J. Inst. Maths Applics (1974) **14,** 41–56

Deficiencies in Safety Schemes which Rely on Stochastically Failing Protective Equipment

J. H. POWELL

Safety in Mines Research Establishment, Department of Trade and Industry, Sheffield

[Received 6 February 1973 and in revised form 15 May 1973]

Probability theory is used to assess the deficiencies of safety schemes which rely on devices which can fail either in an undetected manner only, or in both undetected and detected ways. Three quantities are used to express the deficiencies of these schemes; the mean period during which devices are ineffective, the proportion of time for which they are ineffective and the distribution of the durations of their ineffective periods. Analytical expressions are derived for these quantities for a scheme in which only undetected failures occur and devices are replaced at regular intervals. Monte Carlo simulation techniques are used to estimate the measures of deficiency for situations in which both types of failure are possible. Consideration is given to the "cost-benefit" aspects of safety schemes in simple circumstances in which the rate of occurrence of the hazards involved, and the penalty to be paid in the event of a catastrophe, are known.

1. Introduction

THE CIRCUMSTANCES considered relate to devices which for most of their operational life are "on stand-by", or in a passive state, but which may be called into active operation under conditions that occur infrequently and unexpectedly. Such circumstances occur, for example, with safety devices or protective devices that are not required to operate actively unless the hazardous conditions against which they guard occur. The devices considered are assumed to be subject to at least one form of failure that can go "undetected". In this context the word "failure" is defined as the inability of a device to function as intended if the hazard which it is designed to meet should arise. An "undetected" failure is one in which the potential malfunction of a device does not readily manifest itself in the absence of the hazard—for example, a destructive test may be necessary to reveal the fault or testing arrangements may be defective. Similarly, a "detected" failure is one in which the inability of a device to carry out its designed function is readily revealed by inspection or by simple, *in situ* non-destructive testing.

Two situations are studied here in some detail. In the first situation it is assumed that the safety devices are subject only to the undetected mode of failure, and that some form of renewing all the devices is practised at regular intervals to ensure that, for a reasonable proportion of operational time, there are devices which will operate satisfactorily if called upon to do so. In the second situation, it is assumed that devices are subject to both detected and undetected modes of failure, and that a device which fails detectably is immediately renewed. Additional renewal, either of devices in bulk at regular intervals or of individual devices on the basis of their age in service, may also be practised in this latter situation to increase the protection provided by a safety scheme.

In both situations interest lies in estimating the time during which devices are in an ineffective state, and how this time is related to the failure characteristics of the devices and the frequency of maintenance, inspection, or replacement of the device. Furthermore, it is of practical importance in planning a safety scheme to be able to estimate the rate of supply of new devices or the extent of maintenance facilities required to achieve a given effectiveness of operation. For the simpler situation in which devices fail only in an undetected mode, cost-benefit aspects of operating a safety scheme are considered in circumstances where the rate of the hazard and the cost of a catastrophe are assumed to be known. It is believed that the two sets of circumstances outlined above typify many situations in which warning devices and protective equipment operate.

2. Failure Distributions

Following usual practice (Barlow & Proschan, 1965) the failure characteristics of safety devices are represented by the probability distributions of their time-to-failure, viz.

$$F(t) = \text{Probability } (\tau \leqslant t)$$

where τ is any random value of the time-to-failure, and t is a specified value of this variable. Only continuous probability distribution functions will be used here to describe failure characteristics, so that the probability–density function corresponding to $F(t)$ will be defined by

$$f(t) = F'(t).$$

The failure rate of devices is defined by

$$r(t) = f(t)/(1-F(t))$$

which may be interpreted as either the instantaneous probability of a device failing at time t, or for a sufficiently large population, the ratio of failures occurring per unit time to the number of devices that have not failed up to the time t.

Considerable attention has been devoted elsewhere to the representation of the failure characteristics of manufactured devices by appropriate statistical distribution functions, for example by Barlow & Proschan (1965) and by Gnedenko, Belyayev & Soloyev (1969). The practical aspects of determining these distributions and estimating their parameters for devices under operating conditions are discussed by Gnedenko *et al.* (1969) and by Calabro (1962).

In the present study, failure characteristics of safety devices will, for the most part, be represented by negative exponential distributions of their times-to-failure, which implies constant failure rate, viz.

$$F(t) = 1-\exp(-kt), \quad \text{and} \quad r(t) = k$$

In a sense this is a favourable representation of failure characteristics because it implies that devices do not become more susceptible to failure the longer they are in service. In practice it is often found that manufactured devices have a decreasing failure rate in the early stage of their service as manufacturing faults are exposed by the rigours of service conditions. However, this is usually a transitory stage, and one would presume that quality control and inspection during the manufacture of safety devices would be particularly stringent to mitigate this type of failure.

Failure characteristics which imply deterioration in the reliability of devices with age in service will be represented here by gamma distributions of times-to-failure, since with suitably chosen parameters these distributions imply increasing failure rates. In general, the distribution function and failure rate for gamma distributions are given by

$$F(t) = \gamma(\alpha, bt)/\Gamma(\alpha), \quad \text{and} \quad r(t) = b^{\alpha}t^{\alpha-1} \exp(-bt)/\Gamma(\alpha, bt).$$

For positive integer values of α (say i) and $b > 0$, these become

$$F(t) = 1-e_{i-1}(bt) \exp(-bt), \qquad \text{and} \quad r(t) = b^{i}t^{i-1}/e_{i-1}(bt) \,.\, (i-1)!$$

$r(t)$ being a monotonic increasing function of t. The notation used here is due to Abramowitz & Segun (1964) for the incomplete gamma function and related functions. A physical interpretation of integral-order gamma distributions in representing failure characteristics is that a device will suffer i Poisson-distributed random shocks before it fails, i being the order of the distribution.

For the purpose of comparing the effects that different types of failure characteristics for safety devices will have on the deficiencies of a safety scheme, it is necessary that the devices compared should be of equivalent "quality" in some sense. In the situation in which all devices are renewed at regular intervals, the criterion adopted here for equivalent quality is that the mean time-to-failure for those devices which fail within the renewal interval should be the same for the two distributions used to represent devices having non-deteriorating and deteriorating reliability characteristics respectively. The mean time-to-failure in a renewal interval T is defined by

$$\bar{A}(T) = \int_0^T tf(t)\, dt/F(T).$$

In the particular case of so-called "undetectable" device failures, it is assumed that such failures may be determined under special conditions. Namely, by putting the device or component under laboratory-simulated hazard conditions to see if it responds in the desired manner. Such tests will only be meaningful if they are carried out on devices which have been operating under full service conditions. The tests are envisaged as being of a nature which would disrupt the normal working of a system if carried out *in situ*, and may even destroy the device tested. Thus estimation of the parameters of the failure distribution will, in general, require sampling the system for devices which have spent various times in service and which are still apparently in working order, and subjecting this sample of devices to the special tests.

3. Devices that Fail in an Undetected Manner Only and are Replaced at Regular Intervals

This is the first of the situations mentioned in the introduction. For this situation general expressions for the mean ineffective duration $\bar{l}$, the proportion of time ineffective R, and the distribution function for the durations of ineffective periods $V(t)$ are readily deduced from elementary probability theory, viz.

$$\bar{t} = (1/F(T)) \int_0^T f(T-u)u\,du \tag{3.1}$$

$$R = (1/T) \int_0^T f(T-u)u\,du \tag{3.2}$$

$$V(t) = (1/F(T)) \int_0^t f(T-u)\,du, \qquad 0 < t \leqslant T \tag{3.3}$$

where T is the time interval between replacements.

In particular, for negative exponential distributions of times to failure, these expressions become:

$$\bar{t}_e = (T-1/k+(1/k)\exp(-kT))/(1-\exp(-kT)) \tag{3.4}$$

$$R_e = (1/T)(T-1/k+(1/k)\exp(-kT)) \tag{3.5}$$

$$V_e(t) = (\exp(-k(T-t))-\exp(-kT))/(1-\exp(-kT)), \qquad 0 < t \leqslant T. \tag{3.6}$$

The mean time-to-device-failure in the replacement interval T is given by

$$\bar{A}_e(T) = 1/k - T\exp(-kT)/(1-\exp(-kT)). \tag{3.7}$$

The corresponding quantities for ith order gamma distributions of times to failure are:

$$\bar{t}_g = T - \frac{i(1-\exp(-bT)e_i(bT))}{b(1-\exp(-bT)e_{i-1}(bT))} \tag{3.8}$$

$$R_g = (1-\exp(-bT)e_{i-1}(bT)) - (i/bT)(1-\exp(-bT)e_i(bT)) \tag{3.9}$$

$$V_g(t) = \frac{e_{i-1}(b(T-t))\exp(-b(T-t)) - e_{i-1}(bt)\exp(-bT)}{(1-\exp(-bT)e_{i-1}(bt))}, \qquad 0 < t \leqslant T \tag{3.10}$$

$$\bar{A}_g(T) = i/b - \frac{T\exp(-bT)\,.\,(bT)^{i-1}}{(1-\exp(-bT)e_{i-1}(bT))\,.\,(i-1)!} \tag{3.11}$$

4. Devices which can Fail in Both an Undetected and Detected Manner

This is the second situation mentioned in the introduction. Devices are assumed to be renewed immediately they fail in a detected manner, or (if they do not so fail) when they have been in service for a specified period of time; otherwise they are allowed to continue in service. If a device suffers an undetected failure, this is assumed to have no effect upon its probability of subsequently suffering a detected failure.

For this situation, theoretical expressions are not readily derived from probability theory for all the quantities of interest, and these have been estimated by resorting to Monte Carlo computer simulation of the circumstances. In the particular case in which times to detected and undetected failures are distributed according to negative exponential distributions, and in which no age-renewal of devices is practised, some of the quantities may be deduced from probability theory, and they can therefore be compared with the corresponding statistical estimates from the simulation experiments.

When no age-renewal is practised, devices are renewed only when they fail in a detected mode. Assuming the times-to-detected-failure to be exponentially distributed, the probability of n renewals in a given time t will conform to a Poisson distribution:

$$P_n(t) = \frac{(k_1 t)^n \exp(-k_1 t)}{n!}, \qquad \text{for } n = 0, 1, 2, \ldots. \tag{4.1}$$

where k_1 is the failure rate for devices failing in a detected mode.

In general the assumption of a negative exponential distribution of times to undetected failures does not imply a Poisson distribution for the number of undetected failures in a time t, because, if a device fails in this way, it cannot fail similarly again and must await renewal. However, it is readily shown (cf. Appendix) that the probability that no undetected failure occurs in a time t is given by

$$Q_0(t) = \exp(-k_2 t) \tag{4.2}$$

where k_2 is the failure rate for devices failing in an undetected mode. It will be noted that this particular quantity is, in general, independent of the failure rate assumed for detected failures; and, because of the way in which it is derived, it does not depend on any age-renewal scheme which might be operated. Expressions have also been deduced (cf. Appendix) for the probabilities of one and two undetected failures occurring in a time t, viz.

$$Q_1(t) = \begin{cases} \dfrac{k_2^2(\exp(-k_1 t) - \exp(-k_2 t))}{(k_2 - k_1)^2} - \dfrac{k_1 k_2 t \exp(-k_2 t)}{(k_2 - k_1)}, & k_1 \neq k_2 \quad (4.3a) \\ \exp(-kt)(kt + (kt)^2/2), & k = k_1 = k_2 \quad (4.3b) \end{cases}$$

$$Q_2(t) = \begin{cases} \dfrac{k_1 k_2^2}{(k_2 - k_1)^2} \left\{ \dfrac{(2k_2 + k_1)(\exp(-k_2 t) - \exp(-k_1 t))}{(k_2 - k_1)^2} \right. \\ \qquad + \dfrac{k_2 t(\exp(-k_2 t) + \exp(-k_1 t))}{(k_2 - k_1)} \\ \qquad \left. + k_1 t \exp(-k_2 t)(1/(k_2 - k_1) + t/2) \right\}, & k_1 \neq k_2 \quad (4.4a) \\ \exp(-kt)((kt)^3/3! + (kt)^4/4!), & k = k_1 = k_2 \quad (4.4b) \end{cases}$$

From (4.3b) and (4.4b) one would conjecture that, for $k = k_1 = k_2$, the probability of the occurrence of n undetected failures in time t will be given by

$$Q_n(t) = \exp(-kt)((kt)^{2n-1}/(2n-1)! + (kt)^{2n}/(2n)!), \qquad n > 0 \tag{4.5a}$$

The Laplace transforms of $Q_1(t)$ and $Q_2(t)$ have simple algebraic forms which suggest that the similar transform of the general probability $Q_n(t)$ may be represented by

$$Q_n(s) = \frac{k_1^{n-1} k_2^n (s + k_1 + k_2)}{(s + k_1)^n (s + k_2)^{n+1}}, \qquad n = 1, 2, 3, \ldots.$$

For $k_1 = k_2 = k$, the inverse of this transform gives the result quoted in equation (4.5a). For $k_1 \neq k_2$, the inverse of the transform is

$$Q_n(t) = \frac{k_1^{n-1}k_2^n}{(k_2-k_1)^n} \times$$
$$\times\left\{\frac{\exp(-k_1 t)}{n!(k_2-k_1)}\left[\sum_{i=0}^{n-2}\frac{(n+i)!t^{n-i-2}}{(n-i-2)!i!(k_1-k_2)^i}+k_2\sum_{i=0}^{n-1}\frac{(n+i)!t^{n-i-1}}{(n-i-1)!i!(k_1-k_2)^i}\right]\right.$$
$$\left.+\frac{(-)^n\exp(-k_2 t)}{(n-1)!}\left[\sum_{i=0}^{n-1}\frac{(n+i-1)!t^{n-i-1}}{(n-i-1)!i!(k_2-k_1)^i}+k_1\sum_{i=0}^{n}\frac{(n+i-1)!t^{n-i}}{(n-i)!i!(k_2-k_1)^i}\right]\right\} \tag{4.5b}$$

Substitution of $n = 0$ in (4.5a) or (4.5b) also gives the same result as that derived *ab initio* for $Q_0(t)$.

Another quantity which may be simply derived for this situation is the proportion of undetected failures in the population at any instant. This is achieved by considering an undetected failure to represent a "death" process, and the detected failure of a device which had previously suffered an undetected failure to represent a "rebirth" process. This results in a differential equation.

$$dm/dt = (N-m)k_2 - mk_1 \tag{4.6}$$

where m is the number of undetected failures at time t in a population with N devices in service, and k_1 and k_2 are respectively the failure rates for detected and undetected failures. Clearly $m = 0$ for $t = 0$. This equation has the solution

$$(m/N) = k_2(1-\exp(-(k_1+k_2)t))/(k_1+k_2). \tag{4.7}$$

From (4.7) the proportion of undetected failures in a population when steady-state conditions are attained, $(m/N)_{ss}$, is given by

$$(m/N)_{ss} = k_2/(k_1+k_2). \tag{4.8}$$

5. Monte Carlo Simulation Experiments

The general circumstances typifying the operation of safety schemes were simulated on a computer using a FORTRAN source program which incorporated an assembly-language subroutine for the generation of pseudo-random numbers. The general principles of the Monte Carlo method and those of pseudo-random number generation are described in standard texts, e.g. Schreider (1964) and Hammersley & Handscomb (1964).

In the computer simulation, a course of events involving a succession of failures and renewals of safety devices installed at a particular location is followed. For each device a random selection of its times to detected and undetected failure is made; these two times are compared with each other and also with the specified age-renewal time to determine the period of time (if any) that the device has been ineffective in service, and the time at which the device should be renewed. This procedure is repeated for each of the successive devices installed at the location in question; the times for which devices are ineffective, and the times between renewals, are accumulated. The latter quantity is the time elapsed in the operation of the safety scheme, and a "trial" is said to be completed when the time elapsed indicates the expiry of the predetermined total operation time for the safety scheme. A large number of trials are carried out, each trial using a different sequence of pseudo-random numbers to generate the times-to-failure for the succession of devices. Histograms are compiled of the frequency of occurrence of each type of failure in a trial, and also for the distribution of ineffective periods. Estimates of the mean duration, and the expected proportion of operational time for which devices will be ineffective, are computed from these repeated trials.

An alternative way of viewing this simulation is that each trial represents a possible course of events experienced by an individual member of a large population issued with protective appliances. This interpretation of the simulation gives direct meaning to a quantity mentioned earlier, namely, the proportion of individuals in a population who have defective devices at any time.

With slight modification the same computer program served to simulate each of the two safety-scheme situations mentioned in previous sections.

For the situation in which only undetected failures occur and all devices are renewed at regular intervals, simulation experiments based on 1000 trials gave estimates of $\bar{t}$ and R (cf. Section 3) in close agreement with the theoretical "infinite population" results for both negative exponential and gamma failure distributions (equations (3.4), (3.5), (3.8), and (3.9)). A comparison of the distributions of the durations of ineffective times, $V(t)$, which result from these two failure distributions is shown in Fig. 1. The failure distributions are comparable when judged by the criterion

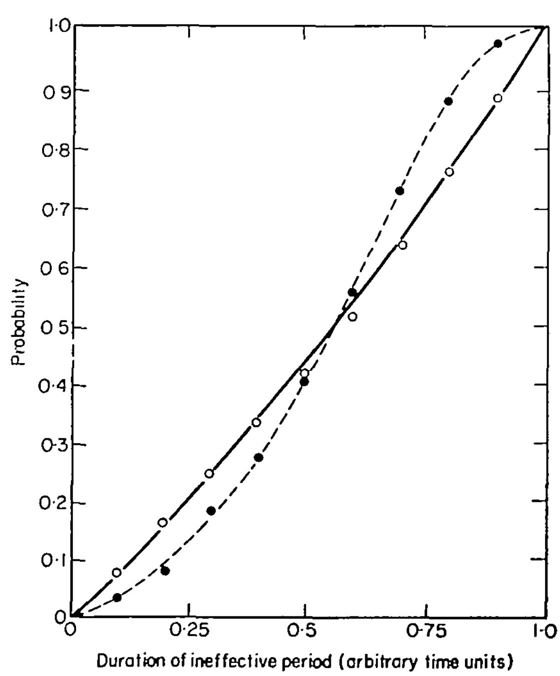

FIG. 1. Distribution function of durations for which devices are ineffective exponential and gamma device failure distributions. —, theoretical distribution function for exponential failure distribution; - - -, theoretical distribution function for 3rd order gamma failure distribution; ○, simulation result for exponential failure distribution; ●, simulation result for 3rd order gamma failure distribution. Replacement interval = 1 arbitrary time unit. Parameter for exponential distribution, $k = 0{\cdot}5t^{-1}$. Parameter for 3rd order gamma distribution, $b = 5{\cdot}88t^{-1}$.

described in Section 2, i.e. $\bar{A}_e(T) = \bar{A}_g(T)$ (cf. equations (3.7) and (3.11)). The points plotted on Fig. 1 are the results of simulation experiments; the curves illustrate the corresponding theoretical results from expressions (3.6) and (3.10).

Similarly, for the situation in which both detected and undetected failures occur and no age-renewal is practised, the simulation experiments using 1000 trials gave estimates in close agreement with the theoretical "infinite population" results from expressions (4.1) to (4.5). A comparison between theoretical and simulation results for the number of undetected failures in a population of 1000 as a function of time for two sets of failure characteristics is shown in Fig. 2. The points are simulation results; the curves are the corresponding theoretical results from (4.7).

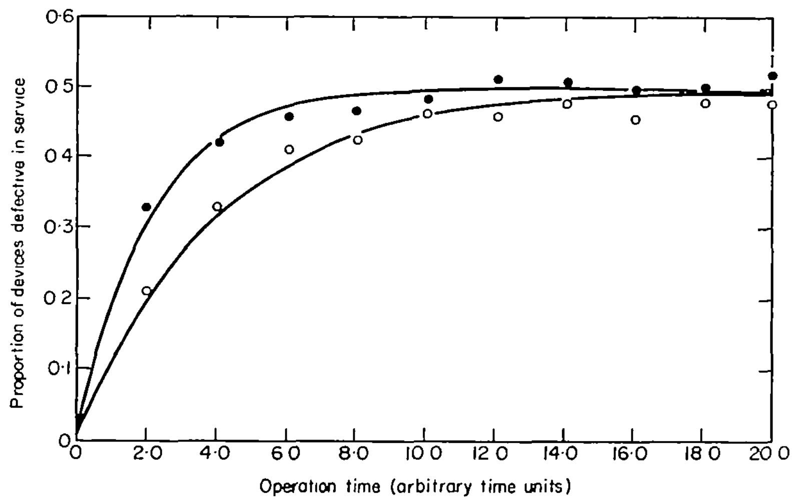

FIG. 2. Proportion of devices defective *vs.* operation time. Upper curve, infinite population results for $k_1 = k_2 = 0{\cdot}25t^{-1}$; lower curve, infinite population results for $k_1 = k_2 = 0{\cdot}125t^{-1}$; see (4.7). ●, simulated results for $k_1 = k_2 = 0{\cdot}25t^{-1}$; ○, simulated results for $k_1 = k_2 = 0{\cdot}125t^{-1}$.

In situations in which detected failures occur, individual devices are renewed at randomly distributed times. This stochastic renewal of devices complicates mathematical analysis of the circumstances so that, as yet, analytical expressions have not been derived for the three quantities $\bar{l}$, R, and $V(t)$ for such situations. However, the quantities mentioned are of importance in assessing the deficiencies of any safety scheme; and, since only estimates derived from simulation are available for them, it is important to have some idea of the statistical accuracy of the simulation results for a reasonable number of trials (1000 trials gave convenient computer run-times in this work). Accordingly, a few extended simulation experiments involving 10,000 trials were carried out. From a comparison of their results with those from experiments involving 1000 trials, it was concluded that the improvement in accuracy of the estimates did not in general justify the additional computer time used. Furthermore, a number of experiments, each of 1000 trials, were carried out using a different sequence of random numbers for each experiment. For a particular set of failure characteristics, the coefficient of variation of the estimates from these latter experiments was 3·2% for the mean period ineffective, and 5·6% for the proportion of time ineffective.

Results of simulation experiments for a range of failure characteristics and age-renewal intervals are shown in Fig. 3 for safety devices which can fail in a detected or an undetected mode at exponentially distributed times. The quantity used in this figure to express deficiency in protection is the proportion of operational time, R, for which devices were ineffective.

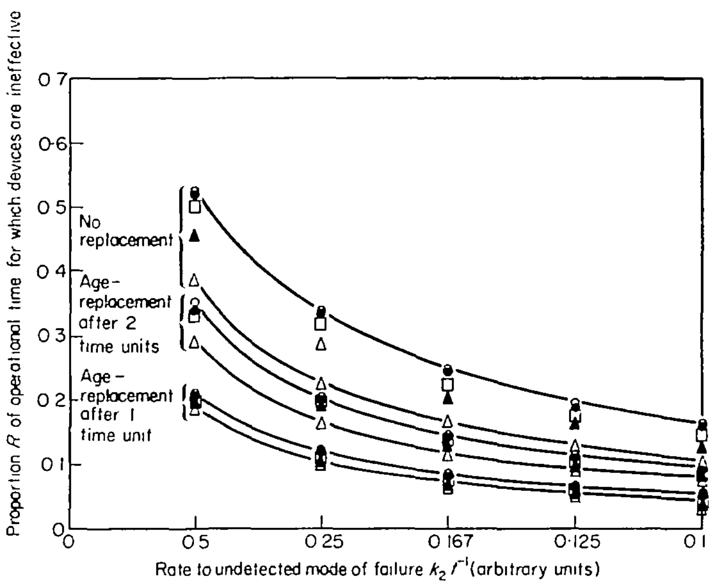

FIG. 3. Proportion of time safety devices are ineffective in an operational period of 4 arbitrary time units. Devices subject to detected and undetected failures at exponentially distributed times. Rates to detected failure are, respectively; ○, $k_1t^{-1} = 0{\cdot}100t^{-1}$; ●, $k_1t^{-1} = 0{\cdot}125t^{-1}$; □, $k_1t^{-1} = 0{\cdot}167t^{-1}$; ▲, $k_1t^{-1} = 0{\cdot}250t^{-1}$; △, $k_1t^{-1} = 0{\cdot}500t^{-1}$.

6. Cost-benefit Aspects of Safety Schemes

Optimal replacement of stochastically failing components has received considerable attention, a variety of circumstances being treated in the literature on the subject. Barlow & Proschan (1962, 1963, 1965) and Radner, Jorgenson & McCall (1967) give summaries and bibliographies of the more recent work.

Most authors assume that the components fail only in an undetected manner, and schemes are optimized in terms of the cost of inspection and/or replacement of components together with a penalty cost which is assumed to be proportional to the period of time for which a component is in service in an undetected, defective state. The main treatment in this study is also for devices which fail in an undetected manner, and are replaced at regular intervals. But in the present paper, the penalty for devices being in a defective state is assumed to be dependent upon the probability of occurrence of hazardous events whilst they are in this condition, and consideration is given to the case where the cost of a device is related to its durability.

In what follows, devices will be assumed to fail in an undetected manner after times which are distributed according to negative exponential distributions. The same form of distribution will be adopted for the times between the hazardous events against which the scheme is intended to offer protection. The quantity to be optimized is the cost per unit time attributable to operation of the safety scheme. This cost will contain a factor relating to the rate of regular replacement of the devices; this will be inversely proportional to the interval T, say, between replacements. The unit cost of devices will be assumed to be a function of their failure rate, say $A(k)$, to express the dependence of this cost on the durability of the devices. Thus the first component of the cost per unit time of the scheme arising from regular replacement of devices has the form $A(k)/T$.

A second component of cost per unit time takes account of the risk that hazardous events will occur during periods when devices are defective. The probability of this in an interval T is

$$H(T) = \begin{cases} 1-\exp(-kT)-kT\exp(-kT), & h = k \\ 1+(1/(h-k))(k\exp(-hT)-h\exp(-kT)), & h \neq k \end{cases} \tag{6.1}$$

where h is the rate of occurrence of hazardous events. Suppose that it is possible to quantify the penalty D attributable to a catastrophe caused by the combination of a hazardous event and a defective device. Then the contribution from this source to the cost per unit time for operating the scheme can be looked upon as having the same form as an insurance premium related to the risk of such an event, viz. $D \,.\, H(T)/T$. Thus the total cost per unit time for operating the safety scheme is

$$C = \begin{cases} A(k)/T+(D/T)(1-\exp(-kT)-kT\exp(-kT)); & h = k \\ A(k)/T+(D/T)(1+(1/(h-k))(k\exp(-hT)-h\exp(-kT))); & h \neq k \end{cases} \tag{6.2}$$

The benefit, B, offered by a safety scheme is assumed to be measured by the proportion of the time between replacements for which, on average, the safety devices are effective. For exponentially distributed times to failure, (3.5) gives this proportion as

$$B = (1-R_e) = (1-\exp(-kT))/kT \tag{6.3}$$

In choosing this quantity as a measure of the benefit derived from operating a safety scheme, the pattern of occurrence of the hazardous events which the scheme is intended to combat has been deliberately ignored. The attitude taken is that the non-occurrence of such events during periods when there is no protection, owing to device failure, is fortuitous and does not accrue from efforts made in operating the scheme. Conversely, if hazardous events do not occur when devices are potentially effective, it is not considered that effort has been wasted in operating the scheme.

The two quantities which may be considered to be at the disposal of the planner of a safety scheme which optimize cost and benefit are the interval between replacements, which is readily controlled, and the failure rate of the safety devices, which is not so readily controllable.

For $k > 0$, and $0 < T < \infty$, (6.3) shows the benefit B as a monotonically decreasing function of T. Thus there is no maximum benefit to be attained for positive values of T or k, so that the benefit required from the scheme must be arbitrarily specified in the range $0 < B < 1$. There is therefore a value of the product kT (a, say) which satisfies (6.3) for a specified benefit.

If the durability of the devices is fixed (i.e. $A(k)$ is a constant, say A), the simplified conditions permit precise mathematical analysis of the situation. Now the replacement interval T is the only quantity on which optimization can be sought. Thus the cost and benefit equations, (6.2) and (6.3) respectively, cannot be satisfied independently. If an arbitrarily required benefit or degree of protection (B) is specified, a replacement time T is implied which is merely the solution of (6.3) for the specified values of B and k.

Alternatively, if estimates are available for the replacement cost (A), the cost of a catastrophe (D), the device failure rate (k), and the hazard rate (h), then the replacement interval which minimizes the cost function (C) can be found by solving the equation

$$A/D = \begin{cases} (1+kT+k^2T^2)\exp(-kT)-1, & h = k \\ \left[\dfrac{v(1+kT)\exp(-kT)-(1+kvT)\exp(-kvT)}{(v-1)}\right]-1, & h \neq k \end{cases} \tag{6.4}$$

where $v = h/k$. For $v, k, T > 0$, this equation has a maximum with respect to T at

$$T = T_c = \begin{cases} 1/k, & h = k \\ \ln(v)/k(v-1), & h \neq k. \end{cases} \tag{6.5}$$

The value of the cost ratio at this point is

$$(A/D)_c = \begin{cases} 3e^{-1}-1, & h = k \\ \left[\dfrac{(v)^{(v-2)/(v-1)}(1+\ln(v)/(v-1))-(v)^{-v/(v-1)}(1+v\ln(v)/(v-1))}{(v-1)}\right]-1, & h \neq k. \end{cases} \tag{6.6}$$

Thus, for a given ratio v of the hazard rate to the device failure rate, there is a critical maximum ratio of the cost of a device to the cost of a catastrophe beyond which the cost function C for a safety scheme cannot be optimized. For a cost ratio less than this critical maximum, there are two roots to (6.4) viz. $0 < T_1 < T_c < T_2$, and the smaller of these, T_1, minimizes the cost function C (expression (6.2)). Table 1 shows the critical maximum cost ratios for various values of v. It is noteworthy that at both extremes of the ratio v the cost of a device must be small compared with the penalty for a catastrophe if a protective scheme is to be justifiable on cost grounds. When the hazard rate is small compared with the device failure rate, the risk of having to pay the penalty for a catastrophe is small. When the hazard rate is large compared with the device failure rate, a very high frequency of device replacement is necessary to maintain protection and to avoid repeated payment of the catastrophe penalty. In practice, estimation of D will be difficult. The damage caused by a catastrophe will usually be difficult to predict; it will contain random components, and if human injury or fatality is possible purely quantitative estimates become notoriously difficult to make.

Table 1 also records the replacement intervals to achieve minimum cost per unit time for operating a scheme for device-to-penalty cost ratios which are a half of the critical values of these ratios, and the corresponding minimum cost for unit device-failure-rate (i.e. $k = 1{\cdot}0$) taking the cost of a device as unity (i.e. $A = 1{\cdot}0$). Optimizing replacement intervals are inversely proportional to device-failure-rate, and minimum costs are directly proportional to this quantity, for a particular value of v.

The foregoing paragraphs describe a particularly simple set of circumstances which serve mainly to illustrate the broad features of the cost–benefit aspects of safety schemes. In general precise and purely analytical investigations of more complicated circumstances will not be possible.

TABLE 1

Cost optimization for safety devices subject to undetected failure

Hazard rate / Failure rate v	Critical maximum cost ratio $(A/D)_c$	Critical replacement interval T_c	Selected cost ratio $(A/D)_s = \frac{1}{2}(A/D)_c$	Optimizing † replacement interval for $(A/D)_s$	Minimum cost † for $(A/D)_s$ for $A = 1$
0·01	0·0085	4·652	0·0042	1·454	1·795
0·10	0·0498	2·558	0·0249	1·023	2·426
0·50	0·0966	1·386	0·0483	0·602	3·985
1·00	0·1036	1·000	0·0518	0·438	5·456
10·00	0·0498	0·256	0·0249	0·102	24·260

† Optimizing intervals and minimum costs are quoted for unit failure rate (i.e. $k = 1$), these are inversely and directly proportional respectively to the failure rate (k) for a fixed hazard rate to failure rate ratio (v).

If the cost of a device is assumed to be related to its durability by the function $A(k)$, and the benefit B required of a scheme is specified, both the replacement interval and the device-failure-rate, which minimizes the cost per unit time for operating a scheme, may be deduced. For a specified benefit $k = a/t$ (where a is the value of the product kT which satisfies (6.3)) can be substituted in the cost function equation (6.2) to give

$$C = \begin{cases} \dfrac{A(a/T)}{T} + \dfrac{D}{T}(1-\exp(-a) - a\exp(-a)), & h = k \\[2ex] A(a/T) + \dfrac{D}{T}\left(1 + \dfrac{a\exp(-hT) - hT\exp(-a)}{(hT-a)}\right), & h \neq k. \end{cases} \tag{6.7}$$

Stationary values of C, if they exist, will be at the values of T which satisfy the equation:

$$\frac{A'T - A}{D} = \begin{cases} 1 - \exp(-a) - a\exp(-a), & hT = a \\[2ex] 1 + \dfrac{a\exp(-hT)(h^2T^2 + (2-a)hT - a) - h^2T^2\exp(-a)}{(hT-a)^2}, & hT \neq a \end{cases} \tag{6.8}$$

where $A' = dA(a/T)/dT$. A specified form for the function $A(k)$ is required to determine the properties of (6.8), so that the conditions under which (6.8) will have real roots in T cannot be generally stated. However, from the formulation of the problem, and the general indications from the analysis of the simpler circumstances given above, one would expect that (6.8) would have real roots in T, and that the least of them would correspond to a minimum for C. If this is not the case, one would suspect inconsistencies amongst the values specified for degree of protection (which will be an arbitrary, subjective assignment), the cost of device replacement, the penalty to be paid in event of a catastrophe, and the hazard rate. Otherwise the smallest real root of (6.8), say T_{opt}, will give the cost-optimizing replacement interval, and the required durability (i.e. failure rate) will be given by $k_{opt} = a/T_{opt}$, to achieve optimization of cost at the specified degree of protection or benefit.

In both the examples considered so far, it has been assumed that devices are replaced at regular intervals and that the rate of occurrence of the hazard is constant. These two assumptions mean that all the replacement intervals making up the total time of operation of the safety scheme are stochastically equivalent to each other, so that only the probabilities of events occurring during an interval T between replacements need to be taken into account in a cost-benefit analysis of the schemes. When either replacements are made at irregular intervals, or the hazard rate is time-dependent, or both, there are no equivalent intervals and it becomes necessary to consider the total time of operation of a safety scheme.

Irregular replacement or renewal of safety devices is, in practice, more likely to be the rule rather than the exception. Many such devices are rendered inoperative after dealing with a hazard; automatically operated fire extinguishers are a common example. Renewal in these circumstances will be at random times determined by occurrence of the hazard itself. Barlow & Proschan (1963) consider another situation where irregular replacement arises, namely, when devices are inspected at intervals but are replaced only if they are found to be defective. These authors develop a computational algorithm for determining the optimum checking procedures in these circumstances. The algorithm takes account of the relative costs of inspection and replacement, failure characteristics of the devices, and a penalty which is proportional to the period of time for which devices are defective in service.

Irregular replacement times are a feature of the situations introduced in Section 4, because devices are replaced when they fail detectably and this mode of failure occurs at randomly distributed times. The effect of this stochastic replacement of devices on the quantities used to measure the deficiency of a safety scheme is exemplified in Fig. 2 by the proportion of individuals in a population having defective devices (alternatively, the probability that a device installed at a particular location will be defective) as a function of the time of operation of a safety scheme in which no age-replacement is practised. The main features of this relationship are the initial gradual increase of the quantity expressing deficiency in protection and the eventual attainment of a steady value of it. The rate of approach to the steady state and the final level of deficiency depend on the device-failure characteristics for both detected and undetected failures (cf. expression 4.8). Other measures of deficiency of protection, proportion of time ineffective, and mean period ineffective, behave in a similar manner. If age-replacement of devices is also practised, this will further complicate the dependence of the deficiency of a scheme on its time of operation. Obviously the probability of the occurrence of a catastrophe will also similarly depend on the time a scheme has been operating under these circumstances.

Precise analysis of the cost–benefit aspects of these time-dependent situations has not been achieved here because it has not proved possible to deduce analytical expressions for the appropriate relationships required to do this. Further work using computational optimization techniques in conjunction with Monte Carlo simulation is being pursued in an attempt to clarify these aspects of the operation of safety schemes. However, the Monte Carlo technique by itself provides a useful tool for assessing the consequences, in terms of degree of protection and device costs, of various device-failure characteristics (cf. Fig. 3), and it permits comparison of alternative replacement policies when a safety scheme is being planned.

7. Conclusions

Elementary probability theory has been used to derive expressions for quantities which measure the deficiency of a safety scheme in which devices only fail in an undetected manner, and in which the devices are replaced at regular intervals. These expressions have been used in an analysis of the cost-benefit aspects of this simple situation in terms of device-failure rate, rate of occurrence of hazards, device cost, replacement interval, and the penalty to be paid in the event of a catastrophe. Conditions under which such simple situations can be optimized in terms of cost and benefit have been deduced.

Consideration has also been given to situations in which safety devices are additionally subject to readily detectable modes of failure and are immediately replaced when they fail in this way. Some features of these situations have been derived from probability theory, but in general it has not been found possible to deduce analytical expressions for quantities relating directly to the deficiencies of safety schemes under these conditions. The Monte Carlo simulation technique has been used to provide estimates for such quantities, and thus to demonstrate that, in these circumstances, the protective capabilities of a safety scheme depend on its time of operation. The Monte Carlo technique does not itself allow precise analysis of the cost-benefit aspects of these time-dependent situations, but it provides a useful tool for assessing the effects of the failure characteristics of safety devices on both the deficiency in protection and the device costs of safety schemes, and for comparing alternative replacement policies for maintaining the effectiveness of such schemes.

Acknowledgements are due to my colleagues at SMRE who assisted in this work.

References

Abramowitz, M. & Stegun, A. I. 1964 *Handbook of mathematical functions.* U.S. National Bureau of Standards.

Barlow, R. E. & Proschan, F. 1962 *Planned replacement, studies in probability and management science*, Eds. Arrow, Karlin and Scarf. Stanford University Press.

Barlow, R. E., Hunter, L. C. & Proschan, F. 1963 *J. Soc. Indust. Appl. Maths.*, **11**, 1075–1095.

Barlow, R. E. & Proschan, F. 1965 *Mathematical theory of reliability.* New York: John Wiley.

Calabro, S. R. 1962 *Reliability principles and practices.* New York: McGraw-Hill Book Co.

Gnedenko, B. V., Belyayev, Yu. K. & Soloyev, A. D. 1969 *Mathematical methods of reliability theory.* New York: Academic Press.

Hammerlsey, J. M. & Handscomb, D. C. 1964 *Monte Carlo methods; Methuen monograph on applied probability and statistics.* London: Methuen.

Radner, R., Jorgenson, D. W. & McCall, J. J. 1967 *Optimal replacement policy.* Amsterdam: North-Holland Publishing Co.

Schreider, Yu. A. 1964 *Method of statistical testing—Monte Carlo method.* New York: Elsevier.

Appendix

Derivation of Expressions for $Q_0(t)$, $Q_1(t)$, and $Q_2(t)$

(a) $Q_0(t)$. Consider a system operating for a period t, during which time there are $n-1$ device-replacements, where replacements are made either because of detected failures or because of age-replacements. Let the intervals between successive replacements be denoted z_j, $j = 2, 3, \ldots, n-1$, further let z_1 be the time to the first replacement, and z_n be the interval between the last replacement and the end of the operating period, so that $\sum_{j=1}^{n} z_j = t$. For the negative exponential failure distribution, the probability of no undetected failure in each of these intervals is given by $\exp(-k_2 z_j)$, $j = 1, 2, \ldots, n$. Thus the probability of no undetected failure in the total period t is the product amongst all these probabilities for the successive intervals, viz.

$$Q_0(t) = \prod_{j=1}^{n} \exp(-k_2 z_j) = \exp\left(-k_2 \sum_{j=1}^{n} z_j\right) = \exp(-k_2 t) \tag{A1}$$

(b) $Q_1(t)$. A single transition of a system to its ineffective state in an operating time t, when no age-replacement is practised, may be represented as occurring in any one of the four possible ways described below.

(i) Only an undetected failure occurs in the operating period. The probability distribution function for this event being

$$q_a(t) = \begin{cases} (1-e^{-k_2 t})\, e^{-k_1 t}, & k_1 \neq k_2 \\ e^{-kt} - e^{-2kt}, & k_1 = k_2 = k. \end{cases} \tag{A2}$$

(ii) An unbroken succession of any number (>0) of detected failures occur followed by an undetected failure. The probability distribution function for this event may be written

$$\begin{aligned} q_b(t) &= k_1 \int_0^t e^{-k_2 u}\,(1-e^{-k_2(t-u)})\, e^{-k_1(t-u)}\, du \\ &= \begin{cases} (k_1/(k_1-k_2))(e^{-k_2 t} - e^{-k_1 t}) - e^{-k_2 t} + e^{-(k_1+k_2)t}, & k_1 \neq k_2 \\ kt\, e^{-kt} - e^{-kt} + e^{-2kt}, & k_1 = k_2 = k. \end{cases} \end{aligned} \tag{A3}$$

(iii) An undetected failure occurs followed by a succession of detected failures. This event has the same probability distribution function as the one given immediately above, i.e. $q_b(t) = q_c(t)$.

(iv) A succession of detected failures is followed by an undetected failure which is followed by another succession of detected failures. The probability distribution for this event may be written:

$$\begin{aligned} q_d(t) &= \int_0^t k_1\, e^{-k_2 u} \int_u^t (1-e^{-k_2(v-u)}) k_1\, e^{-k_1(v-u)}\, e^{-k_2(t-v)}\, dv\, du \\ &= \begin{cases} \dfrac{k_1^2(e^{-k_1 t} - e^{-k_2 t})}{(k_2-k_1)^2} - \dfrac{k_1 k_2 t\, e^{-k_2 t}}{(k_2-k_1)} + e^{-k_2 t} - e^{-(k_1+k_2)t}, & k_1 \neq k_2 \\ \dfrac{k^2 t^2\, e^{-kt}}{2} + e^{-kt} - kt\, e^{-kt} - e^{-2kt}, & k_1 = k_2 = k. \end{cases} \end{aligned} \tag{A4}$$

The probability distribution function $Q_1(t)$ is formed as the sum of the four distribution functions derived above giving the results shown in expressions (4.3a) and (4.3b).

(c) $Q_2(t)$. Two transitions of a system to its ineffective state in an operating time t when no age-replacement is practised may be represented as occurring in one of eight possible ways, which have more complicated structures but are constructed according to similar principles as those illustrated above for the ways of getting one transition to the ineffective state. Again the probability distribution function $Q_2(t)$ is formed as the sum of the probability distribution functions of these eight ways of getting two transitions to the ineffective state of the system, giving the results quoted in expressions (4.4a) and (4.4b).