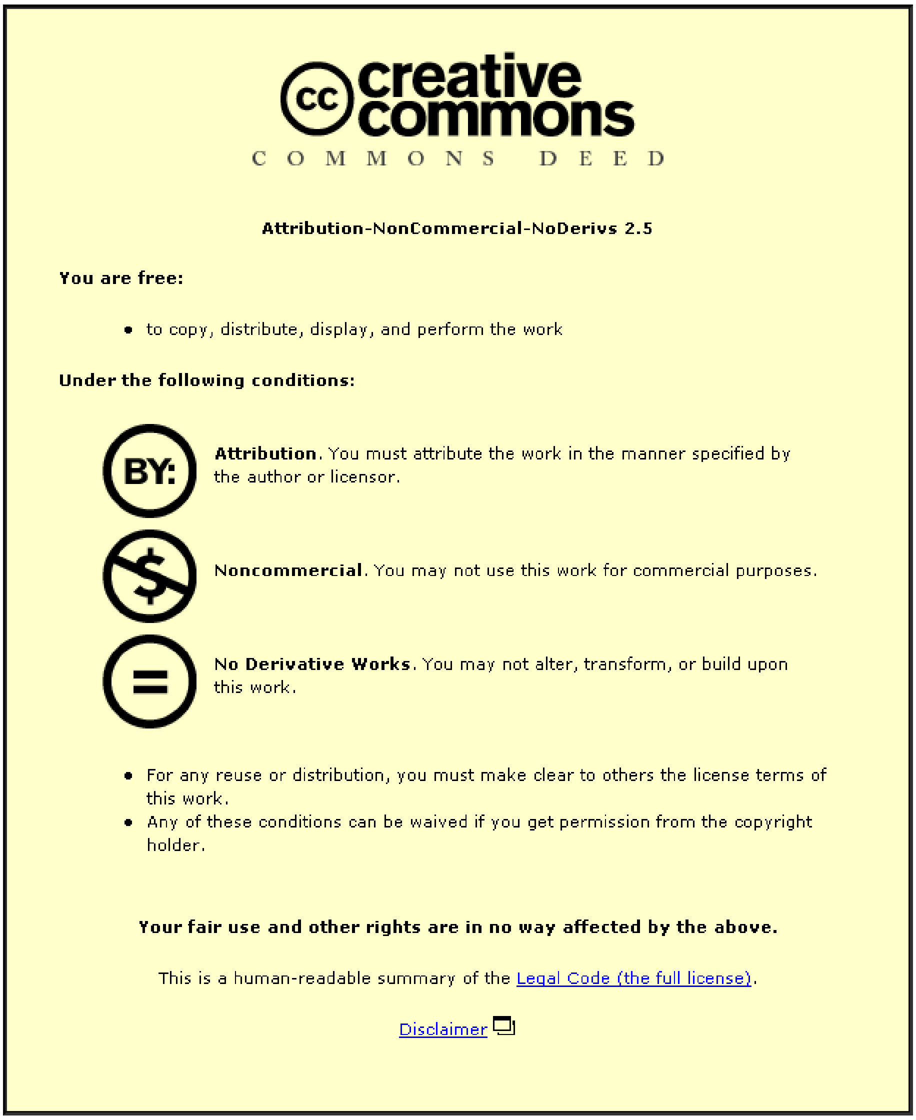

RELIABILITY OF 2–OUT–OF–N:G SYSTEMS WITH NHPP FAILURE FLOWS AND FIXED REPAIR TIMES

V M DWYER, R M GOODALL AND R DIXON

Department of Electronic and Electrical Engineering, Loughborough University,
Loughborough,LE11 3TU, UK
v,m,dwyer@lboro.ac.uk

Received (15th July 2009)

It is commonplace to replicate critical components in order to increase system lifetimes and reduce failure rates. The case of a general N–plexed system, whose failures are modelled as N identical, independent nonhomogeneous Poisson process (NHPP) flows, each with rocof (rate of occurrence of failure) equal to $\lambda(t)$, is considered here. Such situations may arise if either there is a time–dependent factor accelerating failures or if minimal repair maintenance is appropriate. We further assume that system logic for the redundant block is 2–out–of–N:G. Reliability measures are obtained as functions of τ which represents a fixed time after which Maintenance Teams must have replaced any failed component. Such measures are determined for small $\lambda(t)\tau$, which is the parameter range of most interest. The triplex version, which often occurs in practice, is treated in some detail where the system reliability is determined from the solution of a first order differential–delay equation (DDE). This is solved exactly in the case of constant $\lambda(t)$, but must be solved numerically in general. A general means of numerical solution for the triplex system is given, and an example case is solved for a rocof resembling a bath–tub curve.

Keywords: 2-out-of-n:G; NHPP; TMR; minimal repair.

1. Introduction

In safety critical situations such as the rail, aerospace and automotive[1–4] and medical and nuclear[5,6] industries it is quite common to replicate components important to the safety of a system in a redundant block. Such components are run in parallel so that a failure of one does not prevent the overall system from continuing to function correctly. Often the configuration of the block is triplex (three parallel units) or quadruplex (four parallel units). The well known Triple Modular Redundancy (TMR), which involves three parallel components together with a voting system, is a simple example of such systems. Complete system failure of a triplex configured system only occurs when all three components are simultaneously failed, however the system may be regarded as ‘unsafe’ with two failed components. In this case the remaining functioning component allows the system to be closed–down safely for a complete system repair, generally for which it will be taken out of service. This situation with two failed components corresponds to what might be called an operational failure rather than a (much more dangerous) full system failure and corresponds to 2–out–of–3:G logic. A variety of software control systems also work in a similar manner; for example HP's NonStop server[7] or the Space Shuttle's quad–redundant network[8], in which respectively three and four identical, independent boards perform the same calculations and at the end compare notes to see if any board is out of line with the rest. The aim of such redundancy is that faults may be identified and then isolated. HP's literature claims 99.99999% up–time for NonStop server running the TMR option[7]. Availability estimates such as these naturally require assumptions regarding the failure rates of the redundant components and the manner in which they are repaired.

As a simple example of what we are considering in this paper, suppose that a subsystem reliability block, consisting of three microcontrollers, is implementing a 2–out–of–3:G procedure[9] whilst being cooled by a fan. It is also supposed that the controllers are simple to replace (component repair) and if one fails, for whatever reason, it may be replaced within some small time period τ. It is assumed that the operation performed by the controllers is of sufficient importance that running the entire system with only one functioning microcontroller is thought to be too dangerous, so that the system would be shut down in such circumstances and undergo a complete repair (system repair). Thus, this particular mode of system failure will be deemed to have occurred when two of the three microcontrollers are failed simultaneously, leading to the 2–out–of–3:G logic. If the fan's function starts to degrade, so that its cooling effect on the controllers reduces, then the temperature of the controllers will increase and many of their failure modes will be accelerated. In some ways this is equivalent to what happens during a progressive accelerated life test (PALT), and we may describe component failures by a time–varying force of mortality on the controllers, according to some function $\lambda(t)$. To be clear, $\lambda(t)$ is defined such that the probability of each of the controllers failing in the (small) time interval $(t, t + dt)$, whether for the first time or not, given it is functioning at time t, is equal to $\lambda(t)dt + O(dt^2)$. Two further things are assumed here: the first is that such failures are assumed not to be *common cause failures*, they are accelerated by the same common mechanism (increasing temperature here), but the actual failures of the three controller remain quite independent, although the failures occur at an accelerated rate. In other words, $\lambda(T)$ is a function of the local temperature $T(t)$, and this temperature is varying with time. The second assumption is that the age of the controllers does not contribute to the time–varying mortality so in this regard the replaced components are neither necessarily as–good–as–new nor as–bad–as–old, but merely as–good–as–the–others. The distinction here being that a new replacement and a resuscitated old component act in the same manner as their force of mortality is determined by the fan, and not by their own age. Such a situation may arise if replacing the fan is not a realistic option, through being too costly or too involved a procedure. Component ageing may be neglected by implementing a preventative maintenance schedule that requires components to undergo an initial burn–in process off–line and also requires them to be replaced before they age significantly, a version of the standard *age replacement* preventative maintenance policy[9]. This ensures each component operates at the (assumed) flat bottom of their bathtub curve. As a maintenance policy this is not unreasonable, if the purpose of the redundant components is sufficiently important to the system that it is worth the cost of the policy's implementation.

The above example is obviously somewhat contrived, and perhaps a more realistic case would be that of the multiplexing of brake actuators on railway sets where a train's workload may act as the factor accelerating actuator failures. Likewise the failure modes of a variety of electrical systems may be accelerated by workload (for example current density accelerating Electromigration failures), mechanical stress, temperature or even by the weather (e.g. humidity)[10]. It is important to reiterate that the failures are *accelerated* (or perhaps even decelerated) by these changing conditions, still independent, but occurring at a rate which is changing in time. They are not *common cause events* which would imply that the probability of components failures are statistically dependent on one another.

A second case, which is covered by the same analysis, is that of a 2–out–of–3:G sub–system operating under a minimal repair maintenance policy[9], where the actuators (for example) are merely quickly patched up and put back into service. In this maintenance scheme components are repaired rather than being replaced. Their failure rate after repair is assumed to be the same as it was just before the failure. If the repair time is relatively small, then the failure rates of all components may be assumed to be equal. In this system the components are assumed to each fail according to an independent nonhomogeneous Poisson process (or NHPP), determined by the same parameter $\lambda(t)$. To be definite, by $\lambda(t)$ we mean the instantaneous rate of change of $M(t)$, the expected value $E(n(t))$ of the number $n(t)$ of failures of a given component in the time interval $(0, t]$, i.e. the failure rate of the *process*[11]. As simultaneous failures of a given component can be assumed not to occur, the probability of failure of a particular component in the time interval $(t, t + dt)$ is given by $\lambda(t)dt + O(dt^2)$, Ref. 11. In addition the process is assumed to be a regular one (continuous $M(t)$ and possessing independent increments, i.e. for any j, k, $\Pr\{n(t) = k | t \in A\}$ is independent of $\Pr\{n(t) = j | t \in B\}$ if $A \cap B = \varnothing$, see for example Ref. 12) so that $\lambda(t)$, the rate of occurrence of failure (rocof), is identical to the force of mortality of the first failure time[10]. Thus, if a component is working at time t, the probability of it working throughout the interval $[t, t+s)$, i.e. its conditional survival probability at time $t + s$, is

$$R_C(t+s\,|\,t) = \exp\left(-\int_t^{t+s}\lambda(u)du\right) = \frac{R_C(t+s)}{R_C(t)} \tag{1}$$

where $R_C(t)$ is the absolute reliability ($= R_C(t|0)$) of the component, assuming it was working at time $t = 0$. Eq. (1) will be used throughout (e.g. eqs. (12) – (15)), in general though it will be useful to condition on, for example, the time of the most recent component failure.

In a minimal repair policy the repair time is ignored[9] (i.e. the repairs are treated as Instantaneous and the process is a point one), however this idealisation is generally assumed to be valid if the repair time is sufficiently small. Strictly applied, our 2–out–of–3:G redundant system with minimal repair would fail with probability zero. Consequently to be realistic we assume here that the repair time τ is *small enough* that minimal repair remains roughly valid, and with it the use of three identical, independent NHPP failures flows, however we shall be interested in how the reliability measures for the system vary with this (small) repair time. This mild contradiction only arises in the minimal repair case and not in the accelerated failure case. So, when modelling minimal repair, it will be important to be precise in the statement of any results. The likelihood is though that, provided $\lambda(t)$ does not change appreciably on a timescale of τ (e.g. if $|\lambda(t+\tau) - \lambda(t)| << \lambda(t)$ or roughly $\tau\ |d\log(\lambda(t))/dt| << 1$), our results will give accurate results in both cases.

If safety of the system is paramount, and if the components are simple to replace, it will be useful for the Maintenance Engineers to work within some timeframe τ, which is the maximum allowed interval for component replacement from the time of failure. We assume, as a worst case, that all repairs take exactly the allowed time τ and ask the question: How do system reliability measures depend upon the (now deterministic) repair time τ? As well as being useful information for the defining of repair schemes, it is rather more realistic than assuming exponentially distributed repair time, yet avoids the need to specify a particular distribution. To summarize, our assumptions are that:

(1) the reliability of the triplex block is determined by three independent failure flows described by identical NHPP flows with rocof $\lambda(t)$. The time–dependence of the rocof could be either due to a time–dependent acceleration factor or due to component ageing in a minimal repair system;

(2) each component repair completes (as a worst case) exactly a time τ after the component failed. Note that the time τ includes the transportation time as well as the actual repair once an engineer is on site.

Assumption 2 needs some clarification and is assumed here to apply irrespective of the number of components in repair. For example in a 2–out –of–N:G system, in this worst case calculation, if two items are in repair, having failed at times t_1 and t_2 (where necessarily $t_1 \le t_2 \le t_1 + \tau$), a maintenance team is assumed to repair the first failed item at $t = t_1 + \tau$ and a second team repairs the second item at time $t = t_2 + \tau$. Such repairs may occur sooner, but as safety is presumed to be paramount this worst case is taken. This necessarily means that there are two maintenance teams available for the repairs of a quad system and N – 2 teams in the general N–plexed case. Using the language of Queuing Theory[13–15], the general N–redundant system is modelled by 2–out–of–N:G logic, with an M(t)/D/N–2 queue. In addition we assume:

(3) the system is completely observable, so that repairs begin immediately;

(4) repairs are conducted in–service provided that there are at least two functioning components. Should only one component be functioning the system is shut down and an operational system failure is said to have occurred.

A study of the time–to–first–(system) failure (TTF) is analytically equivalent to the case of a similar system without *system* repair. Consequently, it makes sense to discuss the first system failure in terms of a system hazard function $h_S(t)$, a TTFF failure distribution $f_S(t)$ and a ('non–repairable') reliability function $R_S(t)$. The time–to–second–failure of the system (and indeed all future failures) may be obtained from this, e.g. the reliability function for second failure, given the first occurred at $t = t_1$, is

$$R_S(t\,|\,t_1) = \frac{R_S(t)}{R_S(t_1)} = \exp\left(-\int_{t_1}^{t} h_S(u)du\right) \tag{2}$$

Consequently, our aim in this paper is to obtain the distribution of the time–to–first–failure of the system as a function of the allowed (component) repair time τ and in addition expressions for $R_S(t)$ and $h_S(t)$. As a special case we also consider the important case when the failures are described by homogeneous Poisson process (HPP), i.e. where the rocof is constant ($\lambda(t) = \lambda$). The mean TTFF (or MTTFF), equal to the mean time between failures (MTBF), is then also of particular interest. If we label the hazard function with HPP failures by $h_{S0}(\lambda,\tau)$, we wish also to compare the values of $h_S(t)$ and $h_{S0}(\lambda(t),\tau)$ (i.e. the HPP result with λ replaced by $\lambda(t)$, the rocof for the NHPP) as it has been suggested that, under certain conditions, including the small τ limit assumed here, they should be the same[16]. Specifically, the region of parameter space closest to what might be expected of a system in which safety is paramount, is that of small $\lambda(t)\tau$, i.e. fast repair. In the HPP case of $\lambda(t) = \lambda$ (say), then in the limit $\lambda\tau \to 0$, asymptotic reliability theory (see e.g. Refs. 16–21; in particular the review article Ref. 20) demonstrates, using renewal theory, that the TTFF distribution is asymptotically exponential with some system hazard rate $h_{S0} = h_{S0}(\lambda,\tau)$. In addition, Solov'yev and Zaytsev have studied[16] the k–redundant cold standby problem, with a non–stationary (NHPP) flows $\lambda(t)$, in a particular asymptotic limit. To avoid anomalous behaviour[†] they were forced to take the small $\lambda(t)\tau$ limit in the following rather unusual manner. Unable to take the general limit $\lambda(t)\tau \to 0$, they introduce a small parameter $\varepsilon \to 0$, and two fixed functions, $\lambda_0(t)$ and τ_0, independent of ε so that $\lambda_0(t)\tau_0 \sim O(1)$. They then consider the limit $\lambda(t) \to \infty$ as $\sim \lambda_0(t)/\varepsilon^k$ and $\tau \to 0$ as $\sim \tau_0\varepsilon^{k+1}$, so that $\lambda(t)\tau = \lambda_0(t)\tau_0\varepsilon \to 0$. In this case they show, for the k–redundant system (with a time varying $\lambda(t)$), that the failure rate at time t, may be

[†] In Ref [16] a partition of the interval [0, t) is first defined and the conditional system reliability is bounded in each of the resulting sub–divisions. This introduces a second limit, in addition to the limit $\varepsilon \to 0$, as the norm on the partition must also be allowed to approach zero. Difficulties arise with this method since it is necessary to swap the order of these limits, and the conditions imposed on $\lambda(t)$ and τ above are required in order to make this legitimate. Without such conditions, it is possible that when the $dt \to 0$ limit is taken the result may not be Riemann–integrable.

obtained from the instantaneous value of the exponent obtained from the stationary problem, i.e. from $h_S(t) = h_{S0}(\lambda(t),\tau)$. They conjecture that this may be a general result, but add that it will probably require additional conditions on $\lambda(t)$ (such as the condition here that $\lambda(t) = \lambda_0(t)/\varepsilon^k \rightarrow \infty$ in the $\varepsilon \rightarrow 0$ limit)[16].

2. The Triplex (2–out–of–3:G) System

Despite the NHPP flows, the system may be described by a state label k equal to the number of components in repair. The state transition diagram in the triplex case (i.e. 2–out–of– 3:G here) is shown in Fig. (1)[22]. At time t = 0 we assume the system has no failed items and is consequently in state k = 0. If at time t the system makes its first transition from state k = 1 to state k = 2 then it fails and the TTFF is t. As it is the distribution of TTFF that we seek here, there is no system repair from state k = 2 to k = 0. The analysis is more complicated that standard analysis based on Markov chains, as the state k = 1, which has a single component in repair, is a parameterised state with parameter x equal to the remaining repair time. As a result, the complete state of the system is described by k, and if k = 1, by the remaining repair time x also. Note that it is possible to unravel the k = 1 state, approximately, into a large number M (say) of states, denoted by the set $S_1 = \{(k = 1, x = m\tau/M)\}$ for $1 \le m \le M$. It is clear that the unravelled set of states $S = \{(k = 0)\} \cup S_1 \cup \{(k = 2)\}$ has the Markov property that for any set of strictly increasing times

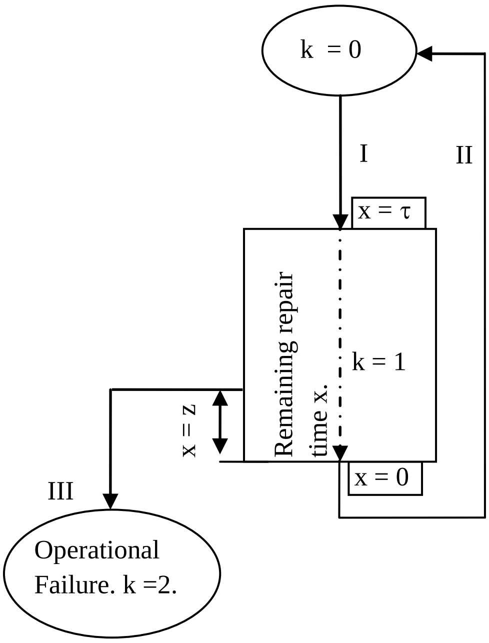

Fig. (1) The state transition diagram for the case of a constant failure rate. State k = 1 is a parameterized state indexed by x, the remaining repair time. After a failure x = τ; if no further failures occur, x will gradually be reduced to 0 and the system returned to state k = 0. A second failure will cause the system to fail, state k = 2.

t_j, $\Pr\{s(t_{j+1}) = s_{j+1}| s(t_j) = s_j, s(t_{j-1}) = s_{j-1}, \ldots, s(t_0) = s_0\} = \Pr(s(t_{j+1}) = s_{j+1}| s(t_j) = s_j\}$ for any $s_k \in S$. In the limit of large M, the mean value of the exponentially distributed sojourn times, in each state in S_1, $\sim \tau/M$, $\rightarrow 0$ and the states in S_1 all become instantaneous. We proceed slightly differently maintaining the continuous parameter x, however the probabilities $P_k(t)$, that the system is in state k at time t, remain the main interest. When k = 1 we also define a density function over $x \in [0, \tau]$, labelled $p_1(t,x)$, such that the probability that the system is in state k = 1 at time t, and has an item in repair with a remaining repair time in the range (x, x + dx), is given by $p_1(t,x)dx$. Then

$P_1(t)$ is the integral of $p_1(t,x)$ over all $x \in [0,\tau]$. If a single component in a fully functioning system fails at time t the system will enter the state k = 1 and will have an item with a remaining repair time of τ. Thus $p_1(t,\tau)dx$, the probability of being in state

k = 1 with an item with a remaining repair time in the range (τ – dx, τ), will be determined both by $P_0(t)$ and by the probability $3\lambda(t)dx$ that one of the three NHPPs generates a failure in the time interval (t, t + dx). Thus $p_1(t,\tau)dx = P_0(t) \times 3\lambda(t)dx$ or

$$p_1(t,\tau) = 3\lambda(t)P_0(t) \tag{3}$$

Likewise a system in state k = 1 at time t, which has an item with a remaining repair time in the region (0, dt), will make a transition to the state k = 0 within the time interval (t, t + dt) and this will tend to increase $P_0(t)$, thus

$$P_0(t+dt) = P_0(t)(1-3\lambda(t)dt) + p_1(t,0)dt \tag{4}$$

or

$$\frac{dP_0(t)}{dt} = -3\lambda(t)P_0(t) + p_1(t,0) \tag{5}$$

Similarly the probability of being in state k = 1 at t + dt, with an item in repair with a remaining repair time in the range (x – dt, x – dt + dx), is determined by the probability that it was in the state k = 1 at time t, with a remaining repair time in the range (x, x + dx), provided that a second component failure did not occur in the interval (t,t + dt). I.e.

$$p_1(t+dt, x-dt)dx = p_1(t,x)dx \times (1-2\lambda(t)dt) \tag{6}$$

or, from Taylor's theorem,

$$\frac{\partial p_1(t,x)}{\partial t} - \frac{\partial p_1(t,x)}{\partial x} = -2\lambda(t)p_1(t,x) \tag{7}$$

With no system repair from state k = 2, we have simply

$$P_2(t+dt) = P_2(t) + 2\lambda(t)dt\int_0^\tau p_1(t,x)dx \tag{8}$$

or

$$\frac{dP_2(t)}{dt} = 2\lambda(t)\int_0^\tau p_1(t,x)dx = 2\lambda(t)P_1(t) \tag{9}$$

Integrating eq. (7) over $0 \le x \le \tau$ and adding the result to eqs. (9) and (5), and using the result from eq. (3), demonstrates the conservation of probability, $P_0(t) + P_1(t) + P_2(t) = 1$.

For a general 2–out–of–N:G system, states k = 1, 2, …, N – 2 will be similarly parameterised (only with k parameters), while the states k = 0 and k = N – 1 will not. Generally the factor of three in eqs. (3) and (5) will be replaced by N, and a partial differential equation (pde) such as eq. (7) will be required for the parameterised states. In the triplex case here eq. (7) can be integrated along the characteristic $\xi = t - x$ (or merely by substitution of eq. (10) into eq. (7)) to give

$$p_1(t,x) = C(t+x-\tau)\exp\left(-\int_0^t 2\lambda(u)du\right) = C(t+x-\tau)R_C^2(t) \tag{10}$$

where eq. (1) has be used for $R_C(t)$. Note that as $p_1(t,x)$ is a continuous function of its arguments, eq. (10) implies that C(t) is also. It will now useful to define a function $Q(t) = C(t)/3\lambda(t)R_C(t)$. Then using eq. (3), $P_0(t) = Q(t)R^3{}_C(t)$, and in eq. (5), with $p_1(t,0) = 3\lambda(t - \tau)R_C(t-\tau)Q(t-\tau)R^2{}_C(t)$, we finally obtain

$$\frac{d}{dt}Q(t) = \frac{3\lambda(t-\tau)R_C(t-\tau)}{R_C(t)}Q(t-\tau) \tag{11}$$

Assuming that the initial system is in state k = 0 at t = 0, it is clear that Q(t) = 0 for t < 0, and Q(t) = 1 for all $0 \le t \le \tau$. Note that setting $\lambda(t) = 0$, $R_C(t) = 1$ and Q(t) = 0 for $-\tau \le t < 0$, Q(0) = 1 as the history for eq. (11) and integrating also gives this result and this latter will be the chosen as the start condition for the numerical integration discussed below. We wish to set up the system equations for a general 2–out–of–N:G system and it is with this in mind that the triplex system has been solved in the manner that it has. However there are other, simpler routes to eq. (11) which will help to justify the method. For example, as for this TTFF calculation, there are no in–service repairs from state k = 2, the system may only be in the state k = 1 at time t if it was in state k = 0 at time t_1 (such that $t_1 > t - \tau$), an item failed at that time and the other two devices survived from t_1 to t. I.e.

$$P_1(t) = \int_{t-\tau}^{t} 3\lambda(t_1)dt_1\frac{R_C^2(t)}{R_C^2(t_1)}P_0(t_1) = R^2(t)\int_{t-\tau}^{t}\frac{3\lambda(t_1)}{R_C^2(t_1)}P_0(t_1)dt_1 \tag{12}$$

which is essentially eq. (10) integrated over all x. Similarly the only way the system can be in state k = 0 at time t is if it has always been in state k = 0 or if it last returned from state k = 1 at time t_1 and has remained there ever since. If it returned from k =1 at time t_1, then it must have been in state k = 0 at time t_1–τ, at which point a failure occurred, the two remaining devices survived from t_1–τ to t_1, and finally the three good devices survived from t_1 to t, thus

$$P_0(t) = R_C^3(t) + R_C^3(t)\int_\tau^t P_0(t_1-\tau)\frac{3\lambda(t_1-\tau)}{R_C^2(t_1-\tau)R_C(t_1)}dt_1 \tag{13}$$

Consequently, changing variables in the integral,

$$\frac{P_0(t)}{R_C^3(t)} = 1 + \int_0^{t-\tau}\frac{P_0(t_1)}{R_C^3(t_1)}\frac{3\lambda(t_1)R_C(t_1)}{R_C(t_1+\tau)}dt_1 \tag{14}$$

Differentiating eq. (14) then gives eq. (11).

Eq. (11) is a differential–delay equation or a differential–difference equation (DDE). Such equations have been studied in the Number Theoretical context of sieve methods as a means of eliminating primes, e.g. Ref. 23. There are very few analytical, and no simple, solutions to such equations. In principle they may be solved using Bellman's Method of Steps[24]. This solves eq. (11) for Q(t) on the time interval t ∈ (nτ, (n+1)τ] using, on the right–hand–side, values from the interval t ∈ ((n–1)τ, nτ]. Thus, for example, integrating eq. (11) with Q(0) = 1 and Q(t < 0) = 0, gives Q(t) = 1 on t ∈ (0, τ], and integrating again

$$Q(t) = 1 + 3\int_0^{t-\tau}\frac{\lambda(t')R(t')}{R(t'+\tau)}dt' \tag{15}$$

on t ∈ (τ, 2τ]. The Method of Steps demonstrates that a solution to eq. (11) exists, and, with the continuity of C(t) and hence of Q(t), that that solution is also unique. However the need for repeated integration makes it difficult to generate a solution with this method except in the very simplest of cases, unless either the repair time τ is large compared to typical values of 1/λ(t), or t is of the order of a few τ. Neither condition is likely to be of interest here; and in addition a solution valid for long times is important. We have assumed in the above description of the system that the rocof λ(t) is not state–dependent, i.e. one failed item does not alter the rocof of the others. This is not strictly necessary, and different values of λ(t) may easily be introduced into eqs. (5) and (7).

In systems in which safety is important it is expected that the allowed repair time will be small compared to typical values of 1/λ(t). First order DDEs with constant coefficients (i.e. , eq. (11) with λ(t) constant) have been considered by Driver et al.[25], with a small delay time τ. They find that for certain conditions on these constant coefficients, corresponding here to the value of $\theta \equiv 3\lambda\tau\exp(\lambda\tau) < \exp(1)$, the asymptotic behaviour of the solution of an equation such as eq. (11) is the same as that obtained by taking the first Taylor approximation

$$C(t-\tau) \approx C(t) - \tau \frac{dC(t)}{dt} \tag{16}$$

It is well known (e.g. Ref. 26) that such approximations are not generally valid, and certainly any hopeful attempt at increasing the accuracy of the solution, for larger τ values, by using higher order Taylor series, may fail through the introduction of oscillatory behaviour. However it is certainly worthwhile considering a similar approximation here, when eq. (11) in terms of C(t) reduces to the ordinary differential equation (ODE),

$$\frac{dC}{dt} \approx \frac{\lambda(t)}{(1+3\lambda(t)\tau)}\left[2 - \frac{d}{dt}\left(\frac{1}{\lambda(t)}\right)\right]C(t) \tag{17}$$

This may be integrated without any further approximation to give

$$\log C(t) = \log(c) + \int_0^t \frac{2\lambda(t)}{(1+3\lambda(t)\tau)}dt + \log\left(\frac{3\lambda(t)\tau}{1+3\lambda(t)\tau}\right) \tag{18}$$

If we use the normalisation constraint that $f_S(t)$ should integrate to one, rather than say the behaviour at t = 0 to determine the integration constant, a simple analysis shows that c = $1/\tau$. In this case the cumulative distribution function $F_S(t)$ and the reliability $R_S(t)$ are then

$$R_S(t) = 1 - F_S(t) \approx \exp\left(-\int_0^t \frac{6\lambda(t)^2\tau}{1+3\lambda(t)\tau}dt'\right) \tag{19}$$

2.1. *Constant λ*

If the rocof is constant, i.e. the failure flows are generated by HPPs, an exact solution to eq. (11) may be obtained, although the notation is simplified by introducing the dimensionless parameter $\theta = 3\lambda\tau\exp(\lambda\tau)$, then with $R_C(t) = \exp(-\lambda t)$, eq. (11) becomes

$$\tau\frac{d}{dt}Q(t) = \theta Q(t-\tau) \tag{20}$$

If the initial state is k = 0, the initial data is Q(0) = 1 and Q(t) = 0 for $-\tau \le t < 0$, as above. Then the Laplace Transform $\tilde{Q}(s)$ of Q(t) is

$$\tilde{Q}(s) = \frac{1}{s - \theta\exp(-s\tau)/\tau} \tag{21}$$

The zeros of the denominator are determined by the Lambert W–function[27], defined such that w = W(z) if $w\exp(w) = z$. The poles of $\tilde{Q}(s)$ occur at $s = s_m = W_m(\theta)/\tau$, where m is the branch index of the Lambert function. The residue values are obtained in the usual manner to be $(1 + s_m\tau)^{-1}$. Note as θ is real, properties of W(x) ensure that s_m and s_{-m} are complex conjugates[27]. Consequently, from eq. (21) the failure time pdf is

$$f_S(t)=\frac{2\lambda(3\lambda-s_0)\tau\exp((s_0-3\lambda)t)}{(1+s_0\tau)(s_0\tau-\lambda\tau)}+4\lambda\,\mathrm{Re}\left(\sum_{m=1}^{\infty}\frac{(3\lambda-s_m)\tau\exp((s_m-3\lambda)t)}{(1+s_m\tau)(s_m\tau-\lambda\tau)}\right) \qquad (22)$$

for t > 0. The t = 0 value of the infinite series in eq. (22) must be understood to represent the limit $t \to 0+$; the sum of the series for Q(t) obtained by setting t = 0 before performing the sum will give an erroneous value of ½ rather than 1. The expression in eq. (22) is dominated by the first term corresponding to m = 0. The 'exact' distribution (including terms in the sum up to m = 400) is shown as the solid curve in Fig. (2), for $\lambda\tau = 0.1$. Also shown in the same figure is the dominant (m = 0) term (dotted curve) and only those terms in eq. (22) corresponding to m = 0, 1 (dashed curve). It is clear from Fig.(2) that, to capture the behaviour for t close to 0, requires a large number of terms from the sum, but only a small number (one or perhaps two terms) is enough for the majority of the time. It is this behaviour, that dictated the manner in which c was chosen in eq. (18).

Examining the pole behaviour as $\lambda\tau$ is decreased demonstrates that the real pole closest to 3λ dominates the failure time distribution, Fig. (3). In the case of *fast repair*, i.e. small $\lambda\tau$, the dominant pole ($s_0\tau = W_0(3\lambda\tau\exp(\lambda\tau))$) comes from the m = 0 branch, where, for small z, $W_0(z) \sim z - z^2 + 3z^3/2$. Thus $s_0\tau \sim 3\lambda\tau - 6\lambda^2\tau^2 + 24\lambda^3\tau^3$, which leads to a dominant term in eq. (22) of $6\lambda^2\tau(1 - 4\lambda\tau)\exp(-6\lambda^2\tau(1 - 4\lambda\tau)t)$. This analysis is also consistent with work on fast repair in reliability problems which predicts that, in the limit of small repair times, the failure time distribution should be asymptotically exponential[16–21]. The value of 1/MTTFF in this case is clearly $6\lambda^2\tau(1 - 4\lambda\tau)$ in the small $\lambda\tau$ limit. We

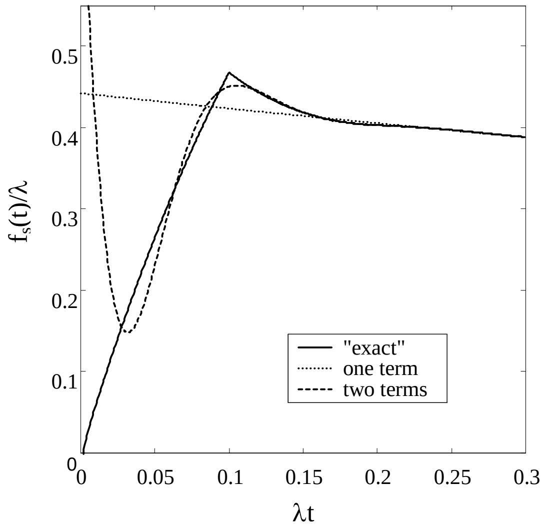

Fig. (2). The system failure distribution for $\lambda\tau = 0.1$. The solid curve is essentially the exact result (up to the m = 400 terms), the dashed curve consists of only the terms corresponding to m = 0 and m = 1 in eq. (22), and the dotted curve is only the dominant exponential term (m = 0).

may check this as moments of the distribution (MTTFF, etc.), may be obtained from the Laplace Transform of $f_S(t)$ which, from eq. (21) and the definition of Q(t), is

$$\tilde{f}_S(s) = 6\lambda^2 \frac{\tilde{Q}(s+3\lambda)}{s+2\lambda}(1-\exp(-(s+2\lambda)\tau)) \tag{23}$$

Thus the MTTFF is given (exactly, and also to O(τ) approximation) by

$$\text{MTTFF}= -\left.\frac{d\tilde{f}_S(s)}{ds}\right|_{s=0} = \frac{1}{2\lambda} + \frac{1}{3\lambda\left(1-\exp(-2\lambda\tau)\right)} = \frac{1+4\lambda\tau}{6\lambda^2\tau} + O(\tau) \tag{24}$$

As to $O(\lambda\tau)$, $(1 - 4\lambda\tau) \sim (1 + 4\lambda\tau)^{-1}$ this agrees with the MTTF discussed above, see also for example Ref. 18. Values of λMTTFF values for $\lambda\tau = 0.1$, are shown Fig.(4).

2.2. *Nonhomogeneous Poisson Process NHPP*

For the non-stationary process eq. (11) must be solved with time–varying $R_C(t)$ and $\lambda(t)$. A familiar step in reliability analysis might be to consider, say, the case of a Weibull distribution as a source of the time–varying rocof, essentially choosing $R_C(t)$ for its simplicity, and to solve for $f_S(t)$ in that case. However, in view of the sophistication of the analysis, it is perhaps more expedient to progress in a slightly different way. Define first the intermediate function

$$\theta(t) = \frac{3\lambda(t-\tau)\tau R_C(t-\tau)}{R_C(t)} \tag{25}$$

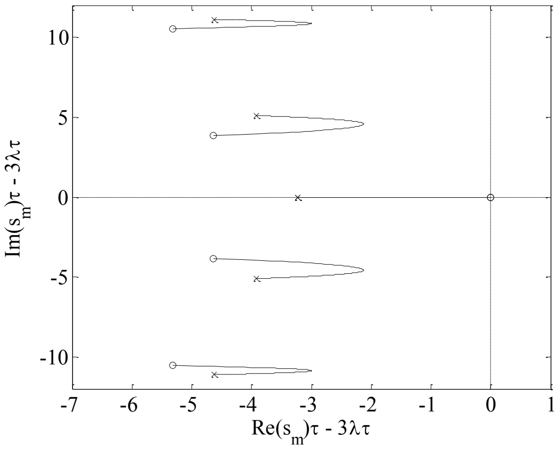

Fig. (3). Poles structure of $\tilde{Q}(s)$ for $0.02 \le \lambda\tau \le 2$. The marker 'o' corresponds to $\lambda\tau = 2$, while 'x' corresponds to $\lambda\tau = 0.02$.

This is in line with the value of θ define earlier for the HPP case. With eq. (25), eq. (11) may now be written in terms of θ(t) as the pair

$$\begin{aligned} &\text{(i)} \qquad 3\tau\frac{dR_C(t)}{dt} = -\theta(t+\tau)R_C(t+\tau) \\ &\text{(ii)} \qquad \tau\frac{dQ(t)}{dt} = \theta(t)Q(t-\tau) \end{aligned} \tag{26}$$

The equation in $R_C(t)$ is an advanced–DDE while that in Q(t) is a retarded–DDE. The pair, eqs. (26), come from adjoint classes, and have been analysed[28–32] (in pairs) for a variety of functions θ(t). The background to this work is again that of the Number Theoretical analysis of prime numbers in which the DDEs developed relate to sieve methods.

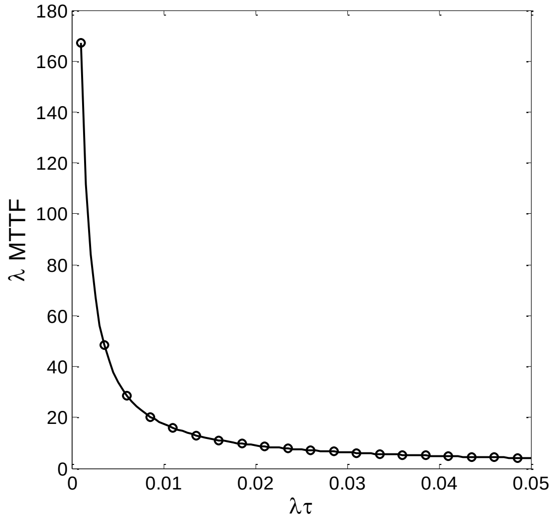

Fig. (4). λMTTFF for exponential failures. The solid curve represents the exact expression, eq. (24) while the circles represent the single exponential approximation from eq. (22).

If, instead of $R_C(t)$ or λ(t), it is θ(t) that is now chosen for expedience, so that eqs. (31) are most easily solved, the adjoint nature of eqs. (26i) and (26ii) allows the single component reliability function $R_C(t)$, that gives rise to that θ(t), (and through that λ(t)) to be solved at the same time as Q(t). However analytical solutions to eqs. (26) only exist in a small number of special cases[28–32]. Bradley and others[29–32] have considered the case

$$\theta(t) = \frac{b}{t+a} \tag{27}$$

which corresponds to a rocof λ(t) decreasing with time roughly as b/(t + a + b), while de Bruijn has analysed[28] the case $\theta(t) = \exp(\alpha t + \beta)$ which gives rise to a roughly linearly increasing λ(t). The complexity of the analysis in each case (respectively Refs 29–32, and Ref. 28) demonstrates clearly that finding analytical solutions to even the most trivial differential-difference equations (DDEs) is extremely difficult. In addition, the form of the solutions obtained is not simple. As a result numerical techniques offer the best options. Such problems can also be difficult to solve numerically, however Shampine[33,34] has developed a MATLAB programme (ddesd) devoted to the solution of DDEs. Shampine's programme uses standard Runge–Kutta methods and proceeds in time–steps controlled by the current estimate of the size of the residual error.

Eq. (11) may be written in terms of C(t) and $f_S(t)$ as the matrix equation

$$\tau\frac{d\underline{\Phi}(t)}{dt}=\begin{pmatrix}\frac{\dot{\lambda}(t)\tau}{\lambda(t)}-\lambda(t)\tau & 0\\ 2\lambda(t)\tau R^2(t) & \frac{\dot{\lambda}(t)}{\lambda(t)}\tau-2\lambda(t)\tau\end{pmatrix}\underline{\Phi}(t)+\begin{pmatrix}3\lambda(t)\tau & 0\\ -2\lambda(t)\tau R^2(t) & 0\end{pmatrix}\underline{\Phi}(t-\tau) \quad (28)$$

where $\underline{\Phi}(t) = [C(t)\tau, \tau f_S(t)]^T$. This must be solved with the initial history condition of $\underline{\Phi}(t) = [0, 0]$ for $-\tau \le t < 0$ and $\underline{\Phi}(0) = [3\lambda(0)\tau, 0]$. For the case of HPPs there is no distinguishable difference between the solution from the DDE solver and from eq. (22). For a perhaps more realistic example we give the numerical solution for a bath–tub like rocof, defined by

$$\lambda(t)\tau=\begin{cases}\dfrac{175}{104(3t/\tau+25)} & 0\le t\le 25\tau\\ 7/416 & 125\tau\le t\le 200\tau\\ \dfrac{7}{416}\dfrac{t/\tau}{200} & 200\tau\le t\end{cases} \quad (29)$$

which is shown, together with the associated single component reliability $R_C(t)$, in Fig. (5). The repair time τ is nominally 7 days and at the bottom of the bath–tub curve the rocof is 1/416 days^{-1}, values consistent with the active suspension example introduced in ref [22]. The code required to run the MATLAB function `ddesd` is

```
opts = ddeset('AbsTol',10^-7,'RelTol',10^-6);
sol = ddesd(@ddeeqn,@delay',@history,[0, 800],opts);
t = sol.x*tau;fs=sol.y(2,:)/tau;
```

A function `history` is required to set up the value of $\underline{\Phi}(t)$ in the range $-\tau < t \le 0$;

```
function ph=history(u);
ph=[0;0];
if u == 0,
   ph=[3*lambda(0)*tau;0];
end;
```

while the function `delay` describes the delays in eq. (28) in units of τ,

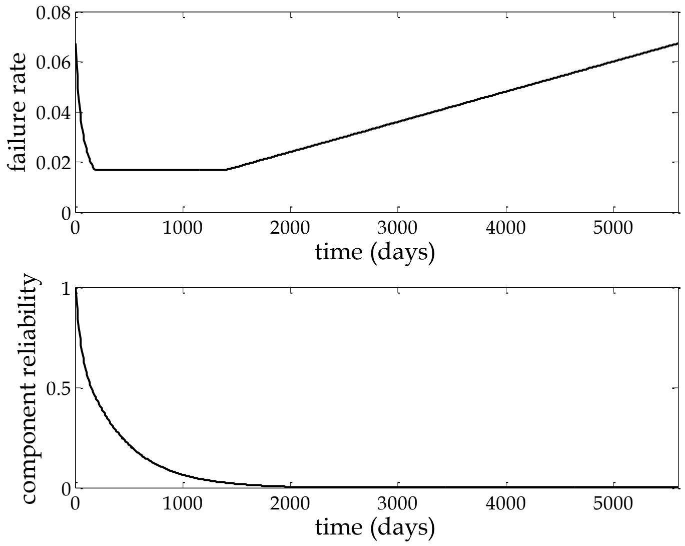

Fig. (5). Single component failure rate λ(t) given in eq. (29), and the appropriate single component reliability function $R_C(t)$.

```
function d = delay(u,y);
d=u-1;
```

Finally a function (here labelled ddeeqn) is required so that the dde algorithm may determine the value of $\dot{\underline{\Phi}}(t)$ (i.e. dphdt) as a function of time, given the current values of t, $\Phi(t)$ and $\Phi(t-\tau)$ (or uτ, ph and ph_1), from the DDE, eq. (28). Thus

```
function dphdt=ddeeqn(u,ph,ph_1);
dphdt=[0; 0];
lam=lambda(u);LT=lam*tau;LT_dot=lamdba_dot(u)*tau;R=RC(u);
dphdt(1)=(lT_dot/lam-lamT)*ph(1)+ 3*lamT*ph_1(1);
dphdt(2)=2*LT*(R^2)*(ph(1)-ph_1(1))+(LT_dot/lam-2*LT)*ph(2);
```

All that is required are functions (lambda(u) and lambda_dot(u)) defining the rocof λ(t) and its derivative and the single component reliability RC(u) defining $R_C(t)$. Fig. (6) shows the TTFF distribution obtained from the DDE solver. It turns out that the quadruplexed system is much more complex than this due to the M(t)/D/2 queuing and results for that case will be considered elsewhere. For now we turn our attention to obtaining approximate results for the general 2–out–of–N:G case for NHPP flows for the small λ(t)τ, for which we shall regard the N = 3 case as a specific example.

3. The General 2–out–of–N:G case with NHPP flows.

In the 2–out–of–N:G system, the system is again described by the state probabilities $P_k(t)$ that there are k items in repair at time t. We denote, for each state $k \neq 0$, N–1, the vector of ordered remaining component repair times by $\underline{x}^{(k)} = [x_1, x_2, \ldots, x_k]$, where $\underline{x}^{(k)} \in X_k \equiv \{\underline{x}^{(k)} \,|\, 0 \le x_1 \le x_2 \le \ldots x_{k-1} \le x_k \le \tau\}$, and define the density functions $p_k(t \,|\, \underline{x}^{(k)})$, such that the probability the system has k items in repair, with an associated

emaining repair time vector in the range $(\underline{x}^{(k)}, \underline{x}^{(k)} + d\underline{x}^{(k)})$, is $p_k(t \,|\, \underline{x}^{(k)}) d\underline{x}^{(k)}$. In this way the item with remaining repair time x_1 is the item which will be returned to service first while that with x_k will be last. The probability that the system is in state k, $P_k(t)$, is then the integral of $p_k(t \,|\, \underline{x}^{(k)}) d\underline{x}^{(k)}$ over its ordered set X_k. Whilst it is perhaps more natural to index the pdf for (say) state k = 1 by the time of the most recent failure t_1 rather than by $x_1 = \tau + t_1 - t$, the latter is chosen as the remaining repair times x_1 are defined on the finite range $[0, \tau]$ and, for small τ, expansions in x_1 are simpler than in $t - t_1$. This is in fact more important in the quadruplex case considered elsewhere [35].

In terms of these probabilities and density functions, the system state–equations are

$$\begin{aligned}
&\text{(i)}\frac{dP_0(t)}{dt} = p_1(t\,|\,0) - N\lambda(t)P_0(t) \\
&\text{(ii)}\frac{\partial p_k(t\,|\,\underline{x}^{(k)})}{\partial t} - \sum_{i=1}^{k}\frac{\partial p_k(t\,|\,\underline{x}^{(k)})}{\partial x_i} = -(N-k)\lambda(t)p_k(t\,|\,\underline{x}^{(k)}) + p_{k+1}(t\,|\,0,\underline{x}^{(k)}) \quad 1 \le k \le N-3 \\
&\text{(iii)}\frac{\partial p_{N-2}(t\,|\,\underline{x}^{(N-2)})}{\partial t} - \sum_{i=1}^{N-2}\frac{\partial p_{N-2}(t\,|\,\underline{x}^{(N-2)})}{\partial x_i} = -2\lambda(t)p_{N-2}(t\,|\,\underline{x}^{(N-2)}) \\
&\text{(iv)}\frac{dP_{N-1}(t)}{dt} = 2\lambda(t)P_{N-2}(t)
\end{aligned} \tag{30}$$

Eq. (30i) describes the transitions out of state k = 0 and may be derived in a manner similar to eq. (5); (30ii) describes the balance in state k ($1 \le k \le$ N–3); (30iii) refers to state k = N – 2 (different from eq. (30ii) as there is no transition out of the failed state k = N–1) and may be derived in a similar manner to eq. (7); finally (30iv) describes transitions into the failed state, k = N–1 and plays the role eq. (9) plays for the triplex case. The continuity conditions at the states boundaries are

$$\begin{aligned}
&p_1(t\,|\,\tau) = N\lambda(t)P_0(t) \\
&p_{k+1}(t\,|\,\underline{x}^{(k)},\tau) = (N-k)\lambda(t)p_k(t\,|\,\underline{x}^{(k)}) \quad 1 \le k \le N-3
\end{aligned} \tag{31}$$

The first of these plays the role of eq. (3) in the triplex case. The second performs the same task at the other state boundaries. Eqs. (31) ensure that the system correctly enters state k + 1 correctly when a failure occurs in state k. The system reliability $R_S(t)$, MTTFF and failure time distribution $f_S(t)$ are given by, respectively,

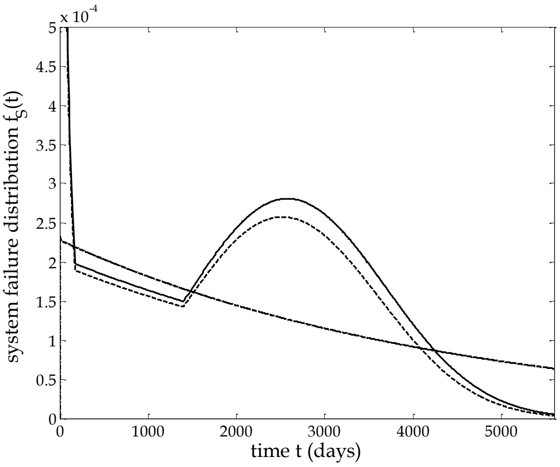

Fig. (6). Comparison of the DDE solution, using the MATLAB ddesd routine[33,34], and the small repair–time approximate solution (eq. (41) with N = 3) for the failure distribution of a 2–out–of–3:G system, each of whose components have the bath–tub type failure–rate given in eq. (29). The numerical solution is represented by the solid line while the dotted curve corresponds to eq. (41). Also shown for comparison is the system failure distribution assuming a constant failure rate equal to that at the bottom of the bath–tub curve (dash–dotted line).

$$\text{(i)}\ R_S(t)=\sum_{k=0}^{N-2}P_k(t)=1-P_{N-1}(t)$$

$$\text{(ii) MTTFF}=\int_0^\infty R_S(t)dt \tag{32}$$

$$\text{(iii)} f_S(t)=2\lambda(t)P_{N-2}(t)=2\lambda(t)\int_{\underline{x}_{N-2}} p_{N-2}(t\,|\,\underline{x}_{N-2})d\underline{x}_{N-2}$$

as $f_S(t)=-\dot{R}_S(t)$.

Generally for a 2–out–of–N:G system, with a fast replacement facility, i.e. small repair time τ, it will be admissible to expand $p_{N-2}(t\,|\,\underline{x}^{(N-2)})$, as a Taylor series around $p_{N-2}(t\,|\,\underline{\tau}^{(N-2)})$. This yields, for $0 \le x_k \le \tau$,

$$p_{N-2}(t\,|\,\underline{x}^{(N-2)})=p_{N-2}(t\,|\,\underline{\tau}^{(N-2)})-\sum_{k=1}^{N-2}(\tau-x_k)\frac{\partial p_{N-2}(t\,|\,\underline{\tau}^{(N-2)})}{\partial x_k}+O(\tau^2) \tag{33}$$

so that, integrating over the ordered set X_{N-2},

$$\begin{aligned}P_{N-2}(t)=\lambda(t)^{N-3}\frac{\tau^{N-2}(N-1)}{2}\left(1-\frac{2\lambda(t)\tau}{N-1}\right)p_1(t\,|\,\tau)-\frac{(N-2)\tau^{N-1}}{2}\frac{\partial[p_1(t\,|\,\tau)]}{\partial t}\lambda(t)^{N-3}\\ -p_1(t\,|\,\tau)\lambda(t)^{N-4}\frac{\tau^{N-1}}{4}\frac{d\lambda(t)}{dt}(N-3)(N-2)+O(\tau^N)\end{aligned} \tag{34}$$

In changing from derivatives with respect to x_k, to those with respect to t, we have used eqs. (30ii). This introduces, in the summation, terms in $\dot{p}_k(t\,|\,\underline{\tau}^{(k)})$ plus a term in (N – k) $(p_k(t|\underline{\tau}^k) - p_k(t|0,\underline{\tau}^{k-1}))$. This latter term is of $O(\lambda(t)\tau)$ compared to the former and at this level of approximation may be ignored. We have also used repeatedly, from eqs. (31),

$$p_{N-2}(t\,|\,\underline{\tau}^{(N-2)}) = \frac{(N-1)!}{2}\lambda(t)^{N-3}p_1(t\,|\,\tau) = \lambda(t)^{N-m-2}\,\frac{(N-m)!}{2}p_m(t\,|\,\underline{\tau}^{(m)}) \qquad (35)$$

Clearly from eqs. (31i), (34) and (35), $P_k(t) \sim O(\lambda(t)^k\tau^k)$ and as a consequence the reliability may also be approximated from eq. (32i) as

$$R_S(t) \approx P_0(t) + P_1(t) = \frac{1+N\lambda(t)\tau}{N\lambda(t)}p_1(t\,|\,\tau) + O(\lambda(t)^2\tau^2) \qquad (36)$$

Notice also that, from eqs. (32iii), (34) and (36), the leading term in the time derivative of $\log(R_S(t))$ is $-N(N\text{-}1)\lambda(t)^{N-1}\tau^{N-2}$ and thus, from eq. (36),

$$\frac{d}{dt}\log p_1(t\,|\,\tau) = \frac{d}{dt}\log\lambda(t) + O(\lambda(t)\tau) \qquad (37)$$

Combining eqs. (32iii), (34), (36) and (37)

$$\begin{aligned} \frac{d\log R_S(t)}{dt} &= -\frac{f_S(t)/p_1(t\,|\,\tau)}{R_S(t)/p_1(t\,|\,\tau)} \\ &= -\frac{2\lambda(t)\binom{N}{2}(\lambda(t)\tau)^{N-2}\left(1-\dfrac{2\lambda(t)\tau}{N-1}\right)+3\binom{N}{3}(\lambda(t)\tau)^{N-1}\dfrac{d\log\lambda(t)}{dt}^{N-1}+O(\tau^N)}{1+N\lambda(t)\tau} \end{aligned} \qquad (38)$$

Integrating this then gives

$$R_S(t) = (1+O(\lambda(t)^2\tau^2))\exp\left(-N(N-1)\tau^{N-2}\int_0^t \frac{\lambda(u)^{N-1}\left(1-\dfrac{2\lambda(u)\tau}{N-1}\right)}{1+N\lambda(u)\tau}du\right) \qquad (39)$$

The first factor in eq. (39) represents the fact that eq. (36) is only accurate to $O(\lambda(t)\tau)$ and also absorbs the second term in eq. (38). It is clearly possible to ignore this factor when t/MTTFF is significantly greater than around $\lambda(t)\tau$. In this case the system may be described by an instantaneous hazard rate of

$$h_S(t) \approx N(N-1)\lambda(t)\frac{\lambda(t)^{N-2}\tau^{N-2}\left(1-\dfrac{2\lambda(t)\tau}{N-1}\right)}{1+N\lambda(t)\tau} \qquad (40)$$

The analysis presented so far is in line with that of Solov'yev and Zaytsev who suggested[16] that, for systems with sufficiently small repair times τ, if the system reliability $R_S(t)$ behaves as $\exp(-h_{S0}(\lambda,\tau)t)$ for constant λ (i. e. MTTFF = $1/h_{S0}(\lambda,\tau)$ as in eq. (12)) then it can be expected that, for time varying $\lambda(t)$, $R_S(t)$

$\sim \exp\left(-\int_0^t h_{S0}(\lambda(u),\tau)du\right)$ as in eq. (10). The hazard function $h_{S0}(\lambda,\tau)$ is a function of λ and τ appropriate to the particular problem under consideration. Here, as opposed to Ref. 16, however, it is clear that that the requirement is only for $\lambda(t)\tau$ to be small.

Compared with triplex, eq. (39) with $\lambda(t)$ constant agrees with eqn (24) to $O(\lambda^2\tau^2)$, and represents a slightly more accurate result than that of eq. (19). It may in fact be derived by retaining the second order term in $\tau^2\ddot{C}(t)/2$ in eq. (16). We should note that it has been assumed here that the Taylor series for $C(t - \tau)$ can be truncated after the first two terms. This requires a relatively slowly changing function $C(t)$ over intervals of length τ. Indeed $\tau\dot{C}(t)$ is only small compared to $C(t)$, from eq. (17), with small $\lambda(t)\tau$, provided that $\dot{\lambda}(t)/\lambda^2(t) \sim O(1)$. Thus, the method of Diver[25] is expected to fail for failure rates which change too rapidly. The DDE solution for the triplex TTFF distribution is compared with the approximate solution obtained above, eqs. (39) and (40), in Fig.(6). Also shown is the exponential distribution with a constant rocof equal to the value of $\lambda(t)$ at the bottom of the bath–tub curve. The solutions are indistinguishable for this case as $\lambda(t)\tau$ is small, so that eqs. (39) and (40) are likely to represent a very good approximation for most realistic safety–critical (small $\lambda(t)\tau$) systems. For larger $\lambda(t)\tau$ the DDE solver is recommended.

For HPP flows in a 2–out–of–N:G system (N-plex redundancy), with small $\lambda\tau$, $\lambda \mathrm{MTTFF}_N$ is then given by the asymptotic expression

$$\lambda \mathrm{MTTFF}_N = \frac{1}{N(N-1)\lambda^{N-2}\tau^{N-2}} + \frac{1+2/(N(N-1))}{(N-1)\lambda^{N-3}\tau^{N-3}} + O\left(\frac{1}{\lambda^{N-4}\tau^{N-4}}\right) \qquad (41)$$

Consequently, for small $\lambda\tau$, increasing the level of redundancy from N–plex to (N+1)–plex improves the MTTFF by a factor of around $(N-1)/(N+1)\lambda\tau \rightarrow (\lambda\tau)^{-1}$ for large N. Using eq. (41) it is possible, for example, to choose the level of redundancy in the active suspension unit to give an MTTFF for that system which will not interfere with the running operation of the parent railway vehicle. Alternatively using eq. (40) one can choose N to ensure that the overall hazard rate is kept within some acceptable value. Thus if λ = 1/416 days^{-1}, τ = 7 days and if it is required that MTTFF is 500,000 h as in Ref. 22, a triplex system (N = 3) will give an MTTFF of around 99,000 h while a quadruplex system (N=4) will give an MTTFF of around 2,900,000 h. Clearly only a quadruplex system will provide the required reliability.

4. Conclusions

We have considered the failure of general 2–out–of–N:G systems, with component failures determined by a time–dependent rocof $\lambda(t)$. The problem definition reflects two possible cases. The analysis corresponds to either the case that an environmental variable causes a common time–dependent acceleration of the single–component rocof, or the components age with rocof λ(t) but undergo a fast, minimal repair. There is a requirement that Maintenance Engineers complete replacements within some maximum time τ which includes any transportation time. As the system is assumed to be safety–critical, this maximum value is assumed for all repairs. In the former case, where the time–variation is due to an environmental change, the Maintenance Schedule must include a regular replacement of components so that failures due to component ageing processes may be excluded. Consequently their time–dependent failure rate λ(t) is assumed to come from other sources such as general degradation of irreplaceable system components placing additional loading onto subsystem components. In the latter case the repair time τ is assumed sufficiently small that minimal repair is a reasonable approximation.

In either of these cases, the TTFF reliability function and hazard rate are determined approximately by eqs. (39) and (40), while the specific case of triplex redundancy is considered in more detail. For a constant single component failure rate λ(t) = λ (constant), the triplex MTTFF is given by eq. (24) and the TTFF distribution by eq. (22). In the case of a more general time–dependent failure rate with NHPP flows, the failure time distribution is governed by the solution of a first order differential–delay equation (DDE), the analytical solutions of which are extremely complex even for simple cases. Such DDE equations are generally suitable only for numerical methods and an illustration case assuming a bath–tub like single component failure rate, using Shampine's ddesd function[33,34] (written for MATLAB), is covered in some detail. Using this method the system hazard rate $h_S(t)$ for any λ(t) may be calculated and a redundancy may readily be chosen that will ensure that the hazard rate is kept within prescribed bounds, or that the MTTFF is sufficiently long.

References

1. M Baleani, A Ferrari, L Mangeruca, A Sangiovanni-Vincentelli, M Peri and S Pezzini, Fault Tolerant Platforms for Automotive Safety, *Proc. Int. Conf. for Compilers, Architecture and Synthesis for Embedded Systems, CASES '03. ACM, NY, USA,* 2003, pp 170–177.
2. M Matsumoto, Y Kon, Y Yokosuka, N Amiya, Y Nagatsugu and E Sasaki. Advanced Signaling Systems Based on Transmission Technology for High-density Traffic, *Hitachi Review* **50** (2001), 149–153.
3. R C Hammett. Networking intelligent components to create intelligent spacecraft. *Aerospace Conference, 2001, IEEE Proceedings,* **5** (2001), 2209–2215.
4. K H Eagle and A S Agarwala. "Redundancy design philosophy for catastrophic loss protection". *ARMS Proceedings,* Las Vegas, USA, 1992, 1–4.
5. N. Popov, R. Ion, S. Yu, R. Duffey, "ACR-1000©. Advanced CANDU Based on Proven Safety of CANDU Reactors, *Int. Topical Meeting on Safety of Nuclear Installations, Dubrovnik, Croatia*, 2008, paper A1-094, 1–16.
6. J Wirkner, J Czech, EPR Safety Concept, Int. Topical Meeting on Safety of Nuclear Installations, Dubrovnik, Croatia, October 2008, paper SS-NNN, 1–15.
7. D Bernick, B Bruckert, P D Vigna, D Garcia, R Jardine, J Klecka, and J Smullen, NonStop® Advanced Architecture, *Conf. on Dependable Systems and Networks*, 2005, 12–21.
8. J R Sklaroff, Redundancy Management techniques for Space Shuttle Computers, *IBM J. of Res. and Dev.,* **20** (1976) 20–28.

9. M Rausand and A Høyland, System Reliability Theory: Models, Statistical Methods and Applications, 2^{nd} Ed., (Wiley), USA, 2004.
10. MILSTD–202G.Test Method Standard for Electronic and Electrical Component Parts, 2002.
11. W A Thompson Jr, On the foundations of reliability, *Technometrics* **23** (1981) 1–13.
12. E Cinlar, *Introduction to Stochastic Processes*, Prentice Hall, New Jersey, (1975).
13. D Gross and C M Harris: *Fundamentals of Queuing Theory*. Wiley, USA, (1982).
14. D Cox, *Renewal Theory*,(Methuen, USA, (1967).
15. C G Cassandras and S Lafortune, *Introduction to Discrete Event Systems*, Springer, USA (1999).
16. A D Solov'yev, and V A Zaytsev. Standby with incomplete renewal, *Engineering Cybernetics*, **13** (1975) 58–62.
17. J Keilson. A Limit Theorem for Passage Times in Ergodic Regenerative Processes, *Ann. Math. Statist.* **37** (1966) 886–870.
18. A D Solov'yev. Asymptotic behaviour of the time of first occurrence of a rare event, *Engineering Cybernetics*, **9** (1971), 1038–1048.
19. V A Zaytsev, and A D Solov'yev, Redundancy of complex systems, *Engineering Cybernetics*, **13**, (1975) 66 – 76.
20. I B Gertsbakh. Asymptotic Methods in Reliability Theory: A Review, *Adv Appl Prob.* **16** (1984) 147 – 175.
21. B V Gnedenko and I A Ushakov. *Probabilistic Reliability Engineering*, Wiley, USA (1995).
22. R M Goodall, R Dixon and V M Dwyer. Operational Reliability Calculations for Critical Systems", *Proc. 6th IFAC Safeprocess conference*, (2006), 823–828.
23. A Y Cheer and D A Goldston, "A differential delay equation arising from the sieve of. Eratosthenes", *Maths of Comp*, **55** (1990) 129–141.
24. R Bellman and K L Cooke, *Differential-Difference Equations*, Academic Press, New York, (1963).
25. R D Driver, D W Sasser and M L Slater, The equation $x'(t) = ax(t) + bx(t - \tau)$ with small delay, *Am Math Monthly*, **80** (1973) 990–995.
26. C Chicone, S Kopeikin, B Mashhoon, and D G Retzlo. Delay equations and radiation damping, *Phys. Letters* **A 285** (2001) 17–26.
27. R M Corless, G H Gonnet, D E G Hare, D J Jeffrey and D E Kuth. On the Lambert W Function, *Adv in Comp Maths* **5** (1996) 329–359.
28. N G de Bruijn. The Difference- Differential Equation $F'(x)=\exp(\alpha x+\beta)F(x-1)$, *Proceedings, Series A* ***56*** *Akademie Van Wetenschappen, Indag. Math*., **15** (1953), pp 449–464.
29. J J A Beenakker, The differential-difference equation $\alpha xf'(x) + f(x–1)=0$, (*Thesis*), Technische Hodgeschool Eindhoven, 1966. Online: http://www.win.tue.nl/lotgevallen/promoties.htm.
30. F S Wheeler. Two differential difference equations arising in number theory, *Trans Am Maths Soc*, **318** (1990) 491–523.
31. D M Bradley. A sieve auxiliary function, *Progress in Math.* **138**, (1996), 173–210.
32. D M Bradley and H Diamond. A Difference Differential Equation of Euler-Cauchy Type, *J. Differential Equations*, **138** (1997) 267–300.
33. L F Shampine and S Thompson. Solving DDEs in MATLAB, *Appl Numer Maths*, **37** (2001) 441–458.
34. L F Shampine. Solving ODEs and DDEs with Residual Control, *Appl Numer Maths*, **52** (2005) 113–127.
35. V M Dwyer. Reliability of various 2–out–of–4:G Redundant Systems with Minimal Repair, *IEEE Trans Reliab*. To be published (2012).

Biographies

Vincent M Dwyer is originally from Manchester, UK. He received the BA degree in Mathematics from the University of Cambridge, UK in 1981 and a DPhil in Theoretical Physics from the University of York in 1986. In 1988, after periods in Trinity College, Dublin and Warwick University, UK, he became a member of the School of Electronic, Electrical and Systems Engineering at Loughborough University, where he is now a Reader in Electronic Devices with particular interests in Reliability and the Physics of Failure.

Roger Dixon spent several years at ALSTOM where he made significant R&D contributions in the areas of control of gasification plant, active vibration control, fault tolerant control of gas turbines and demonstration of novel electromechanical actuators for more-electric aircraft. He joined Loughborough in 2003 and is Head of the Control Systems research group in the School of Electronic Electrical and Systems Engineering. His research focuses on various aspects of control and systems engineering including: application of model-based control systems design, model-based fault detection and isolation, system condition/health monitoring and fault tolerant design of actuators and railway track switches. Roger is a Fellow of the Higher Education Academy, a registered Chartered Engineer and Fellow of the Institution of Mechanical Engineers.

Roger Goodall is Professor of Control Systems Engineering in the School of Electronic, Electrical and Systems Engineering at Loughborough University in the UK. He holds the BA and MA degrees in engineering from the University of Cambridge, and PhD from Loughborough University. From 1970-1982 he worked at British Rail's Research Division in Derby, UK. He moved to Loughborough University in 1982 and became a full professor in 1994. He is an elected Fellow of the Royal Academy of Engineering, and also a Fellow of the professional engineering institutions IET and IMechE.