QUANTITATIVE ASSESSMENTS OF SYSTEM RELIABILITY

By A. E. GREEN†

SYNOPSIS

In the design and operation of plant in various fields of application there is an increasing need to assess, with the minimum of subjectiveness, the reliability of systems. This need arises in various ways such as safeguarding capital investment in a plant or reducing risk to human life.

Some aspects of the prediction of the reliability of protective systems are discussed using quantified reliability techniques.

Introduction

In the design and operation of plant in various fields of application, there is an increasing need to assess, with the minimum of subjectiveness, the reliability of systems. This need arises in various ways such as safeguarding capital investment in a plant, or reducing the consequences of hazards which may lead to loss of protection or risk to human life. Conventionally, according to the particular type of system, a study will be made of its ability to function. However, in practice, variability over the range of performance and the possibilities of complete failure must be considered. Basically, this problem is not one which is limited to the failure of hardware but is a generic problem which will be found in many technological fields, *e.g.*, it is said[1] " *What is now sought from forecasting and planning is to reduce the force and penalties of surprise through perceptive study and analysis of the condition of the environment.* "

Obviously " technological forecasting " also exists in the design and operation of plant. Hence, in considering single stream or multi-stream chemical plants there is a need for assisting management in deciding which line of action to take in the design of such plant and often problems arise because of variability and failure. Means have to be found by which we can organise and apply the experience of the past to predict where we are likely to be in the future. Words such as " it is highly reliable ", " made from good quality materials ", do not appreciably help in this problem and it is necessary to co-ordinate our intuitive ideas and our hard-earned experience into a unity which can be applied within a world of change.

This leads us to face evaluations which have uncertainty attached to them and to lead ourselves into accepting the probabilistic nature of situations which we face. Having satisfied ourselves individually in our assessments of a situation, we then have to communicate the information in some way to all the people involved within the structure of the project so that they will understand our findings with the minimum of subjectiveness. This leads to the requirements for quantifying, as far as possible, the findings and to a probabilistic definition of reliability of the type:

" *reliability is defined as the probability of a device performing in the required manner for a specified period of time or at a specified time under all the relevant conditions.* "

Having made this approach, the way is now open to trying to make things better and better, as could apply in the field of safety, or to creating the requirement to be met which is defined unambiguously. Hence, having made an assessment of the situation, a designer may require to know where to stop and see where is the best place to put the money for the maximum return and then to be able to justify the adequacy of his decision. It is not the intention of this paper to define requirements but to outline the approach and in particular, to discuss quantitative assessments of system reliability. This involves studying the patterns of variations and of failures in systems and estimating the chance of their occurrence. The techniques involved are described in detail in Ref. 14.

Variability and Failures

In the field of safety, people working in various applications such as aircraft, nuclear reactors, *etc.*, have found it necessary to quantify a requirement in some manner. Examples may be seen where the Air Registration Board have quantified the requirement for automatic landing systems[2] by saying that the probability of a fatal landing should not be worse than 10^{-7}, or in the nuclear field where a proposed requirement has been expressed in a slightly more complex way[3, 16] as shown in Fig. 1. Broadly, along one axis there is an increasing consequence and the other axis is related to the probability of occurrence. The consequence is measured by the release of a radioactive fission product expressed in curies of ^{131}I, and the other axis is measured in reactor years or the events occurring in a complete reactor programme; the starting point here being a programme of 30 reactors operating for 30 years which represents 900 reactor years. It is intended that the criterion so stated may permit the reactor designer and user a freedom of choice, provided all consequences and their occurrence produce points which lie below the criterion line. This is considered in more detail in Ref. 4.

Abnormal conditions can arise on plant which necessitate the provision of highly reliable means of protection. Typical examples are the shutdown and venting of chemical plant and similarly nuclear reactors, where the loss of electrical supplies may lead to the need for a protective system to operate. If the protective system fails to operate, there may be a hazard in the safety sense. On the other hand, if it operates when there is no demand for it to do so, it may cause a shutdown of the plant and represent a hazard in the availability sense. Hence, reliability is at a premium and obviously it is prudent to carry out a reliability evaluation in the early stages of the design.[7]

† General Manager, Systems Reliability Service, U.K.A.E.A., Risley, Warrington, Lancs.

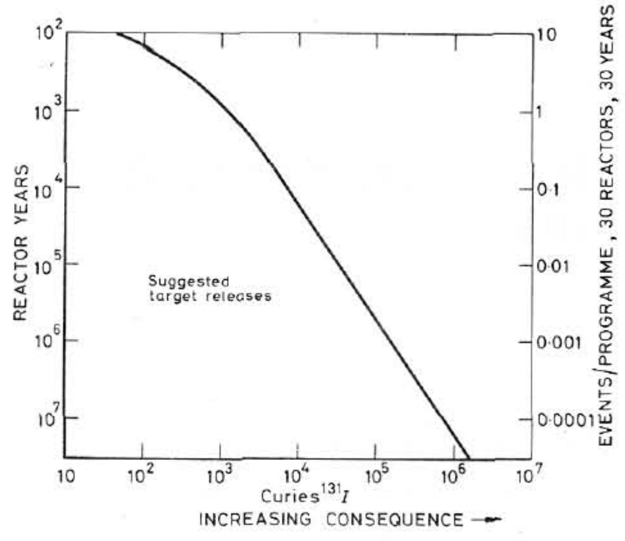

Fig. 1.—*A proposed criterion for nuclear reactors*

In assessing the reliability of a system it is necessary to demonstrate that it has the capability of functioning at least once under one set of conditions, both in space and time, but the question arises will it function under another set of conditions in space and time. Broadly speaking, an attempt is made to make a probabilistic statement on the variability and complete failure of the equipment in the following general form:[5,14]

$$\text{Probability of failing to meet requirement} = (1-p)\int_R^{\infty} f(x)\,dx + p \quad . \quad . \quad (1)$$

where: $f(x)$ = the density function for the variability of performance of the equipment in time.

R = the required performance level which should should not be exceeded.

p = the probability of complete failure of the equipment.

The variability of failure of performance manifests itself in various ways such as the change in performance of equipment which still may cause it to operate but not as intended; for example, the time of operation may be increased; or complete catastrophic failures which permit no operation at all. These changes in the performance of equipment may be revealed inherently by the design of the equipment or by special monitoring facilities. In other cases they may remain completely unrevealed and it is only by special testing procedures that such faults may be found, or they are found by calling upon the equipment or system to operate.

Summarising these ideas in diagrammatic form, as shown in Fig. 2, we have some design estimate of performance about which there is variability which extends through the whole spectrum of performance. The variations in performance illustrate typically that performance values are more likely to occur near to the design estimate or in the catastrophic failure region. Superimposed upon this pattern of variation we have a requirement shown as R but itself may also be distributed in space and time. By carefully considering the forms of the requirement and the achieved performance it may be found that quite simple models of reliability may be acceptable. For example, where the requirement is well removed from the design estimate so that variability in this region does not play an important part, then a castastrophic failure model may be quite adequate for the purpose. On the other hand, where the requirement is close to or overlapping the design estimate, this may lead to marginal operation and cause variability in this region to be very relevant and, in some cases, perhaps, more relevant than catastrophic modes of failure.

Reliability Model

The techniques for preparing a probabilistic model are generic and it is essential to know the exact problem which is being solved. Whilst a probabilistic model may be developed, it is necessary to consider the type of data available to feed into the model. The whole approach raises the question "At what level in the system, be it equipment or component-part level, can pertinent data be derived and used to synthesise the system reliability?" The model for synthesis may need to be changed or adapted in line with the changing characteristics of the system in operation. Hence, the question "By what means can we obtain feedback of data so that the model can be adaptive?" is also pertinent. In carrying out a reliability analysis of a system, it is assumed that a rigorous examination of the system's capability of functioning is undertaken, which serves deterministically to set up a frame of reference on which to build the probabilistic model. Clearly, if a system fundamentally is unable to function in the required way, then there is little point in going to the sophistication of more detailed mathematical models. Obviously, the model will be based on reliability parameters of interest such as the mean rate at which a system may fail. However, in practice, this may be more complex than just a mean figure and requires a statement being made as a function of time or environment in the form:

$$f(t) = \theta(t) \exp\left[-\int \theta(t)\,dt\right] \quad . \quad . \quad (2)$$

$f(t)$ being the probability density function for the events in the time domain and $\theta(t)$ the function describing the rate of occurrence of events with respect to time sometimes known as the event rate function. If $\theta(t)$ is constant of value θ, then the system failure can be interpreted as having a " mean rate of occurrence " and this gives the well known exponential form:

$$f(t) = \theta \exp(-\theta t) \quad . \quad . \quad . \quad (3)$$

The probability of failure up to any given time t, known as the cumulative probability function, $p_f(t)$, is obviously of interest and integrating the density function over this time range gives:

$$p_f(t) = \int_0^t f(t)\,dt \quad . \quad . \quad . \quad (4)$$

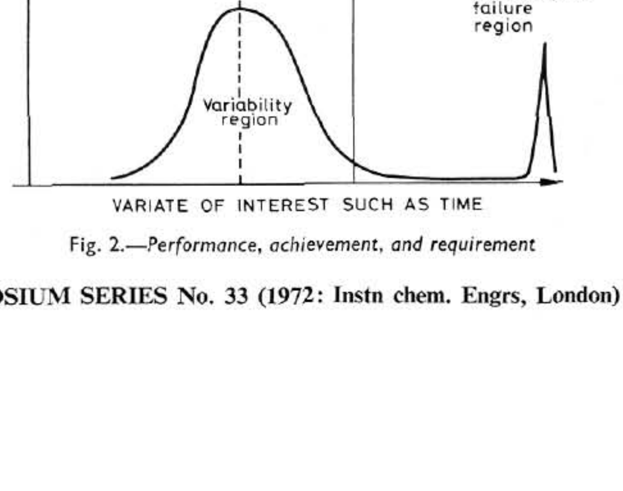

Fig. 2.—*Performance, achievement, and requirement*

If the event rate function can not be considered to be constant, it is pertinent to consider the reliability parameter which is the mean time to the first event or the first failure. This mean value, μ, is given by:

$$\mu = \int_0^\infty t\mathrm{f}(t)\,\mathrm{d}t \quad . \quad . \quad . \quad (5)$$

or:

$$\mu = \int_0^\infty [1-\mathrm{p}_f(t)]\,\mathrm{d}t \quad . \quad . \quad . \quad (6)$$

where $\mathrm{p}_f(t)$ is the cumulative probability function.

Combinations of failures may take place, for example, a failure may occur and stay in this particular state for some period of time during which time a second failure occurs. Clearly, it is necessary to consider the restoration time, or repair time, which will include the repair, replacement or restoring the failed device and the characteristic of repair time may be represented in a similar way to that described previously by replacing $\theta(t)$ with a repair rate function.

The availability $\mathrm{A}(t)$ or its complement, fractional dead time $\mathrm{D}(t)$, is related by $\mathrm{A}(t)+\mathrm{D}(t) = 1$ and it may be shown that the mean fractional dead time of $\mathrm{D}(t)$ is given by:

$$\mathrm{D} = \frac{\mu_r}{\mu_r+\mu_f} \quad . \quad . \quad . \quad (7)$$

where μ_f and μ_r are the mean values of the relevant failure and repair distributions. This equation assumes that the repair process starts immediately failure occurs but in some cases failures may remain undetected until some thorough checking or testing procedure is instituted and it may be shown[6] that the mean fractional dead time is then given by:

$$\mathrm{D} = \frac{1}{\tau_c}\int_0^{\tau_c} \mathrm{p}_f(t)\,\mathrm{d}t \quad . \quad . \quad . \quad (8)$$

where τ_c is the time between the checks or testing of the system.

Various reliability parameters of this type may enter into the mathematical model and calculations in the analysis of the system. Logical flow diagrams may be prepared which enable the probability of failure or success of each item in the system to be represented and the results combined in some logical fashion.

Whilst modelling can be developed along the lines indicated, problems can arise as the system becomes more complex. Hand calculations can become tedious and the use of an appropriate computer program is of great help. Typically, the NOTED program[7] has a strategy for calculating the probability, as a function of age and time delay, that a signal will pass through a network at a given time. This analytical program is general and will accept up to 200 different probability laws. These probability laws simulate any generally conceivable type of distribution and failure together with a variety of repair and maintenance schedules.

Another important point in preparing the model is the need for appropriate reliability data. The reliability analyst is not interested just in the " raw " data itself, but rather in the characteristics which may be derived from such data. These characteristics are those which been defined and illustrated in the foregoing sections and are considered in more detail in Ref. 14.

Plant Systems

The reliable and safe operation of plant is usually dependent upon the functioning of various systems and in the design various decisions have to be made upon the configuration of the systems. This problem is familiar when considering the configuration of a single-stream plant which may be cheaper to build and run but all the " production eggs " may be in one basket. However, redundancy techniques, such as the duplication of critical plant items, may be used to a certain extent and in the ultimate this line of thinking may lead to the consideration of a multi-stream plant where all the " production eggs " are not in one basket. Ideally, in considering the reliability of the various systems and sub-systems, one would like to have complete field data but this may not be readily available and there is a need to assemble or synthesise the reliability of the system from some level at which pertinent data may be available.

In making the decision, on the particular approach, it is necessary to have access to some organised bank of reliability data.[9] Although plant systems may vary from industry to industry, similar equipment and similar configurations are often observed and many of the environmental stressing conditions may be similar. The general areas of uniqueness in particular applications tend to be limited. Obviously, from such observations centralised massing-up of information narrows our confidence limits, or we may say our confidence is increased. Having derived some configuration of the systems involved, it is also of importance to consider the optimum operation and maintenance. The techniques which have been discussed earlier are generic but their application may be altered according to whether one is considering hazard evaluation or availability. In order to give an illustration of the techniques, the case is taken where the designer is called upon to evaluate the risk of a hazard occurring.

A typical plant may be represented by the block diagram in Fig. 3. The reactive feed is mixed with other constituents in stage 1 of the process and passed for further processing in stage 2 which is dependent upon electrical supplies and then to

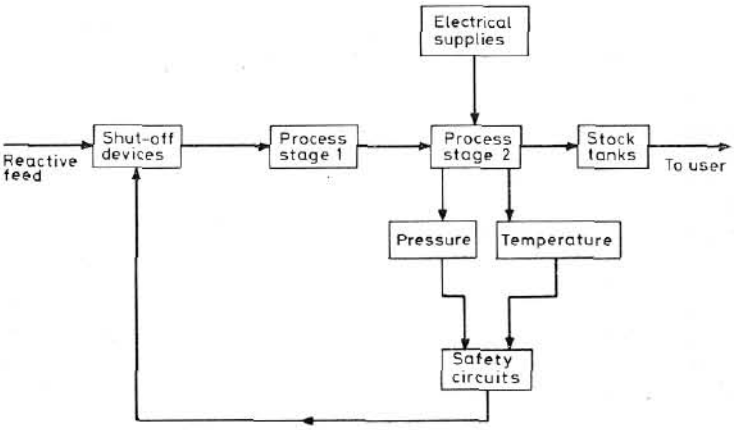

Fig. 3.—*Simplified diagram for typical process plant*

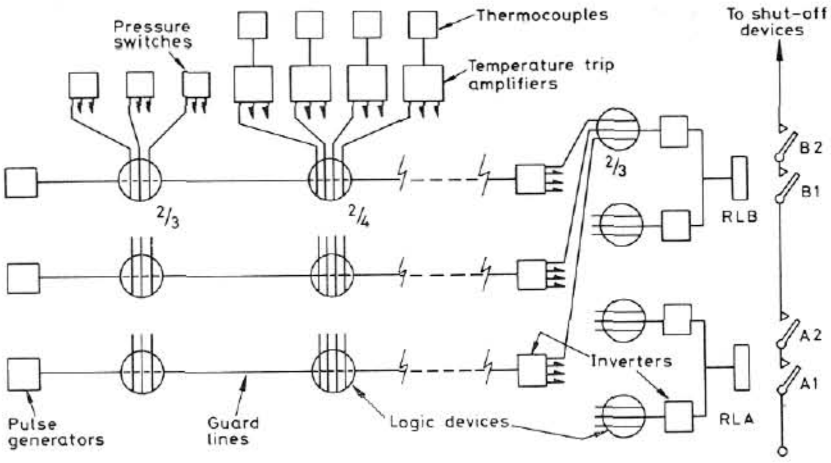

Fig. 4.—*Protective system*

stock tanks. It is assumed that in the event of the loss of electrical supplies then the abnormal conditions which exist give rise to a demand for the reactive feed to be automatically shut-off by the protective system. The equipment for a typical protective system of this type could be as shown in Fig. 4. In this case, pressure and temperature sensors are shown feeding signals on a majority voting basis into guard lines which also operate on a two-out-of-three majority voting basis. The outputs feed *via* contactors into the circuits for releasing the shut-off devices, the overall functional purpose being to operate the shut-off devices when any two or more out of three pressure switches operate or any two or more out of four thermocouples detect abnormal temperatures.

In the evaluation of such a system it will be necessary to commence with an assessment of the inherent ability of the system to operate. Then it will be necessary to study the equipment in its various modes of deviation or complete failure and to estimate the chances of the occurrence of such events. If large sample data exists at the equipment level, then it may be considered that detailed evaluations of the equipment may not be necessary. However, in the field of safety, and particularly when looking at rare events, it is often found necessary to consider the operation of the equipment at the component part level and to synthesise the overall failure time characteristic for the equipment.

Provided the individual component part failure rates are known and can be considered to be independent, then the overall failure rate of an equipment can be found by a process of summation. Therefore, if the equipment has n components working in their useful life phase[14] and if the failure of any one component causes the equipment to fail, then the overall mean failure rate for the equipment is given by:

$$F = \sum_{i=1}^{i=n} F_i \quad . \quad . \quad . \quad (9)$$

where F_i is the mean failure rate of the ith component.

Methods for predicting the failure rate of equipment are described in Refs 10, 11, and 14. Table I indicates the failure rates of some selected component parts and equipment for land-based nuclear installations. It has been found possible to use this type of failure rate information in other plant applications, taking into account different environmental and stress conditions.[14]

TABLE I.—*Component and Equipment Failure Rates*

Item	Failure Rate (faults/year)
Bellows	0·05
Diaphragms, metal	0·05
Gaskets	0·005
Springs, lightly stressed	0·002
Unions and junctions	0·004
Nut and bolt	0·0002
Transistor, alloy germanium	0·01
Transistor, alloy silicon	0·005
Diode, silicon zener	0·001
Relays, each coil (general)	0·003
Relays, each contact pair (general)	0·002
Relays, P.O. type (general)	0·01
Milliameter, moving coil	0·15
Strip chart recorder	1·7
Electronic power supply unit	0·23
Electronic trip amplifier	0·95
Electronic servo trip unit	2·5
Pressure switch	0·14
Pneumatic valve, 5 part	0·97
Pneumatic valve shut-off	1·9
Overhead transmission line	5·4
Three phase, oil-filled transformer	0·09
Centrifugal pump, water	6·0
Diesel engine	8·8
Oil boiler, steam raising	5·6

The failure rates given are applicable in general to components and equipments used in land-based nuclear installations.

Apart from complete failure of the system, it may be necessary to take into account variability of performance such as response time. This can occur for instance, in fast operating protective systems where reliability is very important and there tends to be marginal operation. The distribution of response time requires to be stated. There is a general trend to find that variations in performance parameters of equipment tend to follow a lognormal distribution. In certain types of safety shutdown mechanisms used in nuclear reactors the indications are to-date that the standard deviation of such distributions do not normally exceed about 10% of the mean value. Quite often a normal distribution can be taken as a good approximation over certain ranges of working.

The type of testing and maintenance requires to be considered and times specified for periodic testing and the time to repair it.

An abbreviated list of such characteristics for the simple protective system is given in Table II.

TABLE II.—*Typical Characteristics*

Item	θ_c (f/y)	τ_c (y)	θ_r (f/y)	τ_r (y)	Φ_s **Transfer function**	μ_τ **Mean** (s)	σ_τ **Standard Deviation** (s)
Pressure	0·025	0·25	0·075	10^{-4}	$\frac{s\tau}{1+s\tau}$	39·7	8·0
Temperature	0·05	0·25	0·37	10^{-4}	$\frac{s\tau}{1+s\tau}$	24·3	4·5
Logic device	2×10^{-4}	2·0	—	—	—	—	—
Inverter	10^{-3}	2·0	—	—	—	—	—
Contactor	10^{-3}	2·0	—	—	$e^{-S\tau}$	0·2	0·04

where:

θ_c = mean rate of occurrence of unrevealed faults in units of faults per year.

τ_c = time in years, between the routine test procedures which correct unrevealed faults.

θ_r = mean rate of occurrence of revealed faults in units of faults per year.

τ_r = mean repair time, in years, for the repair of revealed faults.

Φ_s = transfer function representing the operational delay time of the protective system.

μ_τ = mean value, in seconds, of the appropriate time constant.

σ_τ = standard deviation, in seconds, of the appropriate time constant.

A logical flow diagram for the protective system may be prepared as shown in Fig. 5 showing the signal paths and logical operations. A circle represents a logical operation; for example, in the case of a two-out-of-three operation at least two signals require to be present simultaneously in order for an output signal to be passed on through the system. The characteristics of the equipment given in Table II define the boxes shown in this logical flow diagrams. The overall system performance may be synthesized as described in Refs 7 and 14 using the techniques of logical analysis and probability theory. Assuming a specific form of input into the protective system *via* the sensors, then the probability of the failure of this system plotted against the time after a demand arising for action, may be derived as shown in Fig. 6. Due to inertias in the system this curve starts, as would be expected, from unity probability of failure and drops to a lower value of failure as time increases. On average, the temperature measurement would operate the system before the pressure measurement. However, the curve describes the probability of the complete system failing to operate taking into account both measurements. Depending upon the required time, so the probability of failure may be read off the curve, *e.g.*, a required 50 seconds time would correspond with a 10^{-4} probability of failure.

The evaluation of the probability for the loss of electrical supplies can be undertaken in a similar way, it being noted that the loss of electrical supplies in this example gives rise to a demand for automatic protection.

Hazard Probability

The reliability model which has been discussed permits a prediction to be made of the reliability of a system and also its fractional dead time. However, the criteria which have been previously discussed require the probability to be derived for a hazard, that is, when, say, an abnormal condition arises on a plant and the means of protection is in the failed state at the same time. This can be illustrated by the diagram in Fig. 7 where a system of protection is tested periodically at time, *T*, and due to failure the system is in the dead state and a demand *Y* occurs. Where a demand *X* arises and the system is not in the dead state, obviously there is no hazard. Hence, the probability of a hazard occurring will be dependent upon the fractional dead time of the protective system and the probability of the demand arising:

$$P_h(T) = P_d(T) \times D \qquad . \qquad . \quad (10)$$

where:

$P_h(T)$ = the probability of a hazard arising.

$P_d(T)$ = the probability of the demand arising.

D = the mean fraction dead time

= mean time failed/total time of interest.

T = the time of interest.

Hence, for the example of the process plant and assuming a time requirement of 50 s the probability of failure is given as

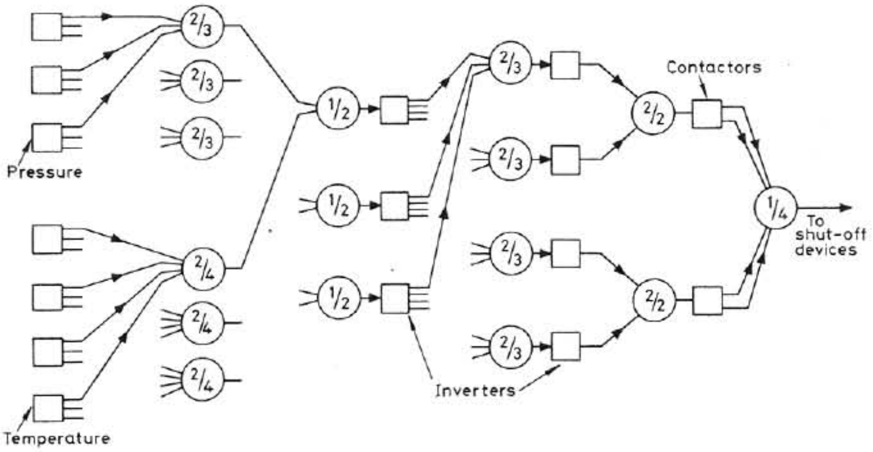

Fig. 5.—*Logical flow diagram*

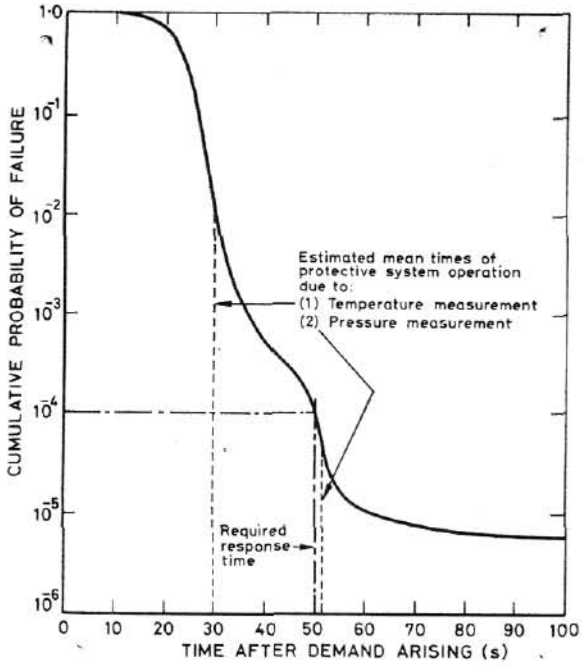

Fig. 6.—*Probability of failure with time*

10^{-4}. The corresponding mean fractional dead time is derived by applying equation (8) to the overall system cumulative probability function as described in Ref. 14, which in this instance can be shown to give:

$$D = 3\times10^{-5} \qquad . \quad . \quad . \quad (11)$$

Assuming that over a particular time of interest, T, the probability of a demand arising, *i.e.*, loss of electrical supplies, is 10^{-1}, then the hazard probability $P_h(T)$ is given from equations (10) and (11) by:

$$\begin{aligned} P_h(T) &= 10^{-1}\times3\times10^{-5} \\ &= 3\times10^{-6} \qquad . \quad . \quad . \quad (12) \end{aligned}$$

This could now be compared with some criterion as discussed earlier. A determination may be made of whether or not the overall hazard probability is acceptable and an evaluation made as to what action should be taken. Such action in the plant example quoted could be to decide whether further money should be expended or whether gains could be made in lessening the demand probability or improving the protective system.[15]

Conclusions

Quantified statements on reliability and related hazards may be used absolutely[12] or in a comparative manner when considering different systems. It must always be borne in mind that assessments involving this type of analysis not only institute a discipline in thinking and design but also give a very useful tool in the process of performance assessment.[13, 14]

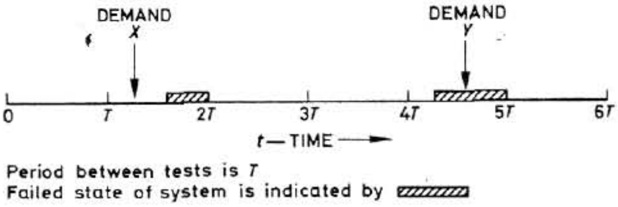
DEMAND
X
DEMAND
Y
0
T
2T
3T
4T
5T
6T
t—TIME
Period between tests is T
Failed state of system is indicated by ▨

Fig. 7.—*Dead time for system*

References

[1] Lindley, B. C. " Technological forecasting and corporate long-range planning ", *Electronics and Power*, October 1970, pp. 364–372.

[2] Tye, W. " *Degree of Reliability Required—Especially in Relation to Future Aircraft* ", The Royal Aeronautical Society and the Institution of Electrical Engineers Joint Conference on the Importance of Electricity in the Control of Aircraft, 1962.

[3] Farmer, F. R. " *Reactor Safety—The Carrot or the Stick*." Symposium on Public Safety—A Growing Factor in Modern Design, May 1, 1969. National Academy of Engineering, U.S.A.

[4] Beattie, J. R., Bell, G. D., and Edwards, J. E. " *Methods for the Evaluation of Risk* ", U.K.A.E.A. Report AHSB (S)R.159.

[5] Green, A. E. " Safety assessment of automatic and manual protective systems for reactors ", *Instrument Practice*, **24**, 109.

[6] Bourne, A. J. *Control*, 1967, **11**, 112.

[7] Woodcock, E. R. " *The Calculation of Reliability of Systems—The Program NOTED* ", U.K.A.E.A. Report AHSB (S)R.153.

[8] Green, A. E., and Bourne, A. J. " Reliability considerations for automatic protective systems ", *Nucl. Engng*, 1965, **10**, 111.

[9] " *SYREL Reliability Data Bank* ", published by the Systems Reliability Service, U.K.A.E.A.

[10] Eames, A. R. " Reliability assessment of protective systems " *Nucl. Engng*, 1966. **11**, No. 118, March.

[11] Green, A. E. " Reliability prediction ", *Proc. Instn Mech. Engng*, 1969–70, **184**, Part 3B.

[12] Bourne, A. J., and Green, A. E. *Nuclear Engineering and Design*, 1970, **13**, No. 2, August.

[13] Hensley, G. *Journal of the Institute of Measurement and Control*, *Vol.* **1**, April 1968.

[14] Green, A. E., and Bourne, A. J. " *Reliability Technology* ". To be published April 1972 by John Wiley & Sons Limited.

[15] Hensley, G. " *Plant and Process Reliability* ", November 1970. North Western Branch, Institution of Chemical Engineers, published in *Instrument Practice*, Vol. 25, No. 11, November 1971.

[16] Farmer, F. R. " *Experience in the Reduction of Risk* ", Institution of Chemical Engineers. *Symposium on Major Loss of Prevention in the Process Industries*, Newcastle upon Tyne, 6–9 July 1971.

The manuscript of this paper was received on 8 *February*, 1971.