearly 20 years after the accident.

In addition to these major accidents, there have been several "near miss events" that are judged to be very near to causing fuel failures. One of the most dangerous of these near misses occurred at the Davis Besse PWR, another modern US-designed pressurized water reactor, in 2002. Slow corrosion of the pressure vessel steel led to a drastic weakening, under conditions of full reactor power. The root cause has not yet been finally determined, but a major factor was poor vigilance on the part of operating and management staff, over a period of years.

II.2 Institutional Failure

A different type of failure occurred at Ontario Hydro, an experienced utility in the Canadian nuclear industry, with a long record of successful operation. What is best described as an Operational Breakdown led in 1997 to shutdown of eight large units. Government, company directors, senior management, and others committed sundry errors. The plants were shut down safely, but major financial consequences have followed. Some years earlier, staff was reduced drastically without proper consideration of resources needed for safe operation. Maintenance had been neglected at the several understaffed units. The four units at Pickering A, and at least two at Bruce A now are being extensively refurbished in preparation for restart.

Mosey[9] examined Institutional Failure in the nuclear industry. Clearly, from consideration of the major events listed above, institutional failure played a part in each of them. From another

perspective, the commonly used term "operator error" that appears in many accident reports must be expanded to include senior management and others, in most cases.

Management, because it (by definition) holds a great deal of authority over system operations, must accept some degree of responsibility for many of the failures in the systems. Front-line workers are no less fallible, but for them the consequences of poor performance usually is less damaging. An interesting book by Weick and Sutcliffe of the University of Michigan business school[10] takes up the theme and applies it to a wide analysis of failures in business. That book broadens our understanding of both the effects of the high-reliability approach and the reality of Normal Accidents, as presented earlier by Perrow.

III Today's Development Directions

Only a small number of reactor development efforts are underway in the world at the present time. These "paper" design projects are mainly aimed at significant cost reduction, because of the nearly exclusive desire of potential plant customers for new generation with low capital cost. As for construction of prototype plants, only one program (the PBMR in South Africa) is significant. Most active work among plant vendors is concentrated on refinement, or incremental evolutionary change, based on well established commercially proven designs.

With regard to safety, the dominant design direction at the present time is toward even greater reliance on high reliability systems. This would appear to be a good thing, both for public safety reasons and for protection of the plant investment. One country (Germany) has enacted legislation that explicitly requires new plant designs to limit the consequences of severe accidents to the surrounding population, regardless of accident probability. Germany is, however, very unlikely to undertake any new plant commitments in the foreseeable future.

Regardless of whether or not new reactor development projects are underway, the time taken between the "fully commercialized" state of any plant design and the later time when it can, even under optimistic assumptions, begin to have an important effect on the world energy supply is measured in decades. During the next fifty years, we must plan for a world in which predominant reactor types are nearly the same as those in service today[11]. If we foresee that a particular reactor type will be highly beneficial in about fifty years from today we must begin work on its introduction today, or at the latest within a few years.

Therefore it is very clear that the human performance component of nuclear plant safety is the preferred area for improvement, for two main reasons. First, the performance of all people supporting safe operation during this crucial period will determine whether or not we continue to suffer major accidents and "close calls". If we do continue in this way it is very unlikely that the public will continue to favour nuclear fission technology regardless of how vital it may be as an energy supply in the long term. The second reason to concentrate on the human dimension in safety is because improvements can be achieved in a comparatively short time. The best example is the remarkable improvement in US plant performance during the past two decades. The central motivation for this improvement was economics rather than safety; however, it is apparent from performance indicators that safety also has gained in US plants during this time.

Following is a brief summary of recommendations to designers in the immediate future, (a) reorganize the responsibility and authority structure of operating utilities and other members of the safety management system, (b) ensure that responsibility and commensurate authority are placed in the same hands, (c) recognize the realities of "normal" accidents., and (d) learn to manage the unexpected - it is expected to happen.

IV The Long Term

If a basic change in design direction is needed in the long term then that change must begin very soon, if it is to be effective within 50-100 years. The critical stages of such a change begin with at least one commitment to build a prototype plant featuring the new design. Someone must risk money and resources to make this happen. Within the present day risk-averse logic of world private-sector companies it is very unlikely that such a venture will be initiated. Government, or more likely a collaborative group of governments, is a more likely initiating mechanism for such a change. The weakness of such a venture lies in its distributed authority, wherein competing factions attempt to dominate the agenda, and the final plant design suffers as a result.

However, if we could ignore these difficulties and set off (theoretically) to choose a new nuclear plant concept, what would we wish to incorporate in its final characteristics?

First, the plant must be practical – it must exhibit competitive economics and must minimize the downside risk to its owner and to plant staff. The continuing assurance of low production cost in the long term, and of very low risk of plant damage should be factored into decisions on design alternatives, so that these risks are considered in the design process. One result of this approach will be higher assurance of good reliability and protection from plant damage. A second result will be a fuel cycle that assures a sustainable fuel supply forward about 100 years from the time the plant is built.

The second high priority choice would be for the plant to be run by a competent, dedicated and 'mindful'[10] operating staff. While it is relatively easy to assemble an excellent staff, it is much more difficult to sustain that excellence for several decades corresponding to the plant's useful life. Performance oversight and review must be a continuous process. Designs that simplify the operator's tasks, that use automatic systems to continuously monitor the condition of the plant systems and components, and designs that 'package' complex functions to the extent possible are more likely to support safe operation in the long-term future. Replaceable components and systems also will assist in achieving this goal.

Recognizing that failures will occur during operation, defence in depth will remain a key aspect of design. Designers also should recall the advice of Dr. John Foster[12], an early engineering manager at AECL: that a nuclear plant should be robust and sturdy -- more akin to a "Gravel Truck" than to a "Formula 1 Racer".

The ultimate defence against serious harm to the public is a plant design that cannot cause major consequences as a result of severe damage to its components and systems, at any frequency. Some designs approach this goal today, and some have inherent characteristics that make that target relatively easy to achieve. Combined with excellent defence in depth, this ultimate

protection feature will permit nuclear energy to fulfill its promise of an abundant energy supply for humanity throughout the coming millennia.

V. Conclusion

Many opportunities exist for improving the safety of nuclear power plants, both in the everyday sense of reliable, steady plant operation and in terms of the greatest public safety concerns; that is, major accidents leading to offsite consequences. Introduction of significant improvement to the whole 'fleet' of the world's nuclear plants will take several decades; however, there is a real opportunity to improve the safety performance of the human safety management system in the short term. To begin, workers engaged in this great enterprise should first carefully consider what needs to be improved, and should then proceed confidently to build this new, excellent, and renewable energy source for the benefit of humanity.

References

1. Wolf Haefele, "Energy in a Finite World - Paths to a Sustainable Future", IIASA, Laxenburg, Austria, (1981) ISBN 0-88410-641-1
2. G. Vendryes, Electricite de France, Private Communication.
3. International Nuclear Safety Advisory Group, "Basic Safety Principles for Nuclear Power Plants", INSAG-12, 75-INSAG-3 Rev. 1, (1999).
4. R.B. Duffey & J.W. Saull, "Know the Risk", Butterworth Heinemann, (2001), ISBN 0-7506-7596
5. C. Perrow, "Normal Accidents", Princeton, (1999), ISBN 0- 691-00412-9
6. K. Ott & G. Campbell, "Statistical Evaluation of Design-Error Related Nuclear-Reactor Accidents, NSE **71** (1979)
7. S. Sagan, "The Limits of Safety", Princeton (1993), ISBN 0-691-02101-5
8. J. Reason, "Human Error", Cambridge, (1990), ISBN 0-521-31419-4
9. D. Mosey, "Reactor Accidents -- Nuclear Safety and the Role of Institutional Failure", NEI Special Publications, Butterworth Scientific Ltd., (1990), ISBN 0-408-06198-7
10. K.E. Weick and K.M. Sutcliffe, "Managing the Unexpected – Assuring High Performance in an Age of Complexity", Wiley & Sons, (2001), ISBN 0-7879-5627-9
11. Key Issue Paper #3, "Nuclear Fuel Cycle and Reactor Strategies: Adjusting to New Realities", IAEA International Symposium, Vienna, (1997)
12. J.S. Foster, private communication