IAEA-CN-39/211

OPTIMIZATION OF NUCLEAR SAFETY SYSTEMS

D. BENINSON, A.J. GONZALEZ
Comisión Nacional de Energía Atómica,
Buenos Aires,
Argentina

Abstract

OPTIMIZATION OF NUCLEAR SAFETY SYSTEMS.

The paper presents an approach for selecting the level of ambition of nuclear safety by a process of optimization based on cost-benefit considerations. Optimization has been incorporated as a requirement for radiation protection, to keep doses "as low as reasonably achievable". In radiation protection, optimization takes account of the costs of protection and the costs of the detriment, minimizing the sum of both. Optimization of a nuclear safety system could conceptually treat similarly the cost of potential damages from nuclear accidents and the cost associated with achieving a given level of safety. Within the above framework a method of optimizing the design of nuclear safety systems is presented, and a simple case of redundancy by output voting techniques is given.

1. INTRODUCTION

The usual way of achieving nuclear safety has been linked to fixed levels of ambition. The design objectives are usually derived from similar considerations to those used in conventional safety and which are expressed in what is sometimes called the "engineering state of the art". Even the introduction of probabilistic approaches to safety did not change this basic way of thinking. In fact, the level of ambition in this case is also fixed and predetermined and is expressed as a level of probability. A current nuclear safety issue is whether any one of such predetermined design objectives, either deterministic or probabilistic, is sufficiently safe [1].

The intention of this paper is to discuss a different approach for decisions regarding safety, without predetermined fixed objectives. In this approach the level of ambition results from a process of optimization based on cost-benefit considerations.

For many years radiation protection has also made use of fixed objectives (e.g. the relevant dose limits), but, in addition, has required that doses be kept 'as low as reasonably achievable' (ALARA). A procedure for implementing this requirement, based on a cost-benefit optimization, has recently been recommended by the International Commission on Radiological Protection [2]. Optimization techniques are old engineering tools and it would be appealing to use them in

International conference on current nuclear power plant safety issues. Estocolmo, 1980.
Current nuclear power plant safety issues. 1981.

nuclear safety as has been done in radiation protection [3]. Some of the problems involved in the use of optimization are briefly discussed in this paper. The material presented, however, is only an outline of ideas and concerns relating to nuclear safety design, and not a technical description of optimization methods for safety systems. Although the main concepts discussed in the paper relate to design, they could conceptually apply also to safety decisions regarding siting, operation, and eventual decommission of nuclear reactors.

2. A BASIC REFERENCE FRAMEWORK

As mentioned in the introduction, a basic framework for optimizing nuclear safety features could be obtained, at least conceptually, from the present approach in radiation protection. A basic requirement in radiation protection is to reduce all exposures to levels as low as reasonably achievable, economic and social factors being taken into account. To determine what is 'reasonably achievable' the ICRP recommends the use of an optimization process aimed at reducing radiation doses to values such that further reductions would imply a larger additional cost than the additional benefit obtained. In this approach, the cost is the cost of radiation protection, while the benefit is the reduction of the radiation detriment. It is obviously required that both cost and detriment be expressed in the same units and, therefore, some assignment of cost to the radiation detriment becomes necessary.

While the use of the optimization approach of radiation protection in nuclear safety could be of interest, the validity of such use is quite controversial. Many difficulties both conceptual and practical are involved, one of the main problems being the definition of the quantity measuring the harm expected to be avoided by the use of nuclear safety systems. The quantity used for measuring the harm avoided by radiation protection systems is the radiation detriment. It would be attractive to use this quantity also in assessments related to exposures, the occurrence of which is of stochastic nature. In fact, since the detriment is a mathematical expectation, it would be conceptually possible to define a detriment of a second order of stochasticity, which would take into account not only the probability of suffering deleterious effects from a given exposure to radiation but the probability of occurrence of the exposure as well.

The assignment of a cost to the harm that could occur if a safety system fails, is a very controversial issue. If the postulated failure is of stochastic nature and not very unlikely, the product of probability times the cost of the consequences could be used as a reasonable quantity in the optimization procedure. At very low failure probabilities, the inherent uncertainty of the product of probability and consequences makes the use of this quantity rather doubtful [4].

In the general case, the value assigned would follow a utility function of probability and consequence. The utility function should probably give more weight to larger accidents than would be implied by the direct product probability times consequence.

In the methodology presented in this report, the value of the potential radiation consequence will be presented as an undefined function of the probability of failure of the system and of the consequence. In the exemplification of that methodology, however, the simplistic assumption will be made that the value is proportional to consequence expectation, i.e. to the product of probability and consequence.

3. METHOD OF OPTIMIZING THE DESIGN OF NUCLEAR SAFETY SYSTEMS

As used in this report, optimization is a process for identifying the most favourable among several options of safety systems by minimizing the total cost associated with a safety decision. This cost comprises the actual and expected costs incurred as a result of the introduction of the safety system, X, and the value assigned to the expected consequences from the eventual failure of the system, Y. The process has to be carried out within the constraints imposed by the engineering design and respecting certain limits, both deterministic and probabilistic. The deterministic boundary conditions are given by the codes defining the engineering state of the art. A probabilistic design limit can also be applied to ensure that certain individual risks will not be exceeded in any circumstances.

The process of optimization of a nuclear safety design could be formally described by the following set of expressions [5]:

(i) an objective function
$U = X + Y = \text{minimum}$

(ii) constraining functions
$X = X(m_1, m_2, \ldots)$
$Y = Y(m_1, m_2, \ldots)$

where

X and Y have been defined in the previous paragraph
$m_1, m_2, \ldots$ are the control parameters defining the level of safety (i.e. one of them could be the number of channels of a redundant safety system).

The cost of safety, X, can be directly assessed by summing the installation and the operating costs of the system and the expected cost of reduction in availability attributable to the presence of the safety system under consideration.

Conceptually optimization can be applied to all procedures which would increase the level of safety of a given basic design, either by overdesign of the safety system components or by increasing the system redundancy directly or by output voting techniques [6]. Overdesign of a component is the increase of the value of the reliability-related parameters over these values which would be sufficient to ensure proper function, but obviously at a lower level of reliability. The use of optimization techniques (as presented in this report) to determine the optimum amount of overdesign presents some practical difficulties, mainly in the uncertainty of the cost-reliability relationship, and will not be discussed in this paper. Optimization of redundancy, on the other hand, involves simpler problems in the assessment of the relation of cost and reliability level.

As an exemplification of optimization, the following simple case of redundancy by output voting techniques is discussed. Output voting techniques make use of logic systems 'm' out of 'n' safety chains. The system would perform satisfactorily if 'm' out of the 'n' available chains respond to demand. It is well known that the advantage of these majority logics in a nuclear safety system is that they improve the reliability for safety and affect much less the reliability for availability.

For a system of 'm' out of 'n', the probability P of non-performing the safety function when required (or unreliability for safety) is:

$$P = 1 - \sum_{i=0}^{i=n-m} \binom{n}{i} p^i (1-p)^{n-i}$$

where p is the probability of non-performing the safety action for any one redundant safety branch.

On the other hand the probability, Q, of the system acting without a safety need (unreliability for availability) could be expressed as:

$$Q = \sum_{i=m}^{i=n} \binom{n}{i} q^i (1-q)^{n-i}$$

where q is the probability of occurrence of the undesired action in any one redundant safety branch.

Usually, p and q are small and n is not very high. In these cases, the high order terms in the equations for P and Q can reasonably be neglected, and the expressions can be simplified to:

$$P = \frac{n!}{(n-m+1)!\,(m-1)!}\,p^{n-m+1}$$

$$.Q = \frac{n!}{m!\,(n-m)!}\,q^{m}$$

As discussed previously, the cost of the potential radiological detriment could be expressed, for a given consequence, as

$$Y = K(P) \cdot P(n, m) = k(n, m)\,P(n, m) = k(n, m)\,\frac{n!}{(n-m+1)!\,(m-1)!}\,p^{n-m+1}$$

where K(P) is the selected utility function, which is related to P and, therefore, to n and m by a function k(n, m), and includes the cost of the consequence.

The cost incurred as a result of the decision to use a given logic (n, m), or cost of safety, X, would have two components. One is the cost of the system itself, which basically can be assumed to be proportional to n. Another relates to the potential loss in availability due to the presence of the safety system and which would be proportional to Q. The latter could be the main component in power reactors generating electricity. The cost of safety, therefore, could be expressed as an addition of a cost and an expectation of cost:

$$X = X_a Q\,(n, m) + X_s n = X_a\,\frac{n!}{m!\,(n-m)!}\,q^{m}$$

where

X_a is the cost of availability loss, namely the cost incurred as a result of an unwarranted action of the safety system

X_s is the cost of one branch of the safety system.

As discussed before, optimization implies the minimization of the sum (X + Y), using as constraining functions the relationships between X, Y, m and n, shown in the previous paragraphs. In this case m and n are the control parameters to be optimized.

If it is assumed that any additional constraints are automatically respected, the optimum solution can be found by searching all possible combinations of n and m, selecting that which minimizes (X + Y).

In spite of n and m being discrete variables, an approximate simple solution found by differentiation requires that the optimum combination n* and m* approaches the values of the equations:

$$\left(\frac{\partial Y}{\partial n}\right)_{n*} = -\left(\frac{\partial X}{\partial n}\right)_{n*}$$

$$\left(\frac{\partial Y}{\partial m}\right)_{m*} = -\left(\frac{\partial X}{\partial m}\right)_{m*}$$

On the assumption that the utility function of the radiological consequence is proportional to the consequence expectation, and therefore that the cost Y is given by Y = C.P (where C is the assigned cost to the consequence), the above equations could be solved analytically, approximating the factorials by the Stirling formula [7].

The unreliability for availability has been considered in the example to be a non-safety-related parameter. Although conceptually correct, the assumption can be challenged on practical grounds. It is obviously undesirable, from a safety viewpoint, to have unnecessary alterations in the normal operations of an installation. It seems to be very difficult, however, to attempt a quantification of the safety implications of the unavailability of an installation.

It sould not be assumed that optimization of redundancy can be validly used at all levels of reliability. Redundant systems can be affected by common-mode failures. A common-mode failure is the result of events which, because of dependencies, cause a coincidence of failure states of components in two or more separate channels of a redundant system, leading to the system failing to perform its intended function. The potential for common-mode failures can limit the possibility of increasing the reliability of redundant safety systems.

Some studies on common-mode failures in redundant systems in nuclear reactors show relatively high probability of these failures per operational year [8]. The method and example presented assume naively that common-mode failures were prevented by proper measures such as functional and equipment diversity, design and operational controls, safe failure modes and physical separation. However, in more sophisticated analysis the consideration of common-mode failures could become a relevant part of optimization of redundant safety systems [9, 10].

A word of caution is necessary regarding the terminology, to avoid confusion. Optimization, as used in this paper, has a different meaning from that usually used in reliability studies [6, 11–13]. Optimization models used in reliability studies intend to maximize the system reliability, subject to constraints involving resources, dimensions, probability of failure and cost of each component, number of components, etc. It is essential to avoid confusion between this type of optimization and an optimization resulting from cost-benefit analysis which includes the consequences of the system failure.

REFERENCES

[1] CAVE, L., HOLMES, R.E., HOLMES, P.J., "The need for a new approach to reactor safety", IAEA-CN-39/87, these Proceedings.

[2] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Recommendations of the International Commission on Radiological Protection, ICRP Publication 26, Annals of the ICRP, Vol. 1, No.3, Pergamon Press (1977).

[3] GONZALEZ, A.J., "Un criterio para la evaluación de la seguridad nuclear", Siting of Nuclear Facilities (Proc. Symp. Vienna, 1974), IAEA, Vienna (1975) 265.

[4] BENINSON, D., LINDELL, B., "Critical views on the evaluation of accident probabilities and consequences", IAEA-CN-39/4, these Proceedings.

[5] SIDALL, J.N., Analytical Decision-Making in Engineering Design, Prentice Hall, Inc., Englewood, New Jersey (1972).

[6] FRAIR, L.C., GHARE, P.M., FRAIR, K.L., Optimization of system reliability via redundancy and/or design considerations, IEEE Trans. Reliab. R-29 1 (1980) 33.

[7] GONZALEZ, A.J., Criterios de optimización para los sistemas de instrumentación y control de centrales nucleares, CNEA-NT 28/77, Comisión Nacional de Energía Atómica, Buenos Aires (1977).

[8] EDWARDS, G.T., WATSON, I.A., A Study of Common Mode Failures, SRD R 146, U.K. Atomic Energy Authority, Warrington (July, 1979).

[9] APOSTOLAKIS, G.E., The effect of a certain class of potential common mode failures on the reliability of redundant systems, Nucl. Eng. Des. 36 (1976) 123.

[10] EASTERLING, R.G., "Probabilistic analysis of common mode failures", in: Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Los Angeles, California, May 8–10, 1978.

[11] MIZUKAMI, K., Optimum redundancy for maximum system reliability by methods of convex and integer programming, Oper. Res. 16 (1968) 392.

[12] PAL, M.N., BHATTACHARJEE, M., Redundancy optimization through simplex pattern search, IEEE Trans. Reliab. R-27 2 (1978) 120.

[13] NARASIMHALU, A.D., SIVARAMAKRISHNAN, H., A rapid algorithm for reliability optimization of parallel redundant systems, IEEE Trans. Reliab. R-27 4 (1978) 261.

DISCUSSION

H. FUCHS: Should the optimization process be applied to different plants built in series or during the design of a single plant? If it were applied during the design of a single plant, this might lead to more design errors, since it is more difficult to hit a moving target.

A.J. GONZALEZ: It can be shown that independent systems (or independent installations) can be optimized by treating each one independently. In this sense there would be no difference between the alternatives you mention. However, there would be practical advantages to optimizing the design for a series of standardized installations.

G. TENAGLIA: I agree that the utility function is part of the concept of risk, and that it must be used when one is talking about risk. However, bearing in mind that a utility function relates to society as a whole, it is necessary to consider who is going to determine it – government, parliament, safety authority or somebody else – and what kind of process would be needed for this function to be established.

A.J. GONZALEZ: The utility function should be decided upon by the competent authority in the country. How it is empowered to do so is a question outside the scope of my paper. However, even a tentative decision by the competent authority, before any final agreement was reached at the political level, would ensure a coherent approach in nuclear safety design. Very simple functions, such as that of probability multiplied by consequence alone, may be sufficient to optimize several systems nationally.

A similar trend can be observed in radiation protection, where authorities in some countries have decided on a value for the cost of the man-rem, while in other countries a tentative value is used without it having been officially approved. International discussions may eventually lead to a common approach.

C. O'FARRELLY: Some months ago I saw a pre-TMI safety-optimization study regarding a district heating plant. According to the study, by placing the plant at 20–30 km from the city the costs of hot water piping would be increased. Allowing a high value for human life but a low probability of accident, after pages of mathematical equations the predictable conclusion was reached that the plant should be built in the city centre.

I have given many public talks on nuclear power, and after one has spoken of probabilities it can happen that a member of the audience asks: "What happens if the electric lines are cut?". If I answer that we have three diesel engines he will say: "What happens if the three diesels, which are not noted for reliability, fail to start?" What should one say? If one says there will be a core melt in a relatively short time you will soon see another car sticker saying "Nuclear Power? – No Thanks". If you evade the question, you lose respect and credibility. How should one deal with this dilemma?

A.J. GONZALEZ: Your dilemma does not relate to optimization techniques but to the so-called "zero-infinite" problem, i.e. the problem of how to judge events which have a very low probability of occurrence but considerable consequences if they do occur. As has been pointed out in other papers at this Conference, the product of probability and consequence may not be the relevant quantity, and another utility function will have to be chosen by the authority. Once decided upon, that utility function could be used for optimization in the way described in our paper.