PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Reliability Analysis in the Design of Safe Nuclear Power Plants [and Discussion]

G. M. Ballard, B. Littlewood, K. Sachs and J. Bibby

Phil. Trans. R. Soc. Lond. A 1989 **327**, 549-564
doi: 10.1098/rsta.1989.0010

Phil. Trans. R. Soc. Lond. A **327**, 549–564 (1989)
Printed in Great Britain

Reliability analysis in the design of safe nuclear power plants

By G. M. Ballard

Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, Wigshaw Lane, Culceth, Warrington WA3 4NE, U.K.

The requirement for all potentially hazardous plant is to achieve high reliability of engineering systems *by design*. The process of reliability analysis is a fundamental part of the design process in the nuclear power industry. Such analysis recognizes that there is always some possibility of engineering equipment failing and therefore the ability of the plant to be reasonably tolerant of such failures is investigated. In this paper the methods and philosophy underlying reliability analysis are briefly explained with examples of qualitative techniques such as failure modes and effects analysis, and fault tree analysis. In addition some of the quantitative models of equipment reliability are discussed and the need for robust statistical techniques for data analysis explained.

Introduction

The need to achieve safe operation of potentially hazardous plant or equipment is not new. After almost every accident in recent industrial history someone has suggested that we should ensure 'that this never happens again'. However, a more recent need is to be able to achieve the reliability of plant and equipment required for safety without invoking the 'trial and error' process which has been the foundation of many industrial developments, but also, unfortunately, the cause of many accidents. The engineering design of bridges is perhaps a notable example of our ability to build very technically advanced systems, but only with the benefit of experience from a significant number of catastrophic failures.

The task in the nuclear industry has therefore been to develop a new technology involving a number of pioneering engineering innovations, while at the same time ensuring that the safety of both workforce and public is protected. The development of new technology necessarily means that we must learn from experience, and some of that experience will undoubtedly include significant failures of plant and equipment. Our plant must, however, be designed to be tolerant, in a safety sense, of such failures.

The requirement has been to achieve a high reliability of engineering systems by design rather than by trial and error. The techniques of reliability analysis have played a significant role in the pursuit of that objective.

Reliability analysis

What are the fundamental elements of a reliability analysis?

(i) First and foremost it involves an engineering analysis of a system from a different perspective; not that of the designer who asks how he can make the system work, but that of a reliability analyst who asks how it might fail. Underlying this analysis is the recognition that there is always a 'chance' of failure no matter how good the engineering is.

(ii) A second element is a systematic and structured identification and analysis of the individual components of the system. Such analysis aims to recognize all the important failure modes of components and to understand the effects of such failures.

(iii) Next, the logical interconnections of the components that comprise the system need to be identified so that the system reliability may be modelled both in terms of the reliability of its components and the interactions between such components.

(iv) A further element is a quantitative analysis aimed at answering such questions as 'How reliable is it?' and 'Is it reliable enough?' The quantitative analysis relies heavily on the data from past engineering experience to provide the key to the relative and absolute importance of the potential failures identified in the qualitative analysis.

In this paper attention will primarily be focused on the quantitative aspects of reliability analysis, to reflect the objectives of this meeting. However, the qualitative recognition of the potential reliability problems of systems is of major importance and will therefore be briefly described first.

Qualitative reliability analysis

The reliability analysis of a proposed design of a nuclear power plant is carried out within the following boundaries.

(i) There is a 'chance' (later to be expressed as a probability) that engineered equipment and systems shall fail.

(ii) The plant's design needs to demonstrate a reasonable tolerance of such engineering failures.

(iii) Failures which are not tolerated by the plant's design need to be demonstrated to be sufficiently rare occurrences.

The task of the qualitative reliability analysis is to recognize the failures that may occur, to understand the plant's response to such failures and to identify those areas where the plant's design may not be adequately tolerant of such failures. To carry out this task a number of techniques are employed to produce a systematic, structured and logical analysis. Two particular techniques are failure modes and effects analysis (FMEA) and fault tree analysis (FTA). Both techniques are aimed at establishing a 'cause-and-effect' relation, although initially they are antithetical.

FMEA starts by identifying all the potential failure modes of the individual items of equipment that comprise any particular plant's system. The effect of such failure modes on the system's performance is then investigated. Such effects may include a slight degradation in designed performance, a 'fail-safe' response of the system or ultimately a complete failure of the system to respond as designed. The importance and attention paid to potential failure modes of equipment will clearly reflect the severity of the system effect produced. The important aspect of an FMEA is that it is a complete record of our understanding about the behaviour of the components of a system. There is no implicit assumption about the likelihood of failure of equipment; all failure modes that could, in principle, occur are analysed.

Fault trees were developed as a logical expression of the deductive approach in which the effect being investigated is analysed into its potential causes. Thus FTA starts from the end of the cause–effect relation opposite to that of an FMEA. The essence of FTA is to progress in small, logical steps from an effect to its immediate cause. That cause can then be treated as an effect to be similarly analysed into its causes. This iterative approach can continue until the

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

causes are individual failure modes of equipment or human operations. The particular advantage of an FTA is its capability to explicitly recognize logical connections between components within a system; a task which an FMEA finds more difficult.

Consider an example which illustrates the two techniques. The standby electrical power system in a power station may schematically look like figure 1. The system is designed to detect loss of power from the main grid and to automatically start standby diesel generators (DGs) to provide electric power to essential loads. Various circuit breakers are provided to isolate bus-bar faults and to provide proper loading of the standby generators. The system has considerable redundancy to provide fault tolerance and system success is achieved if any one of the four essential loads is energized.

Each failure mode of every component is listed in an FMEA table, part of which may look like table 1. Such a listing can identify issues which may appear 'fail-safe' such as the spurious

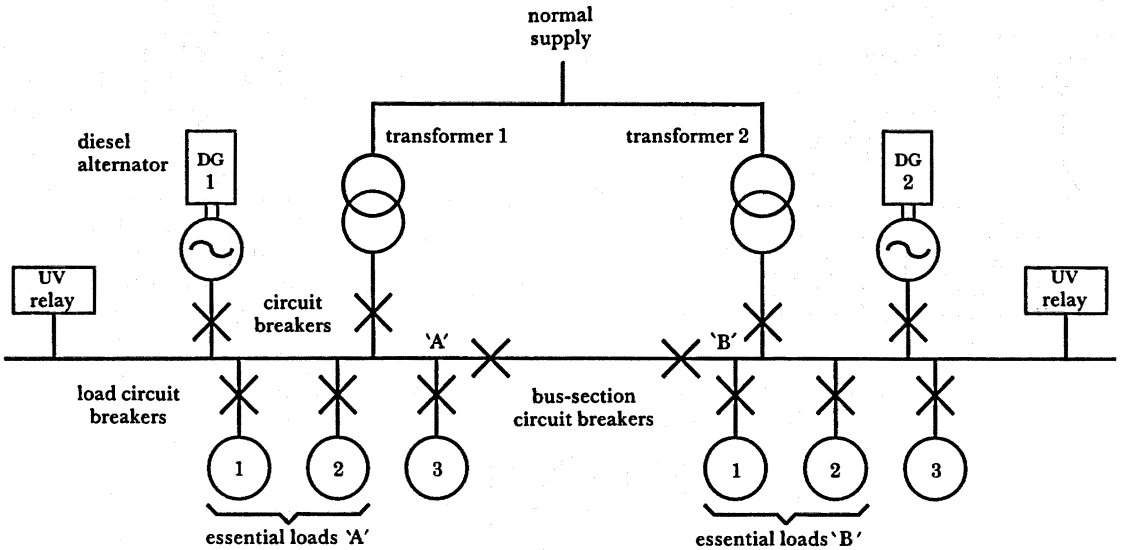

FIGURE 1. Schematic arrangement for the standby supply system. (UV is undervoltage.)

TABLE 1.

(LCB is load circuit breaker.)

component	failure mode	failure effect	related components and comments
LCB 003	failure to open on loss of grid	electrical load remains on bus A and will cause DG A to trip when bus A is energized	LCB 001/002/003/004/005/006 potential common mode failure
	failure to close	not required for non-essential load	
UV A relay	output fixed due to internal failure low	spurious isolation of grid and demand on DGs	increases frequency of demand on safety system; two out three voting may be preferable
	high	will not trip on loss of grid; system will still operate if UV B trips	possible unrevealed fault; regular test required

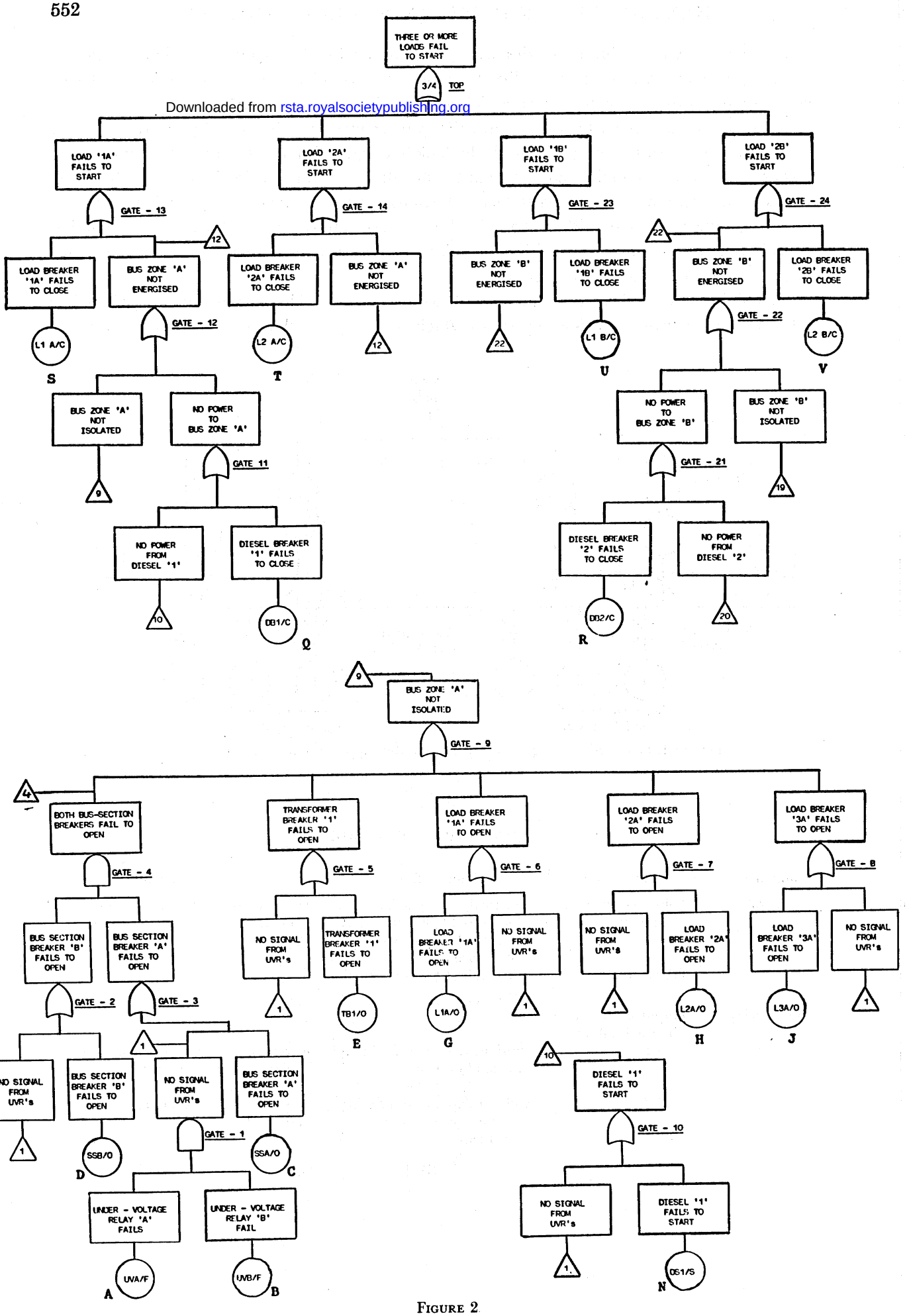

FIGURE 2

tripping of an undervoltage (UV) relay. However, it is noted that such a spurious trip increases the frequency of safety-system demands and may therefore be an undesirable feature. A two out of three voting system of UV relays could help to reduce this problem without materially increasing the 'fail-danger' probability.

A fault tree for this system may be similar to figure 2 in which part of a full tree is represented. The 'top event' is identified as a system failure because more than three out of four of the essential loads fail to start after a loss of main grid. In small logical steps the tree is then developed downwards. It can be seen, for example, that the failure to open of LCB 003 (LCB is load circuit breaker) is again recognized as a potential contributor to the system's degradation.

The result of such analysis is a clear understanding of the potential reliability of the system in terms of both its weak points (problems caused by single-component failures) and its fault tolerance (redundant or standby capacity). Frequently such qualitative analysis alone is sufficient to indicate the need or desirability of modifications to the design; the process is straightforward and inexpensive because at this stage the design exists only on paper and we have not had to construct a full system to learn of its potential shortcomings. However, as the design progresses questions such as 'Is it now reliable enough?' will be raised and these can only sensibly be answered by having some quantitative measure of reliability.

Quantitative reliability analysis

The task of quantitative reliability analysis is to model the reliability of components in a way which allows adequate prediction of future performance and subsequent measurement. The starting point has to be a definition of what we mean by reliability.

> Reliability is defined as that characteristic of a component or system expressed as the probability that it will perform its required function in the desired manner under all relevant conditions and on the occasions when it is required so to perform.

In this definition, the probability of an event is a direct consequence of the failures of our system being uncertain and that the best we can do is to discuss their probability of occurrence. The designer does not intend his system to fail; the recognition of a 'chance' of failure is an acceptance that our design, manufacturing and operating processes cannot be perfect.

The definition also tells us how to measure reliability; ideally the frequency, in a large number of repeated trials, of correct operation. Unfortunately, we very rarely have such detailed information (electronic product-testing by manufacturers is the nearest to this ideal) and thus we have to use a combination of models and available data, supported by a number of assumptions.

The first assumption is to limit analysis to a two-state model of component performance; components are either working or failed. In practice we know that some components can be in a continuous spectrum of degraded performance, but such problems can be overcome by defining a boundary between acceptable (working) and unacceptable (failed) performance. Within this two-state model there are three categories of component for which there are important differences in reliability behaviour.

Component reliability models

A component normally begins its operational life in a working state and then, at some time later, is likely to transfer to a failed state. After some type of repair procedure the working state

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

will be restored and the component then continues to alternate between the working and failed states throughout its effective life. The features that distinguish categories in this general behaviour are the ability to repair a component and the extent to which failure modes of components are revealed when they occur.

Thus the first category is the non-repairable component whose history is represented by figure 3.

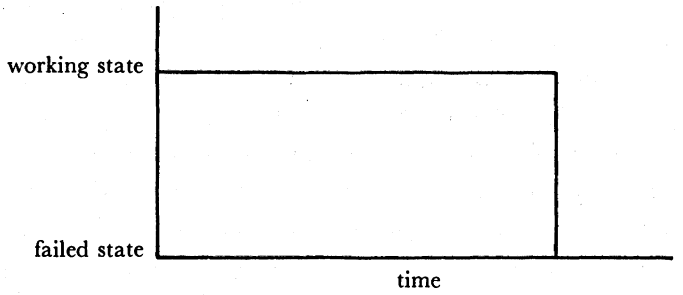

FIGURE 3.

The reason for the component being non-repairable may be a question of economics or perhaps of access; e.g. a space satellite or some components inside a nuclear reactor. For this type of component the reliability parameter of interest is the time before its first failure.

The second category of components are those which can be repaired only when failure has been detected. The failure mode may not be revealed even after it has occurred either because the component is in standby and has not been required to operate or because the component is operating but the particular failure mode is only revealed by a change in the demand on the component. Safety systems frequently have components in this category because of their role as passive systems waiting to operate when required. The reliability of this category of components shall not only depend on the frequency with which is fails, but when and how the failure is subsequently detected. Regular testing is the normal strategy employed in this case and the time history looks like figure 4, where τ is the test interval.

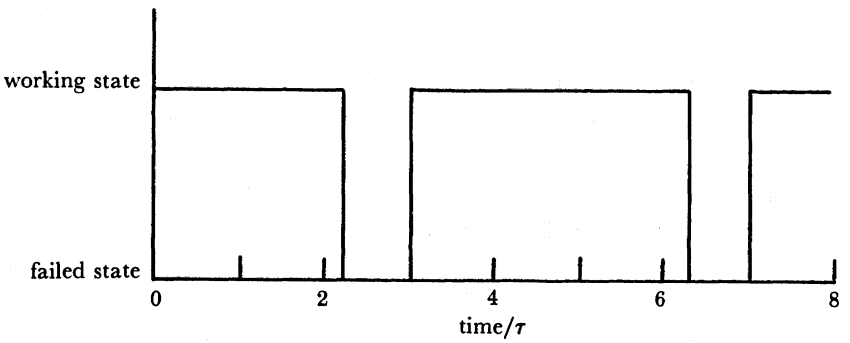

FIGURE 4.

The final category of components comprises the majority of engineering equipment which is both repairable and has failures which are either readily revealed during operation, revealed by fail-safe response when in standby or revealed by continuously monitoring for operability.

These components have a time history as in figure 5. The main parameters determining the reliability here are thus the frequency of failure and the time taken to restore or repair the component.

A simple model for the reliability R of the general component is therefore going to be

$$R = f(x_1, x_2, x_3, x_4),$$

where x_1 is the distribution of time-to-failure for revealed faults; x_2 is the distribution of time-to-failure for unrevealed faults; x_3 is the distribution of time-to-repair for a fault; x_4 is the length of time between planned tests.

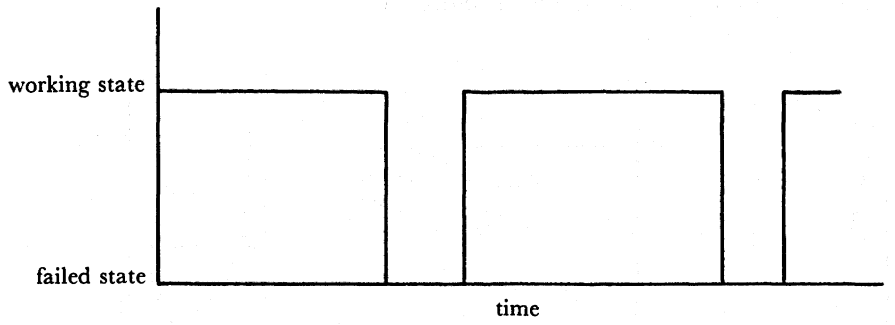

FIGURE 5.

It can be shown, under certain conditions for a component with revealed, repairable failures, that the reliability, expressed as the probability of the component being in a working state at any time, is

$$R = T_f/(T_f + T_r)$$

where T_f is the mean time to fault occurrence and T_r is the mean time to fault repair.

Such an equation illustrates the prime role of two particular parameters, the mean time-to-failure and the mean time-to-repair. One of the simplest models of component reliability which can be constructed using these two parameters uses the assumption that the failure times and repair times are exponentially distributed; for example

$$f(t) = (1/T_f) \exp(-t/T_f),$$

where t is the time to failure, T_f the mean time-to-failure and $f(t)$ the probability density function for t. For an exponential distribution with a time-independent time constant T_f, the probability of component failure between t and $t+\Delta t$, given that the component has not failed between 0 and t, is $\Delta t/T_f$.

For convenience the expression $1/T_f$ is usually referred to as the failure rate of the component λ, and similarly $1/T_r$ is referred to as the repair rate μ. With this model, the following expressions for the various categories previously described are straightforward.

Non-repairable component: the mean time-to-failure (expected life) is $1/\lambda = T_f$.

Repairable, unrevealed failures: the mean probability of being in a failed state is $\frac{1}{2}\lambda\tau$.

Repairable, revealed failures: the mean probability of being in a failed state is $\lambda/(\lambda+\mu)$.

In principle many more complex models of a component's reliability are possible by using a range of alternative distributions for the time-to-failure and the time-to-repair. A convenient way of categorizing such models is by using a feature of the distribution known as the hazard

function. This is defined for any density function $f(t)$ and corresponding cumulative function $p(t)$ as

$$z(t)\,\Delta t = \frac{f(t)}{1-p(t)}\Delta t.$$

In reliability terms $z(t)$ is the conditional probability density of component failure at time t given successful operation until time t. It can be seen that for the exponential distribution the hazard function $z(t)$ is equal to λ, the component failure rate. A class of distributions which allow wide ranging variants of $z(t)$ are the Weibull distributions,

$$f(t) = \beta t^{\beta-1}\lambda^{\beta}\exp\left[-(\lambda t)^{\beta}\right].$$

The variations of $z(t)$, $f(t)$ and $p(t)$ are shown in figure 6.

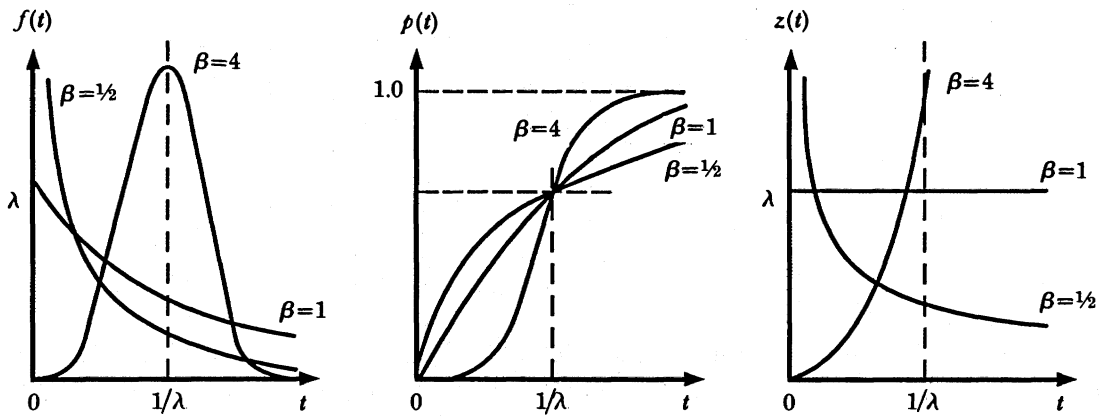

FIGURE 6. Density function, $f(t)$, cumulative distribution function, $p(t)$ and hazard function, $z(t)$, of the Wiebull distribution for different values of β.

Component failure rates

The choice of any particular reliability model clearly depends on several factors including the engineering evidence, the availability of data and the prospective use of the model. Let us consider these factors in turn.

If we are to use any model in our evaluation of the safety of the design, then that model must at least have some features which represent our engineering experience of components' reliability. There is no value in using, say, an exponential model if we cannot understand why the failure rate should be reasonably constant in time. The objective is not mathematical modelling for its own sake, but the use of models to represent our understanding of engineering in a way which allows us to quantify reliability and make sensible predictions for the future. Take for example a rather complex component, the human being. The hazard function as a function of age will typically be similar to figure 7.

The most noticeable characteristics of this plot are that the hazard function decreases sharply during early life, remains approximately constant during the major part of life and then progressively increases towards the end of life. Such features accord with our intuitive experience that babies are at relatively high risk, but that risk decreases as they grow older. During the majority of life we are prone to many risks, but these are not particularly sensitive to age and they affect people in a fairly random manner. However, towards the end of life once

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

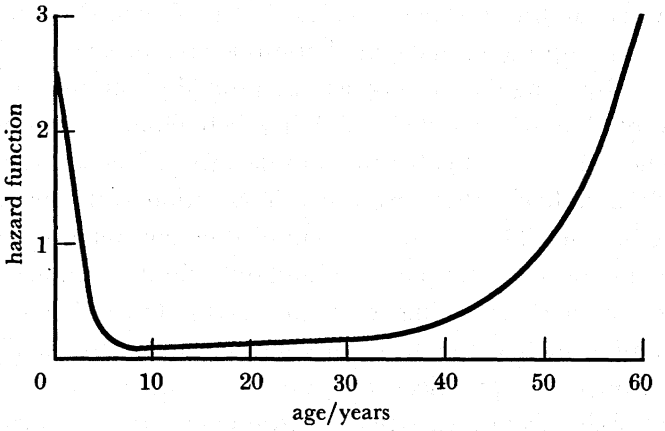

FIGURE 7. Death-rate characteristic for males living in England and Wales for the years 1960 to 1962.

again our risk rises as we become more frail and vulnerable. A reliability model that represented human beings by a constant failure in the middle years of life may therefore reasonably be judged to be in accord with experience.

Experience with engineering components and systems suggest that a similar dependence of failure rate on time exists; see figure 8. The first phase represents a pattern of failure events which typically arise from initial production, test or assembly faults. This is sometimes called the 'burn-in' or 'infant-mortality' phase and reflects the early 'teething' troubles which often arise in practice with engineering devices. The last phase illustrates the effects of ageing when the component is beginning to wear out and the failure rate increases. In between these phases is one which may be termed the 'useful life' of the component where the failure rate is sensibly constant or follows a slowly changing trend. It might be judged necessary to model all these phases by using, for example, the Weibull distributions. However, many systems are designed so that they operate essentially in the useful-life phase. This may be achieved by soak testing or commissioning procedures to weed out components with high initial failure rates, and by replacement or refurbishment of components before they enter the wear-out phase. With these operating practices a constant failure rate may frequently be an adequate representation of the components' average behaviour.

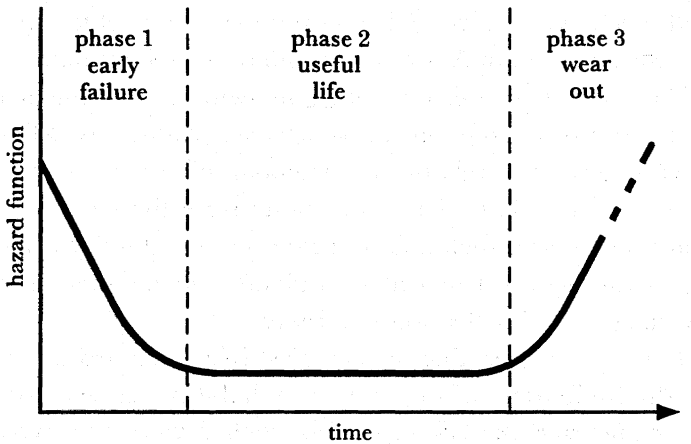

FIGURE 8. Typical failure-rate characteristic for engineering devices.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

At this point it is worth noting the reference to the components' average behaviour. The reliability evaluation is attempting to make predictions for the future operation of engineering components and systems by using data from past operational experience of similar equipment. However, it is apparent that the detailed reliability behaviour of any specific engineering installation will depend on the particular magnitude of some contributing factors for that specific installation. It is unlikely that any other installation will mirror exactly the same specific combination of factors. The reliability analysis therefore relies upon identifying major engineering characteristics of systems, such as redundancy, fault tolerance, fail-safe behaviour, condition monitoring, etc., and modelling these specifically. Other less specific factors which can be difficult to quantify, such as the degree of quality control, the quality of maintenance, the adherence to good operating practices, etc., are represented in a component's 'average' failure rate which is compiled from a variety of operating experience encompassing variations in these factors. This average failure rate may not be representative of any particular installation, but will be representative of a typical achievement using good engineering practice. It is therefore appropriate for use in assessing future designs where the exact details and effects of some factors may not be known until the plant has been operating for some years. The use of such failure rates also emphasizes that complex reliability models using detailed distributions are rarely justifiable. An exponential distribution of time-to-failure and time-to-repair and a constant failure rate are usually most appropriate unless the availability of detailed and specifically applicable data suggests otherwise.

However, there are situations where a more detailed representation of component's and system's failure behaviour is appropriate. The first concerns plant which has been operating for some years and has therefore accumulated significant data concerning the operation of its components. Such data can be analysed to identify the nature of past reliability problems and then appropriate models used to indicate the likely future performance of the plant. In this paper, however, our interest is not in the analysis of currently operating plant, but in the design of new plants. For these plants a useful aim would be to identify aspects of the design and operation of components which have a systematic and consistent influence on reliability. The data from a range of operating plants offers the possibility of analysis which yields conclusions which are not just specific to one installation, but have a more generic relevance and therefore could be applied with confidence to the modelling of new designs. Such analysis is best illustrated by examples; consider the reliability of two very different components, microelectronic devices and mechanical valves. Given a number of sets of failure data on a general type of component operating at a number of plants, all of the failure data can be combined to calculate an average failure rate for this type of component, despite the fact that the data on failure rates for specific groups of components on specific plants may differ considerably. In practice one is assuming that the reliability behaviour of these groups of components is equivalent or that it is not possible to determine or measure the factors which influence the reliability. As previously discussed, such a failure rate is a useful guide for new plant designs, but there are clearly advantages in being able to identify engineering aspects of design and operation which have a systematic effect on reliability.

Where data from testing and operating are plentiful fairly detailed analysis is possible and reasonably detailed discrimination of component reliability factors possible. This is the situation in microelectronics and the failure rate for such devices may typically be described by equations such as

$$\lambda = \pi_{\mathrm{Q}} \pi_{\mathrm{L}} [c_1 \pi_{\mathrm{T}} \pi_{\mathrm{V}} + (c_2 + c_3) \pi_{\mathrm{E}}]/10^6 \text{ h},$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

where π_Q reflects quality control; π_L is a learning factor for new unproven devices; π_E takes account of environment; π_V is a voltage derating factor; π_T is related to maximum junction temperatures; and c_1, c_2 and c_3 are complexity factors.

All of the factors in this equation are derived from failure data and a typical example is shown in figure 9, where the temperature factor is plotted for some typical device types. Although it must be stressed that such equations only indicate the reliability performance achievable given good engineering practices, the guidance of such a relation can be of considerable assistance in ensuring that a system will have the reliability required from it.

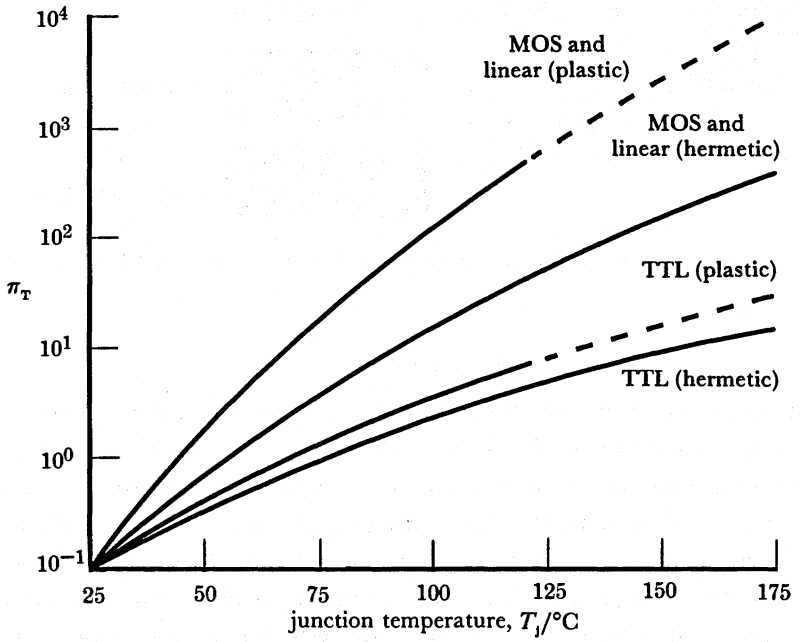

FIGURE 9. π_T against temperature for microelectronic devices. $T_j \approx$ ambient temperature/25 °C (hermetic) and $T_j \approx$ ambient temperature/60 °C (plastic).

Unfortunately, the wealth of data available for microelectronic devices is not so easily available for other devices, particularly in the mechanical field. Nonetheless, useful information can be obtained by analysis of that data which does exist, particularly if such analysis is guided by engineering knowledge and experience. Instead of the primarily data-driven approach adopted for electronic components, the method relies on engineering hypotheses which are then tested against available data. For example, consider the reliability of mechanical valves and look at, say, the failure of such a valve due to leakage. Our engineering knowledge about such failures can be used to identify those parameters that may contribute to such a failure mode. Figure 10 illustrates the type of deductive process involved.

The significance of these parameters can now be examined by testing against the available data-sets. A typical method might use the proportional hazard model (PHM). This model assumes that the effect of the various parameters on the component hazard function will take the form

$$z(t) = z_0(t) \exp(\beta_1 y_1 + \beta_2 y_2 + \ldots + \beta_n y_n),$$

where $y_1, \ldots, y_n$ are the independent variables, $\beta_1, \ldots, \beta_n$ are weighing factors and $z_0(t)$ is the baseline hazard function. Such a model is relatively simple, but probably reflects the quality of data currently available and a proper concern to use only robust conclusions from such analysis.

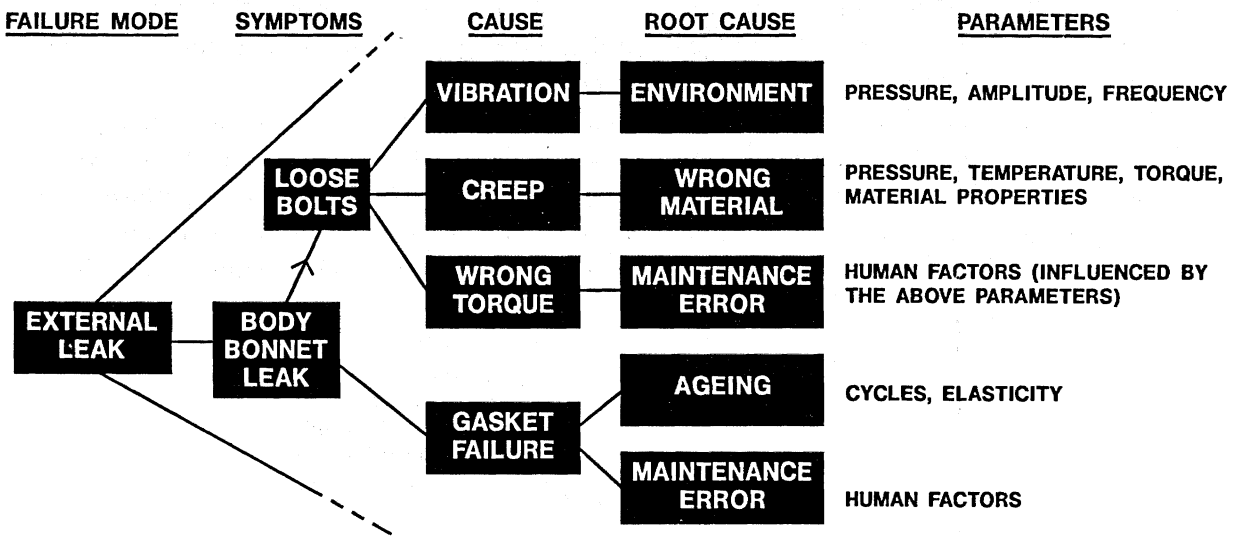

FIGURE 10. An extract from a schematic failure diagram for a gate valve.

Uncertainties

It will be clear from the previous discussion that the quantitative aspects of reliability analysis involve some uncertainty. Such uncertainty is either inherent because of the probabilistic nature of the modelling or because of assumptions in the analysis of components' performance or data. To deal with the latter uncertainty a reliability analysis involves an assessment of sensitivity. All assumptions and data which have the capacity to significantly influence the conclusions of the analysis are varied within possible limits. In many cases such variations will not materially alter the reliability analysis and therefore no further action is required. However, if critical issues are identified which have a major effect on the analysis when varied within possible limits, then action is required to reduce the sensitivity. This may either entail more detailed study to refine the analysis and reduce the possible variational limits or, if the information or data are not available to do this, design modifications to reduce the system's sensitivity to the particular issue.

In practice, despite the 'average' character of much of the data used, the reliability analyses performed in the past have proved satisfactorily accurate. Figure 11 shows the results of prediction against actual operation for some systems analysed by the Safety and Reliability Directorate over the last 20 years.

To some extent the accuracy is because in any system comprising a number of components there will be compensating deviations. Undoubtedly, the detailed accuracy of reliability analysis will be aided by the increasing ability to investigate substantial collections of failure data and thus be more specific in the application of failure rates to particular components. There is, however, a need for robust statistical modelling techniques to support such developments.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

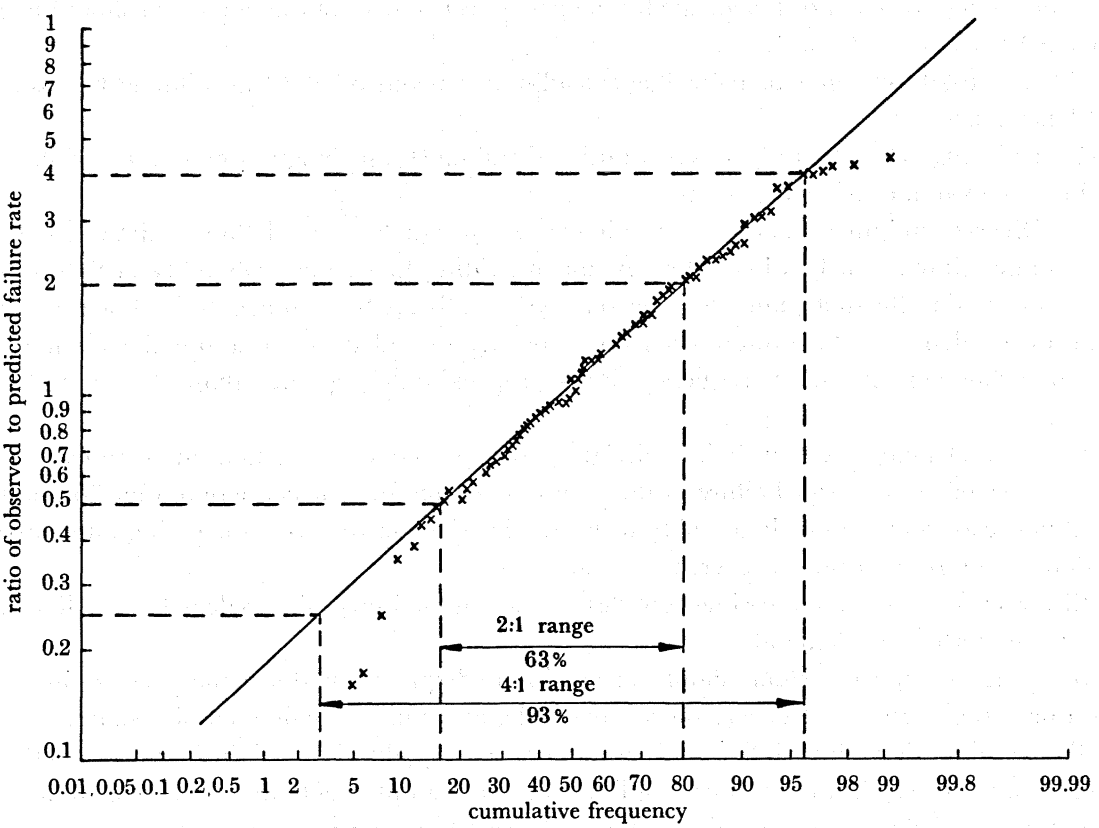

FIGURE 11. Frequency distribution of the failure rate ratio.

RELIABILITY GUIDELINES

The previous discussion has shown that it is possible to give careful and detailed consideration to the reliability and safety of a plant while it is still at the design stage. Such analysis is systematic and structured and, by using data from past experience, should provide good guidance on the actual performance of a future plant. To assist the use of reliability analysis in design evaluation the nuclear industry has compiled a number of guidelines and criteria which aid the interpretation of such analysis. Thus, for example, the Nuclear Installations Inspectorate publish *Safety assessment principles for nuclear power reactors* and the Central Electricity Generating Board (CEGB) have compiled both *Design safety criteria* for CEGB nuclear power stations and *Design safety guidelines* which amplify such criteria for individual types of nuclear power plant. The aim of such criteria was to 'encourage a design process which demanded disciplined and systematic thinking and a comprehensive and rigorous approach'. Experience had given the CEGB the appreciation that reliability analysis was a valuable aid to judgement when reviewing the adequacy of plant safety and they therefore decided that such methods should be built into the design process.

The CEGB's criteria and guidelines are a combination of qualitative and quantitative targets. For example, two quantitative targets are the following.

(i) For any single accident which could give rise to a large uncontrolled release of radioactivity to the environment resulting from some or all of the protective systems and

barriers being breached or failed, the frequency of occurrence (of the sequence) should be less than 10^{-7} per reactor year.

(ii) The total frequency of all accidents leading to uncontrolled releases should be less than 10^{-6} per reactor year.

In achieving these overall targets additional guidance on design is given. The following points are examples of such guidance.

(i) Diverse equipment shall be provided unless it can be argued that common mode or systematic failures can be discounted. As an overriding limit, the probability of failure of a common mode affecting plant items of one type shall not be assumed to be less than 10^{-5} failures per demand. As a result diverse systems are provided for those functions which are essential following the most frequency faults (approximately greater than 10^{-2} to 10^{-3} per year).

(ii) The safeguards system shall be designed so that no operator actions are claimed within 30 minutes of reactor trip. Failure of the operator to take the correct action after 30 minutes shall not lead to any immediate safety hazard. The effect of the operator taking an incorrect action at any time must, however, be assessed.

(iii) Following any fault arising from design, the unreliability of the safeguards shall always be less than 10^{-3} per demand.

(iv) The safeguards systems should at all times adequately perform their whole function, with or without off-site electrical power available, assuming a single credible failure.

This combination of reliability analysis coupled with qualitative and quantitative reliability targets has had significant practical application. For example, such attention to reliability led to a number of changes to the Westinghouse design of pressurized water reactor power plant before it was acceptable as a design for Sizewell B (see table 2).

TABLE 2. SOME OF THE SIGNIFICANT CHANGES TO THE WESTINGHOUSE DESIGN WHICH ARE RELATED TO RELIABILITY CONSIDERATIONS

(HHSI is high-head safety injection, ESWS is essential service water system.)

system	Westinghouse	Sizewell B
emergency core cooling system	two HHSI pumps	four HHSI pumps of increased capacity
	four 33% accumulators	four 50% accumulators
chemical and volume control system	two centrifugal pumps and one positive displacement pump	two centrifugal pumps plus emergency charging system comprising two steam turbine driven positive displacement pumps
electrical system	two 100% diesel generators feeding two separate distribution boards	four 100% diesel generators feeding four separate distribution boards (note: non-electric drives for auxiliary feedwater and charging pumps)
boration system	rapid boration system (within HHSI system) included	rapid boration system deleted, emergency boration system added
heat rejection systems	two pump ESWS and water-cooled ultimate heat sink	four pump ESWS and air-cooled reserve ultimate heat sinks

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Conclusions

The nuclear industry is very conscious of the need to develop the technology in a safe way and yet still be able to learn from practical experience. Since practical experience sometimes indicates unsatisfactory design features it is important that nuclear power plants are designed to be tolerant of operational problems. Reliability analysis provides a valuable method of guiding plant design so that potential weak points in design are identified and corrected. In addition the expected safety performance of the design can be assessed against safety guidelines and criteria to help to ensure that the plant will indeed be appropriately safe during its operation.

A significant factor in quantitative reliability analysis is the use of reliability data collected from past operating experience. It is important that such data be analysed so that it may provide the best guidance to the assessment of future plant. Robust statistical methods for such data analysis are being used, but further developments in this area may prove helpful.

Discussion

B. Littlewood (*Centre for Software Reliability, The City University, London, U.K.*). Dr Ballard was confident that he could satisfy a requirement that uncontrolled releases of radioactivity occur at a rate of no more than 10^{-7} per reactor year. This seems an extraordinarily stringent requirement even for system failures resulting from failures of components in a fault-tolerant hardware architecture. It would appear that he must assume independence between different failure processes to achieve such a figure. Is there any evidence to support such an assumption?

Perhaps more significantly, such an analysis seems to ignore the possibility of failures arising from inherent design faults. Recent events (crashes of DC10 aircraft and the space shuttle, the Three Mile Island incident) suggest that it would be wrong to assume that complex systems do not contain such design faults. In which case we need to be concerned about the rate at which these will show themselves, since such manifestations are a possible cause of catastrophic system failure. To achieve his 10^{-7} figure for the total system, the contribution from these failures caused by design faults must be even smaller.

As design failures of hardware are very similar to the software failures discussed in my own paper, I should be interested to know how the rate of occurrence of such failures can be shown to be less than one per hundred million reactor years.

G. M. Ballard. In assessing the potential frequency of large releases of radioactivity from nuclear power plants it is recognized that there will be interdependence between hardware failures, so-called common-cause failures. A major design feature to minimize the effect of such dependence is the use of diverse safety systems; that is safety systems which achieve the objective of shutting down and cooling the reactor, but do so by entirely different engineering means. Analysis of past operational experience in all types of hazardous industry indicates that diversity is an effective protection against failure dependence.

Diversity is also an effective defence against design error because the design process involved in the diverse systems is usually fundamentally different. Additionally, other design features such as 'fail-safe' operation, the use of proven technology and the careful monitoring of systems during operation help to reduce unexpected hazardous behaviour. Finally, a major difference

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

between software and hardware is in complexity and the predictability of failure modes. Hardware generally is kept simple so that its performance is predictable and any failures are also predictable. By contrast software is generally more complex and the failure modes of software much more varied and unpredictable.

K. Sachs (*GKN Technology Ltd, Wolverhampton, U.K.*). Dr Ballard has made the point that all faults are due to human error and fail-safe designs need to safeguard against its foreseeable consequences.

We have had recent examples in public life of human error leading to tragic consequences. Air traffic control, the social services, cross-channel ferries, underground transport and, of course, the nuclear industry have all provided such examples.

There is strong anecdotal evidence that in many cases the probability of human error has been accentuated by overloading of the human operators, often as a result of cost cutting. Each of us has an empirical perception that excessive pressure on people increases the incidence of human error, while the complete absence of pressure leads to familiarity and negligence.

Are there any quantitative studies of this important topic?

G. M. Ballard. The basic design principles of nuclear power plant are that safety should be ensured by three factors.

(i) Inherently safe operating features.

(ii) Engineered safety systems.

(iii) Operating procedures.

This is a priority order so that by and large safety should not depend on human actions. Thus, for example, our civil stations require that no operator action should be needed for safety reasons within 30 minutes of an incident occurring. We therefore expect that safe plant design will be a major feature in reducing the significance of human error. However, we do also analyse the possibility of human error using such methods as task analysis. These assessments highlight those factors which are likely to have the most influence on the reliability of human actions and if they are judged significant, design action can be initiated. Finally, the likelihood of human error is quantified in a number of probabilistic safety assessments (see, for example, WASH-1400), but the accuracy of the data used is still in some doubt.

J. Bibby (*Edinburgh, U.K.*). To what extent do the calculations which Dr Ballard presented take account of 'external' or human factors such as cyclones, earthquakes, sabotage or external attack? To take the last example, the probability of this country being at war in any given year may be of the order of 10^{-2}. If we are at war, the probability of a power station being attacked might have the same order of magnitude. Thus we could have probabilities of destruction of nuclear power plants considerably greater than the 10^{-6} and 10^{-7} quoted by Dr Ballard. I should welcome his comments on this.

G. M. Ballard. External natural hazards to nuclear plant, such as earthquakes, fire, floods, storms, etc., are part of the normal design requirements and are also included in the probabilistic reliability analysis. With regard to the threat from war, this is not included within the safety analysis (although the effects of such peacetime events as aircraft crashes, which are already included, may often be equivalent to such threats). However, in the event of war I suggest that the hazard from a nuclear power station would be insignificant compared to that from nuclear bombs.

Reference

WASH-1400 1975 *Reactor safety studies*. Washington, D.C.: U.S. Nuclear Regulatory Commission.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES