Safety and Economic Classification of Systems and Components

J.W.H. Price
National Nuclear Corporation Ltd., Booths Hall, Knutsford, Cheshire WA16 8QZ, U.K.

ABSTRACT.

The paper discusses the concept of classification describing its significance and its practicability. Various ways of determining the class of a component are discussed.

1 INTRODUCTION

A common sense principle is that some components of a plant will have a greater significance than others and so should be designed, manufactured and operated with more care. With nuclear plant and with particular respect to safety this principle has been developed into a system termed safety classification of components. In general the principle could be applied to any plant.

An underlying notion behind the idea of classification is that it should be applicable systematically to all components in a plant as a managerial or regulatory requirement. Thus the class of a component should be determined by the authorities responsible for safety and economics. Once the class is agreed this gives clearly defined minimum requirements to the manufacturers and operators. Theauthorities, in this notion of classification, do not intervene futher in design nor need they be versed in the details of it. This perception of classification underlies the system used in the nuclear industry for safety classification of nuclear components.

In a classification scheme each class should corresspond to a level in a heirarchy of design, manufacturing and operating standards. Applying a class to a component is a shorthand way of specifying a large range of requirements for that component. Placing a component in a high class ensures that it will receive a larger effort in design, manufacturing and operating and thus will also cost more. The intention is that this extra cost will be repaid by a greater assurance of safety and by greater reliability of the component.

This paper examines the subject of classification from various perspectives in order to examine its practicality and usefulness.

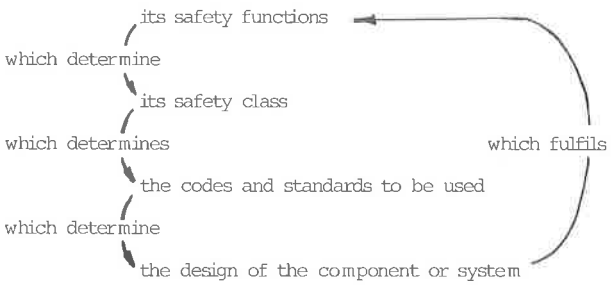
The paper is based on work done under contract by the National Nuclear Corporation, U.K. for the Commission of European Communities, Fast Reactor Coordinating Committee, Working Group on Codes and Standards. However the contents of this paper are solely the opinion of the author and do not represent the view of any organization or the CEC.

2 CLASSIFICATION SCHEMES

The implication from the Introduction is that classification can be applied to a component by considering its contribution to plant safety or economics. In this paper the rules which might govern this classification are termed ´classification schemes´. In this section the most developed classification schemes - those for nuclear safety classification - are discussed.

The context of the activity of safety classification in the nuclear plant is slightly complicated but can be described as follows. The safety functions of a plant are fulfilled by components and systems. These components and systems are each designed to a set of manufacturing codes and standards. The codes and standards to be used are determined by the safety class which has been given to the components. Thus safety classification is the process by which the significance of each component to the safety functions is identified.

The relationships between all these factors can be clarified by illustrating them as a feed back loop for a component or system:



This feed-back nature of the subject of classification sometimes confuses the understanding of it.

There are several published documents which discuss safety classifications. Each of these identifies a small number of classes:

IAEA Safety Guide 50-SG-D1 (Ref 1)	4 Nuclear Safety classes for Light Water Reactors (LWRs). The lowest is identified with conventional practices.
ANS Nuclear Safety Criteria 18.2 (Ref 2) 51.1 (Ref 3)	3 Nuclclear safety classes plus 1 Non nuclear safety (NNS) class identified with conventional practices (for PWRs)
ANS Safety Classification for LMFBRs 54.6 (Ref 4)	3 Mechanical nuclear safety classes plus 1 NNS class also 1 electrical safety class and 1 structural safety class.
KTA Classification for LWRs (Germany) 3202.1 (Ref 5)	5 Nuclear safety classes. Class 5 is identified with conventional rules. Classes 3 and 4 differ only in that there is extra independent checking in class 3.

The reasons why the number of safety classes must be limited is discussed in the IAEA Safety Guide:

> 'Fewer classes would result in over-stringent design requirements being applied in satisfying certain safety functions (those of less importance to safety within a class). More classes would result in impractically fine distinctions being drawn between the design requirements appropriate to adjacent safety classes in the heirarchial order'

An important practical point underlies why most classification schemes have tended to define three nuclear classes plus one non-nuclear class. The most important design and manufacturing codes, those of ASME, are split into three nuclear classes (in ASME III) plus a non-nuclear set of design codes (eg. ASME VIII) and are in extensive use internationally. There is no point in defining safety classes which cannot be matched to design codes .

Various rules for connecting safety functions to the safety classifications have been proposed. In this paper we will examine the three most important schemes.

2.1 ARBITRARY SCHEMES.

The Arbitrary classification scheme is well established and typified by the U.S. documents ANS-18.2 (Ref 4). In this type of scheme coponents contributing to various safety functions are assigned to a safety class by definition. The arbitrary scheme does not specify any rationale which would permit the designer to allocate components to a class independently.

This exerpt from ANS-54.6 for LMFBs (Ref 4) and ANS-54.6 (Ref). typifies the arbitrary approach:

'Safety class 1M (Mechanical) applies to ... mechanical systems [or] components [which] ...

(1) are part of the reactor coolant boundary (components within the capability of the normal make-up systems are excepted)...

(2) perform reactor trip functions...

(3) are ... inside the reactor vessel and whose failure could result in exceeding the safety design bases for either core coolability or core reactivity control (replaceable items in core are excepted as is in-vessel instrumentation)'

This set of rules raises many questions. For example is the presence of a leak jacket of any relevance to determining the class of the reactor coolant boundary? If the reactor trip can be performed by redundant or diverse systems, how is this to be taken into account? What is the significance of replacability of in-core components and does their replacibility reduce their importance to safety?

The arbitrary scheme gives no answer to these questions, and the inevitable result is that the logic behind the classifications is not clear. There is no credit for the provision of redundancy in safety systems, nor is there any guidance for components which are not specifically mentioned in the rules.

Despite these problems the arbitrary scheme is the only one in common use. Its main advantage is that it can be applied as a fixed rule and can thus form the basis of regulatory requirements.

2.2 LINES OF PROTECTION SCHEMES

The concept of 'lines of protection' is that , if possible, plant should be designed so that more than one component or system has to fail before there is a major accident, i.e. more than one line of protection must be breached before there is a release.

This idea can eventually lead to a classification scheme. Clearly if there is no line of protection against the failure of a component and the result of the failure is very serious then that component would be in the highest safety class. If however there are many lines of protection then a lower class is justifiable. In one interpretation if there are numerous lines of protection then all the components involved in that particular accident sequence can be given a lower safety class.

Another interpretation is that components further down the sequence can be given lower classes than those at the beginning of the sequence. This is illustrated in section A2.2 of the IAEA Safety Guide (Ref 1). Class 2 is suggested for components which mitigate the consequences of an accident or prevent operationaloccurrences from leading to accidental conditions. Class 3 is for componets which perform a support role.

The lines of protection scheme is not defined enough for detailed application and is open to a number of interpretations. However there is an underlying logic which is actually better understood when considered in the light of the probabalistic scheme since it is an approximate form of the probabalistic scheme.

2.3 THE PROBABALISTIC SCHEME

A probabalistic scheme for safety classification is included in the IAEA Safety Guide (Ref 1). The safety guide suggests that in order to assign a safety class to a component the product of the following three factors should be considered:

'(i) The consequences of failure of that safety function

(ii) The probability that the safety function would be required

(iii) The probability that the safety function would not be accomplished when required

The product of these three factors must be acceptably low.'

The implication of the IAEA proposal is that a quantative approach to safety classification may be used. The product of the three factors results in a value of probability times consequences which in the nuclear industry is associated with the concept of risk. The approach can thus be seen as an extension of probabalistic risk assessment (PRA). It is also attractive theoretically and can be used as a background assessment of all safety classifications.

The IAEA Safety Guide however does not develop the approach in sufficient detail for it to be applied rigorously. As part of the work for the CEC an algebraic formulation of the probabalistic scheme was devised.

3 ALGEBRAIC FORMULATION OF THE PROBABALISTIC SCHEME

Consider the classification of a system B in the middle of the event tree. In the terms of the IAEA probabalistic scheme three factors and their product must be evaluated.

(i) The consequences of failure of system B.

The consequences of each sequence of events m can be labeled Cm. However it is clear that the probability of each sequence of events must also be taken into account. If we take into account all the branches of the event tree, we must consider not only failures of B but all its response modes. Hence the fullest statement of the consequences of the response of system B is given by the formula

$$\sum_{m=1}^{M} Qkm\,Cm$$

where Qkm is the probability that a sequence of events, m will follow on the response mode k of system B
M is the number of separate sequences of events possible involving the system B

(ii) The probability that the safety function would be required.

This depends on the frequency of relevant initiating events and the probability of other systems carrying out the function before a demand is made on system B. If we take into account all initiating events which may place a demand on B for completeness, then the probability of a demand being placed on B is

$$\sum_{i=1}^{I} \sum_{j=1}^{J} FiPij$$

where Fi is the frequency of an initiating event, mode i, which can place a demand on system B
Pij is the probability of the sequence j leading from initiating event mode i to system B
J is the total number of events placing a demand on system B

I is the total number of initiating modes placing a demand on the system.

(iii) The probability that the safety function would not be accomplished.

Again for completeness all response modes of system B will be taken into account when expressing this probability as follows:

S_{jk}

where S_{jk} is the probability of response mode k of system B resulting from the preceding sequence of events j. There are K different response modes of the system.

(iv) The product of these three factors must be acceptably low.

Let us assume that a single quantity, R, has been defined, where R (the risk) is a consequence times a frequency. The product of all the preceding factors can be expressed in the following equation which uses tensor notation:

$$F_i P_{ij} S_{jk} Q_{km} C_m < R$$

If B is a component which can initiate an event sequence then a different formulation results

$$F_i Q_{im} C_m < R$$

where F_i is the frequency of failure of component B in mode i
Q_{im} is the probability that the protection systems will respond to a failure in mode i with a sequence of events m.

4 PRACTICALITIES OF PROBABALISTIC CLASSIFICATION

As can be seen above there are a large number of factors which should be considered when determining the reliability requirements, S_{jk} or F_i of the system being considered. The number of factors can be greatly reduced from this large total, which results from the rigorous formulation, by ignoring those branches of the event tree which place no real demand on the system.

There are, however, still a number of difficulties in applying the formulae as they stand. For example, it is unlikely that many of the probabilities or consequences will be well known, and the value of risk, R, will not be well defined. However, in principle these problems could be resolved by further research.

There are two basic question which are more problematic.

Firstly, how do the values of required reliability, S_{jk} or F_i, relate to safety classes? To illustrate this suppose a required reliability has been determined for a system B of 10^{-5}. The simplest approach to this is to arbitrariy define classes as for example;

Class 1 less than 10^{-6}

Class 2 10^{-4} to 10^{-6} and so on.

But this has the objection that the method is no longer totally objective but now includes a significant arbitrary element.

The second point relates to the first from another point of view. Supposing a required reliability has been determined, how do design codes relate to it? At present the design codes are not probabalistic in nature but are essentially arbitrary sets of rules which experience tells us have some connection with reliability. There is virtually no prospect that design codes will be developed which will relate directly to reliability for complex components such as pressure vessels.

There are also practical problems with applying the rigorous classification. The large number of factors involved in the formulae mean that the required reliability can be altered by changes in other parts of the plant. For example changes in design on one system would lead to changes in requirements on other components. This is a virtually intolerable situation for designers and manufactures who need a fixed set of rules at an early stage.

5 CONCLUSIONS

The probabalistic classification scheme generated a great deal of interest from the parties involved in the CEC study. The interest stemmed largely from the clarification it gives to the underlying philosophy of classification.

Despite its difficulties the probabalistic scheme of classification does assist in giving a strong theoretical background, so that there can be much more understanding of the design objectives for systems and components. The approach could also be extended to economics without great difficulty. In this case the values of consequences, Cm, would be expressed as sums of money, and the risk, R, would be money times frequency, i.e. an annual cost.

However another thing became clearer during the CEC study: philosophical classification as an approach was becoming less favoured. The tendancy is increasingly for regulatory authorities and utilies to agree, in great detail, on design and manufacturing requirements for many individual important components. This tendancy runs contrary to the concept of classification as an activity carried out in isolation by the regulatory authorities. Since it is often difficult to generalize about a wide range of components in a design code, the greater attention to individual components can be seen as a more sophisticated approach and should ensure greater safety.

It is also clear that there is still much work to be done to develop a heirarchy of properly differentiated codes which will cover the range of components being designed.

ACKNOWLEDGEMENTS

The concepts in this paper evolved over three years and in discussion with a large number of specialists in several EEC countries. I would particularly like to thank Dr.E.C.Cobb of NNC for his invaluable advice and assistance throughout the period.

REFERENCES

1 Safety functions and Component Classification for BWR, PWR, and PTR, IAEA Safety Guides, No 50-SG-D1, Vienna, 1979

2 Nuclear Safety Criteria for the design of Stationary PWRs, American Nuclear Society, La Grange Park, ANS-18.2, 1973.

3 Proposed American National Standard, Nuclear Safety Criteria for the design of stationary PWRs, ANS-51.1, 1981.

4 Proposed American National Standard, LMFBR Safety Classifcation and Related Requirements, ANS-54.6, 1979. (Trial use and comment)

5 KTA 3202.1 'Klassifizierung ... in Kernkraftwerken mit Leichwasserreaktoren ... Teil 1 Druckwasserreaktoren' (Draft). KTA-Dok-Nr-3202/81/ Regelentwurfsvorlage,1981.