OPERATIONAL RELIABILITY CALCULATIONS FOR CRITICAL SYSTEMS

Roger Goodall, Roger Dixon, Vincent M Dwyer

Electronic and Electrical Engineering Department
Loughborough University, LE11 3TU, UK
r.m.goodall@lboro.ac.uk

Abstract: Reliability theory deals with the effect of mean time to repair upon overall system failure rates, but for critical systems such calculations are not what is required because an important performance criterion relates to operational failures, which are fundamentally different to unsafe failures: essentially they are the result of the system-level response to avoid unsafe failures. This paper introduces the particular problem for critical systems in general, presents an analysis of some of the relevant conditions and provides some simulation results in the context of a railway active suspension application that illustrate the overall effects and trends.

Keywords: Reliability analysis, fault tolerance, railways, safety analysis

1. INTRODUCTION

In critical systems parallel/functional redundancy is used to ensure continued operation in the present of faults, the objective being to accommodate faults such that they don't cause unsafe system failures, probabilistically determined to be consistent with the specified safety integrity level (BSI 2002, Jesty and Hobley 2000). In practice fault monitoring is included such that remedial action is taken to avoid unsafe conditions, for example when one more fault would cause a system failure – i.e. an aircraft landing at the nearest airport, a train running at reduced speed or stopping completely, an adaptive cruise control system in a car identifying the problem and handing responsibility back to the driver. All these can be classified as "operational failures" because the intended schedule or operational state can no longer be sustained, and the corresponding level of "operational reliability" is clearly an important system-level performance indicator.

It is therefore necessary to distinguish between the mean time between actual (i.e. unsafe) failures (MTBF) and the mean time between operational failures (MTBOF). The former will typically be required 10^8 – 10^9 hours for modern high-intensity systems (SIL4), i.e. so high that one would not normally expect to encounter such a situation within the working life of a particular system or set of systems. The latter will inevitably be substantially lower and will reflect the service quality that must be provided.

2. OPERATIONAL RELIABILITY DEFINITION

In practice, if a single fault causes an unsafe condition then some level of functional replication or redundancy is essential. This will usually ensure a satisfactory level of safety but always compromises reliability in some manner. The well known formula MTBF/(MTBF + MTRR) takes account of repair time to predict system availability, but this is different from operational availability because for a fault-tolerant system with redundancy operation continues while the repair is being effected. With a duplex system, if either of the channels fails then this then represents an operational failure for a safety critical system – unless of course the probability of the second channel failing before the first channel has been repaired is sufficiently low to meet the specified probability of an unsafe failure. In practice triplication is required, in which case the following paragraph defines the problem to be solved:

> *A system consists of three identical and independent units, each of which is working under the same conditions. Each unit has a constant failure rate. When any one unit fails, it is repaired in a fixed time τ. An operational failure occurs if, after any unit has failed, a second unit fails within a time τ, such that then there would only be one of the three units left operating (and is therefore potentially unsafe). What is the mean-time until the system first fails?*

The paper also analyses the situation for a quadruplex system, in which case an operational failure occurs if there are two further failures before the first unit has been repaired.

It should be emphasised that the basic elements in a critical system will often be so-called Line Replaceable Units (LRUs). In general these will not be repaired: there will be a stock of functioning units that the maintenance engineers can use to replace the failed unit (which may subsequently be repaired in the background). In this paper we have continued to use the word "repair", even though in practice it will usually mean "replace".

In terms of existing approaches, one way is to identify the most critical component in the system, and then calculate the probability of failure of the system with this component removed. However this gives a pessimistic assessment of reliability because it does not allow for repair and therefore is not considered further in this paper. In general the problem comes under the category of "k out of N" reliability problems in which of N units, N - k units are redundant, e.g. (Moustafa 2001). Two scenarios are considered here:

(i) After a unit fails it takes some time τ to be repaired. This standard view models the situation in which the train is still operational while the repairs are being undertaken. If other units fail
during this time the overall system may become operationally unsafe. Repair times are assumed to follow some general distribution $f(\tau)$. We also consider the specific examples of (a) the exponential distribution, which has been considered by many authors and may be solved by the Chapmann-Kolmogorov technique, e.g. [3], (b) the case of fixed replacement times where τ is constant. Triplex and quadruplex systems i.e. 2 out of 3 and 2 out of 4 systems, are sufficiently simple to allow a general analysis.

(ii) Additionally we consider the case of a fixed maintenance schedule in which maintenance periods are scheduled at intervals of time T, during which the train is assumed to be non-operational. It is assumed that all existing failures are fixed during this down–time.

This latter case is probably more realistic in practice and provides an interesting alternative to the more usual methods.

3. ANALYSIS

This section presents the operational reliability calculation techniques. It has been carried out for both triplex and quadruplex systems, the former resulting in a closed form solution, the latter requiring a numerical solution of the equations. Both analyses have been validated by means of simulation, which also shows the failure probability distribution with time. In all cases a constant failure rate giving an exponential distribution has been assumed, although the analyses can readily be conducted for other failure scenarios.

3.1 Triplex system

We consider first the case of a triplex system in which the failures of each unit are described by independent, identical (iid) exponential distributions with a constant failure rate λ. Two classes of repair strategy are considered. The first assumes that repair times for the three units are described by the same general iid probability distribution function (pdf)$f(\tau)$; specific examples also considered here are the well known case of an exponential repair time distribution of constant repair rate μ, and the case of a constant repair time. Of particular interest to the current work is the case in which repair times are generally much smaller than failure times.

3.1.1 Arbitrary repair time distribution.

The system is described by a state machine with parameter S, equal to the number of units currently in repair. The system starts, at time t = 0, in state S = 0, with all units operational, Fig. (1). When a component fails it moves to state S = 1 with a repair time of τ. Provided that there are no further failures it will progress through this state returning to S = 0 after a time τ. If a further failure occurs it will progress to the failure state S = 2.

The state diagram approach works because the MTBOF can be conditioned, on the first and then subsequent failures. Suppose that the pdf for the system failure time is $f_{tf}(t_f)$, the pdf for the system failure time given that the first failure occurred at t_1 is $f_{tf}(t_f \mid t_1)$ and the pdf for the time of the first failure is $f_{t1}(t_1)$. The MTBOF may then be written generally as

$$\langle t_f \rangle = \int_0^\infty t_f f_{tf}(t_f)dt_f = \int_0^\infty dt_f \int_0^{t_f} t_f f_{tf}(t_f \mid t_1) f_{t1}(t_1)dt_1 \qquad (1)$$
$$= \int_0^\infty f_{t1}(t_1)dt_1 \int_{t_1}^\infty t_f f_{tf}(t_f \mid t_1)dt_f$$

Now, if the failure rate is fixed, it is clear that the value of $f_{tf}(t_f \mid t_1)$ depends upon t_f and t_1 only through terms in $z = (t_f - t_1)$, the additional time to system failure after the failure of the first unit. Thus

$$\langle t_f \rangle = \int_0^\infty f(t_1)dt_1 \int_0^\infty (t_1 + z) f_z(z)dz = \langle t_1 \rangle + \int_0^\infty z f_z(z)dz \qquad (2)$$

As $f_{t1}(t_1) = 3\lambda\exp(-3\lambda t)$ in this case, the first term in eqn (2) is simply $(3\lambda)^{-1}$, while the second term is the expected additional time to failure, after the first unit fails. If we suppose that the repair time for the failed unit is τ, then with probability $\exp(-2\lambda\tau)$, there will be no more failures in the time interval $(0, \tau)$ and the system will be restored to state S = 0 after the extra time τ. Alternatively if there is another failure, the system will enter the state S = 2 of operational failure. This will occur with probability $1 - \exp(-2\lambda\tau)$. Given that a failure occurs in that interval, the expected extra time to failure (given repair time τ) is

$$\langle t_{12} \mid \tau \rangle = \int_0^{\tau} t \frac{2\lambda \exp(-2\lambda t)}{1-\exp(-2\lambda\tau)} dt = \frac{\int_0^{x} 2t\lambda \exp(-2\lambda t) dt}{1-\exp(-2\lambda\tau)} \quad (3)$$

Combining eqns (2) and (3) we obtain

$$\langle t_f \mid \tau \rangle = \frac{1}{3\lambda} + (\tau + \langle t_f \rangle)\exp(-2\lambda\tau) + 2\lambda \int_0^{\tau} t \exp(-2\lambda t) dt \quad (4)$$

$$= \frac{1}{3\lambda} + \langle t_f \rangle \exp(-2\lambda\tau) + \frac{1-\exp(-2\lambda\tau)}{2\lambda}$$

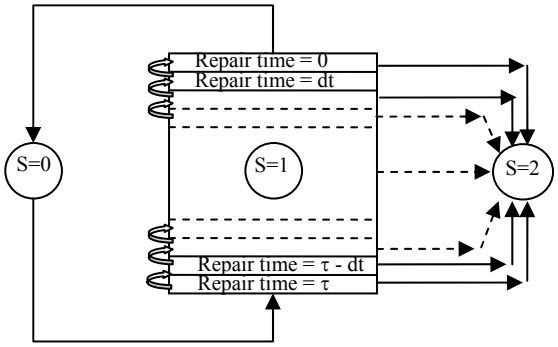

Fig. 1 State transitions for the triplex system.

In the special case that all repair times are equal, $\langle t_{12} \mid \tau \rangle$ is independent of τ and $\langle t_{12} \mid \tau \rangle = \langle t_{12} \rangle$. Thus eqn (4) gives

$$\langle t_f \rangle = \frac{\frac{1}{3\lambda} + \frac{1-\exp(-2\lambda\tau)}{2\lambda}}{1-\exp(-2\lambda\tau)} = \frac{1}{3\lambda(1-\exp(-2\lambda\tau))} + \frac{1}{2\lambda} \quad (5)$$

Notice that in the limit of $\tau \to \infty$ we obtain the expected result that $\langle t_{12} \rangle = 5/6\lambda$ and in the limit of small $\tau \to 0$

$$\lambda \langle t_f \rangle \sim \frac{(1+\lambda\tau)}{6\lambda\tau} + \frac{1}{2} = \frac{1}{6\lambda\tau} + \frac{2}{3} \quad (6)$$

In the case of more general repairs with repair time distribution $f(\tau)$ we obtain

$$\lambda \langle t_f \rangle = \lambda \int_0^{\infty} \langle t_f \mid \tau \rangle f(\tau) d\tau = \frac{\frac{5}{6} - \frac{1}{2}\tilde{f}(2\lambda)}{1-\tilde{f}(2\lambda)} \quad (7)$$

where $\tilde{f}$ is the Laplace Transform of $f(\tau)$. In particular, for the exponential repair case of $f(\tau) = \mu \exp(-\mu\tau)$, eqn (7) reduces to

$$\lambda \langle t_f \rangle = \frac{5(\mu+2\lambda)}{12\lambda} - \frac{\mu}{4\lambda} = \frac{5}{6} + \frac{\mu}{6\lambda} \quad (8)$$

which can be confirmed using the usual imbedded Markov methods and the Chapmann-Kolmogorov equations, see e.g. Rausand and Hoyland.

Expanding the Laplace Transform around small repair times

$$\tilde{f}(2\lambda) = \int_0^{\infty} f(\tau)\exp(-2\lambda\tau) d\tau \sim 1 - 2\lambda\langle\tau\rangle + 2\lambda^2\langle\tau^2\rangle + \ldots \quad (9)$$

eqn (7) becomes approximately

$$\lambda \langle t_f \rangle \sim \frac{\frac{1}{3} + \lambda\langle\tau\rangle}{2\lambda\langle\tau\rangle - 2\lambda^2\langle\tau^2\rangle} = \frac{1}{6\lambda\langle\tau\rangle}\left(1 + 3\lambda\langle\tau\rangle + \lambda\langle\tau^2\rangle/\langle\tau\rangle\right) \quad (10)$$

which agrees with eqn (6) for a fixed repair time, i.e. $f(\tau) = \delta(\tau - \tau_0)$.

3.1.2 Defined maintenance schedule

As a comparison we consider also the case of a fixed maintenance schedule. This assumes that units are working continuously between maintenance periods regularly spaced T days apart. This strategy is more representative of what occurs in many practical situations and, provided that repairs are conducted during these periods, requires no specific knowledge of the repair time distribution. It is a simple matter to allow the schedule periods to be stochastic and is useful as it allows us to see the effect, on the MTBOF, of missed maintenance periods. To do this we condition the MTBOF on the length of time T before the next scheduled maintenance. Thus, in general,

$$\langle t_f \rangle = \int_0^{\infty} dt_f \int_0^{\infty} t_f f_{tf}(t_f \mid T) f_T(T) dT \quad (11)$$

$$= \int_0^{\infty} f_T(T) dT \int_0^{\infty} t_f f_{tf}(t_f \mid T) dt_f = \int_0^{\infty} G(t_f \mid T) f_T(T) dT$$

where $G(t_f|T)$ is the mean time to failure given that the next maintenance is in time T.

As all units are assumed to be fixed during the maintenance period, our concern is only whether or not the system fails in time t. If it does not then it is returned to state S = 0 at time t which will occur, if the failure rate is constant, with probability $p = \exp(-3\lambda t) + 3\exp(-2\lambda t)(1 - \exp(-\lambda t))$. Failure occurs with probability $(1 - p)$ and occurs after a time

$$\langle t_f \mid T \rangle = \frac{1}{1-p} \int_0^{T} t\left(3\exp(-2\lambda t) - 2\exp(-3\lambda t)\right) dt \quad (12)$$

Thus we can write in a similar fashion to eqn (4)

$$G(t_f \mid T) = (T + \langle t_f \rangle)p + \int_0^{T} t\left(3\exp(-2\lambda t) - 2\exp(-3\lambda t)\right) dt$$

$$= \langle t_f \rangle \left(3\exp(-2\lambda T) - 2\exp(-3\lambda T)\right) + 3\frac{1-\exp(-2\lambda T)}{2\lambda}$$

$$- 2\frac{1-\exp(-3\lambda T)}{3\lambda} \quad (13)$$

Again in the case that T is constant $G(t_f \mid T) = \langle t_f \rangle$ and eqn (13) may be rearranged to give

$$\lambda \langle t_f \rangle = \frac{\frac{5}{6} - \frac{3}{2}\exp(-2\lambda T) + \frac{2}{3}\exp(-3\lambda T)}{1 - 3\exp(-2\lambda T) + 2\exp(-3\lambda T)} \quad (14)$$

$$= \frac{\frac{5}{6} + \frac{5}{6}\exp(-\lambda T) - \frac{2}{3}\exp(-2\lambda T)}{1 + \exp(-\lambda T) - 2\exp(-2\lambda T)}$$

Clearly in the limit of $T \to \infty$ we again obtain the expected result that $\lambda\langle t_f \rangle = 5/6$ and in the limit of small T

$$\lambda \langle t_f \rangle \sim \frac{1 + \frac{5}{3}\lambda T}{3\lambda T} = \frac{1}{3\lambda T} + \frac{5}{9} \quad (15)$$

Finally, with a stochastic maintenance schedule, combining eqns (11) and (13) yields

$$\lambda \langle t_f \rangle = \frac{5 - 9\tilde{F}(2\lambda) + 4\tilde{F}(3\lambda)}{6\left(1 - 3\tilde{F}(2\lambda) + 2\tilde{F}(3\lambda)\right)} \sim \frac{\lambda\langle T\rangle + O(\lambda^3\langle T^3\rangle)}{3\lambda^2\langle T^2\rangle - 5\lambda^3\langle T^3\rangle} \quad (16)$$

$$= \frac{1}{3\lambda\langle T^2\rangle/\langle T\rangle}\left(1 + \frac{5\lambda\langle T^3\rangle}{3\langle T^2\rangle}\right)$$

where $\widetilde{F}$ is the Laplace Transform of $f_T(T)$.

Suppose, for example, that 10% of the maintenance periods are missed so that

$$f_T(T) = 0.9\delta(T - T_0) + 0.1\delta(T - 2T_0) \quad (17)$$

Eqn (16) then gives

$$\lambda\langle t_f\rangle = \frac{1}{3.9\lambda T_0}\left(1 + \frac{8.5\lambda T_0}{3.9}\right) \quad (18)$$

which decreases the MTBOF by around 25%.

3.2 Quadruplex system

For quadruplex systems the analysis is much the same, although now the system can continue running in the state S = 2. In the case of fixed repair times, failing units go into and come out of repair in the same order, while for a general repair time distribution this may not be the case. The state representation is still appropriate although, except for the case of exponentially distributed repair times with constant repair rate μ, the Markov method cannot be used as the transition rates between states also depend upon the remaining repair times for those objects still in repair. The state transition diagram is shown in Fig. 2 and is of M/G/2 type (Cassandras and Lafortune). This is more complex than the triplex case as $H(y_1, y_2)$, the additional time to failure given that two units are in repair with remaining repair times y_1 and y_2, is also required. Note that the parameterized states S = 1 and S = 2 have been condensed for the sake of brevity. In reality the state S = 1 is identical to that in Fig. 1, while the state S = 2 is a two dimensional version and would be represented by a checker board using the same sort of representation.

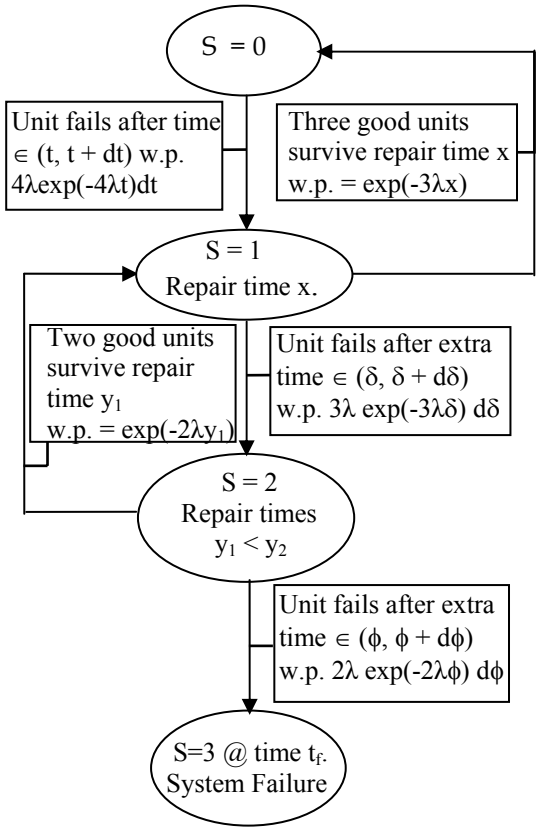

Fig. 2 State-transition diagram for quad–system.

The details of the analysis of this case can be found in Dwyer, et al. The equivalent expressions of eqn (4) in the triplex case, in this case, is:

$$G(\tau) = \langle t_f \mid \tau\rangle = \frac{1}{4\lambda} + \langle t_f\rangle\exp(-3\lambda\tau) + \frac{1-\exp(-3\lambda\tau)}{3\lambda} + 3\int_0^{\tau} d\Delta \exp(-3\Delta)\int_0^{\infty} f(y')H(x-\Delta, y')dy' \quad (19)$$

where

$$H(y, y') = \frac{1-\exp(-w)}{2} + \exp(-w)G(|y - y'|) \quad (20)$$

for $w = \min(y, y')$. For the case of exponential repair $f(\tau) = \mu\exp(-\mu\tau)$, Laplace Transforming eqns (19) and (20) provides the same result as the imbedded Markov method and the appropriate Chapman-Kolmogorov equations, giving a value of MTBOF of

$$\lambda\langle t_f\rangle = \frac{13}{12} + \frac{5\mu}{12\lambda} + \frac{\mu^2}{12\lambda^2} \quad (21)$$

For the case of a fixed repair time eqns (19) and (20) combine to produce

$$\lambda G(x) = \lambda G(0)\exp(-3\lambda x) - \frac{3}{2}\exp(-2\lambda x) + \frac{2}{3}\exp(-3\lambda x) + \frac{5}{6} + 3\lambda\exp(-3\lambda x)\int_0^{x} dw \exp(\lambda w)\lambda G(\tau - w) \quad (22)$$

together with the condition

$$\lambda MTTOF = \lambda G(0) = \frac{1}{4} + \lambda G(\tau) \quad (23)$$

which expresses the fact that if there is no time left until the repair is finished, the extra time to failure will be equal to the MTBOF. The closed form analytic solution to the integral equation, eqn (22), does not have a simple form (Dwyer et al). Moreover, the Fredholm equation is numerically stable and may readily be solved iteratively. For large values of λτ the result is the expected value of 1/4λ + 1/3λ + 1/2λ = 13/12λ, while for small λτ we can expand eqn (22) to give

$$\lambda\langle t_f\rangle \sim \frac{1}{12\lambda^2\tau^2} + \frac{7}{14\lambda\tau} + \ldots \quad (24)$$

The, validity of the numerical solution to eqn (22) and the accuracy of the approximation, eqn (24), is demonstrated in Fig. (3)

Finally with the repair schedule described in section 3.1.ii, the appropriate results are, for a fixed maintenance period,

$$\lambda\langle t_f\rangle = \frac{\frac{13}{12} + \frac{13}{12}\exp(-\lambda T) - \frac{23}{12}\exp(-2\lambda T) + \frac{3}{4}\exp(-3\lambda T)}{1 + \exp(-\lambda T) - 5\exp(-2\lambda T) + 3\exp(-3\lambda T)} \sim \frac{1}{4\lambda^2 T^2} + \frac{9}{16\lambda T} + \ldots \quad (25)$$

for small λT, while for a stochastic period given by pdf $F_T(T)$

$$\lambda\langle t_f\rangle = \frac{\frac{13}{12} - 3\widetilde{F}(2\lambda) + \frac{8}{3}\widetilde{F}(3\lambda) - \frac{3}{4}\widetilde{F}(4\lambda)}{1 - 6\widetilde{F}(2\lambda) + 8\widetilde{F}(3\lambda) - 3\widetilde{F}(4\lambda)} \sim \frac{1}{4\lambda^2\langle T^3\rangle/\langle T\rangle}\left(1 + \frac{9\lambda\langle T^4\rangle}{4\langle T^3\rangle}\right) \quad (26)$$

In this case missing 10% of the scheduled repair periods will lower MTBOF by around 35%.

3.3 Comparison

For the safety-critical systems under investigation here, the expected repair times, or the expected maintenance period, will be significantly smaller than the expected failure times so the region of interest is that of small values of ε equal to $\lambda\langle\tau\rangle$ or λT. Comparing eqns (5, 8, 10, 15) with eqns (21, 24, 25, 26) it is clear that, in this limit, the λMTBOF of triplex systems ~ $1/\lambda\langle\tau\rangle$, while for quadruplex systems, λMTBOF ~ $1/\lambda^2\langle\tau^2\rangle$. For higher order redundancy, N-plex systems, one would expect a behaviour of $\sim\lambda^{N-2}\langle\tau^{N-2}\rangle$. For a value of ε = 0.01, the quadruplex system has a MTBOF of around 50 – 100 times that of the triplex system.

A scheduled maintenance scheme with a maintenance interval of $\tau\sqrt{3}$ gives the same MTBOF as a scheme which fixes failures with a constant repair time τ. Conversely, fixing failed items with a constant repair time of $T/\sqrt{3}$ is equivalent to a proposed maintenance schedule of fixed period T.

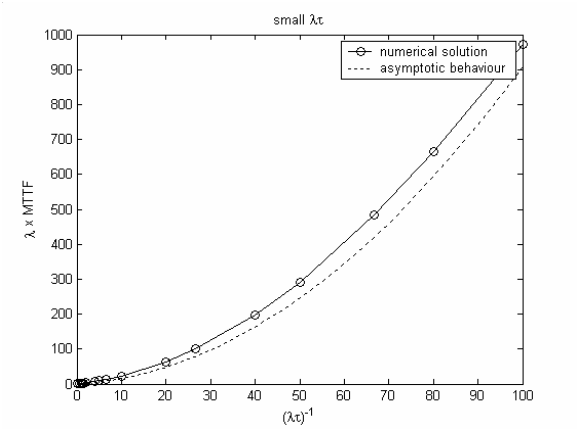

Fig. 3 Numerical solution to eqn (22)

4. AN ENGINEERING EXAMPLE (ACTIVELY-CONTROLLED RAILWAY BOGIE)

4.1 Problem description

The work described in the paper is motivated by research into active suspension technology applied to railway vehicles (Goodall et al 2005). Some types of active suspension are not critical systems, for example when they are just used to improve ride quality they can simply be switched off in case of a fault. However, when the active control technology is applied to control the wheels and wheelsets to provide steering and/or stability control of the running gear, a failure is likely to cause an unsafe condition such as derailment of the train. A typical modern train will on average operate for 50,000 hours (typically 80,000km of operation, depending upon the type of service) before a fault interrupts its operation, and so the MTBOF due to the additional active suspension equipment needs to be specified as 500,000 hours or higher, i.e. such that it has only a marginal impact upon the overall train casualty rate.

The situation has been analysed for equipment having a MTBF of 410 days (10,000 hours) which is considered typical for a function involving sensor, processor and power electronics. A repair time of 7 days (i.e. a weekly maintenance schedule), is used.

With a weekly schedule, the appropriate results are given in eqn (15) for triplex systems and eqn (25) for quadruplex. For $\lambda T = 7/410$, eqn (15) gives λMTBOF = 410/21 ≈ 20, thus MTBOF ≈ 8200 days or around 200,000 hours. By contrast, eqn (25) gives λMTBOF $(410/7)^2/4 \approx 860$, so MTBOF ≈ 8×10^6 hours. This implies that the reliability of a triplex suspension, with weekly maintenance, will affect the train's overall reliability somewhat, whereas a quadruplex suspension will essentially have no impact.

4.2 Results

For the parameter values listed in section 4.1, the MTBOF values corresponding to the leading order expressions are listed in Table 1, and their corresponding numerical values for the railway example are given in Table 2. To facilitate comparison the period of the maintenance schedule is assumed equal to the mean repair time $\langle\tau\rangle$.

Table 1 Expressions giving MTBOFs

	Triplex	Quadruplex
General τ Distribution	$\frac{1}{6\lambda\langle\tau\rangle}+\frac{1}{2}+\frac{\langle\tau^2\rangle}{6\langle\tau\rangle^2}$	---
Chap-Kolm Mean time 1/μ	$\frac{1}{6\lambda\langle\tau\rangle}+\frac{5}{6}$	$\frac{1}{12\lambda^2\langle\tau^2\rangle}+\frac{5}{12\lambda\langle\tau\rangle}$
Fixed τ	$\frac{1}{6\lambda\tau}+\frac{2}{3}$	$\frac{1}{12\lambda^2\tau^2}+\frac{7}{24\lambda\tau}$
Scheduled Maintenance	$\frac{1}{3\lambda T}+\frac{5}{9}$	$\frac{1}{4\lambda^2T^2}+\frac{9}{16\lambda T}$

Table 2 Values of MTBOFs

	Triplex	Quadruplex
General τ Distribution	~ 100,000 h	~ 3,000,000 h
Chap-Kolm Mean time 1/μ	104,257 h	3,053,245 h
Fixed τ	102,617 h	2,933,173 h
Scheduled Maintenance	197,581 h	8,763,499 h

The analysis discussed above does not give the failure probability distributions, and so a simulation experiment has been developed to provide the distributions. The simulation uses time-stepping loops with an assessment being made at each time-step as to whether an individual unit has failed (the failed units will then be returned to full health once the repair period is complete). If, in the case of the triplex system, two simultaneous failures occur the

operational failure time is recorded and the simulation repeated. In this way, over many runs (e.g., 5000) a PDF can be built up. Note that, the simulation results can also be used to confirm the analytical results (in terms of MTBOF).

Typical PDF results for the active suspension example are given in Figs. 4 and 5. The profound effect of repairing failed units is clear from the graph shown in Fig.4. The simulation uses 5000 runs and but still will not give an exact comparison: it shows a MTBOF of 4681days compared with the analytical expression which gives 4396, about a 6% error. Increasing the number of simulation runs progressively decreases this error.

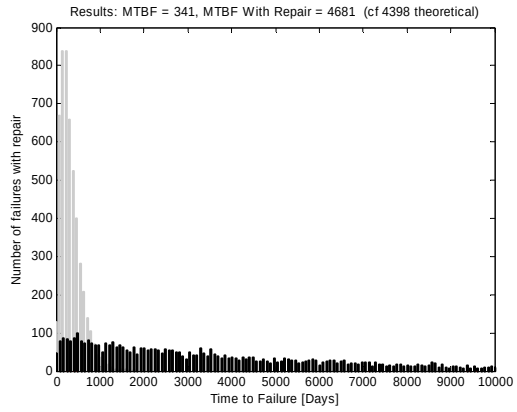

Fig. 4 Simulation pdfs for the triplex railway application with fixed repair time (Note: grey represents results for no repair, black with repair).

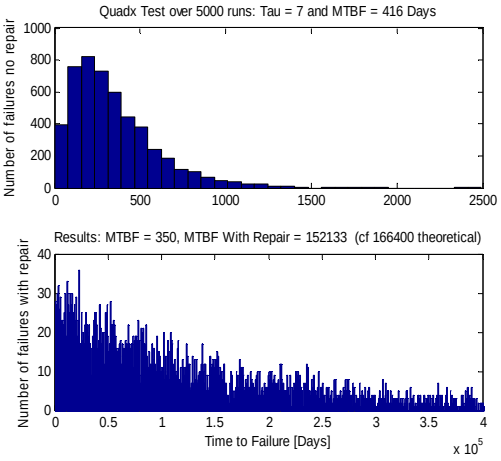

Fig. 5 Simulation pdfs for the quadruplex railway application (fixed repair time)

In the quadruplex case (Fig. 5) the large difference in scales means that showing the results on the same graph is not useful – hence the two graphs. Note that again the simulation results match the theoretical value fairly closely.

5. CONCLUSIONS

This paper analyses the situation for fault-handling in high-integrity systems, in particular representing a realistic maintenance approach. It is focussed not upon the probability of an unsafe failure, but upon the consequent effect of the redundancy (introduced to assure high-integrity) upon operational reliability. It shows that the well-known Chapman-Kolmogorov equations give a good assessment if the mean value of the exponential distribution assumed for these equations is equal to the fixed repair time (although the failure distribution will be very different in the two cases). However the exponential distribution of repair times is not what is encountered in a practical maintenance situation. A fixed maintenance schedule is not well predicted by these equations, and the analysis shows that the MTBOF is favourably increased - by a factor of around 2 for triplex and 3 for quadruplex systems.

It is also useful to see the effect of moving from triplex to quadruplex, for which the MTBOF is typically increased by a factor of 30.

The MTBOF, as opposed to the classical MTBF, is an idea that is practically important but seems to have neglected in reliability engineering. Further work is required to consolidate the concept and to refine it for more complex situations. Some of this work is considered in Dwyer et al. (submitted).

REFERENCES

BS EN 61508 “Functional safety of electrical / electronic / programmable electronic safety-related systems” (2002).

Goodall R M, Bruni S and Mei TX, “Concepts and prospects for actively-controlled railway running gear” Proc 19th IAVSD Symposium (2005) Milan, Italy

Jesty P H, Hobley K M, Evans R, and Kendall I, “Safety Analysis of Vehicle-Based Systems,” Proceedings of the Eighth Safety Critical Systems Symposium (2000) pp. 90-110.

Moustafa M S “Availability of *K*-out-of-*N*:*G* Systems with Exponential Failures and General Repairs”, Economic Quality Control **16** (2001), 75 – 82.

Dwyer V M, Goodall R M and Dixon R, “Reliability of Triplex and Quadruplex safety systems with fixed repair times”, submitted to IEEE Transactions on Reliability.

Cassandras C G and Lafortune S, “Introduction to Discrete Event Systems”, Springer, USA, (1999).

Rausand M and Høyland A, System Reliability Theory, Models, Statistical Methods and Applications, 2nd Ed., Wiley, 2004.