DEFERRED MAINTENANCE OF REDUNDANT SYSTEMS

VITALI VOLOVOI*
Alpharetta, Georgia, USA
e-mail: vitali@volovoi.com

Redundancy is commonly used as an effective means to ensure the high dependability of engineering systems. This leads to a trade-off related to the timing of replacing failed components: faster replacement reduces the risk of system failure but is generally more expensive. This paper discusses several approaches to assessing the risks of system failure in the presence of deferred maintenance. The relationships among several existing models are examined, with a focus on the commonality and limitations of those models. In addition to Markov models, the impact of deviating from those assumptions is studied for two applications with the fixed time repair delays.

Keywords: Deferred Maintenance, Time-Limited Dispatch, Redundant Systems

1. Background

Historically, the dominant application domain was safety-critical systems (in particular, this is referred to in the filed of aerospace as Time-Limited Dispatch [1,2]). The estimated risks were quite small, which impacted the choice of models. In particular, the implicit assumption of the models was that the expected time to repair was significantly less than the expected time to failure. The technologies associated with the Internet of Things provide both the opportunity and the incentives for making maintenance strategies more sophisticated. As a result, deferred maintenance policies are likely to expand in scope, potentially exposing the limitations of some models. The goal of this paper is to provide a unified view of the existing approaches and to evaluate alternative methods that can either improve the models' accuracy or their scalability. In particular, an application of a procedure described in [3] is provided to capture non-Markovian effects.

Deferred maintenance can be construed as one of the fundamental reliability problems for repairable systems: as systems degrade, the timing of

*Corresponding Author

maintenance actions must be selected to balance the risks of systems failures with the maintenance costs. Let us consider the following system states: a set of up states, $U_1 \dots U_n$, including the original (full-up) state U_1; and the failed states $F_1 \dots F_m$ (aggregating all failed states into a single failed state F does not impact the dynamic of the up states U_i). Memoryless (*i.e.,* constant rate, or following exponential distribution) assumption for the transitions between system states is often utilized for continuous time processes. The resulting Markov processes are attractive due to their superior analytical tractability, but the impact on the resulting accuracy of the model is not always clear in practical applications. On the one hand, failures and repairs often don't follow exponential distributions; on the other hand, the resulting modeling error for the metrics of interest can be still small (or absent), depending on the structure of the problem.

There is extensive research on non-Markovian processes going back over sixty years [4] (see also the review of the recent state-of-the-art [5]). However, to date the practical reliability applications of the existing methods are quite limited due to their complexity. Monte Carlo simulation provides the flexibility of modeling non-Markovian processes with the cost of a lack of analytical transparency and computational errors that can be significant for rare events. In this context, this paper relies on a relatively simple analytical method that allows the modeling of non-exponential holding (sojourn) times [3]. The generality of the method is further explored in [3], while here the application of the method to two problems with constant repair delays is demonstrated. Instead of solving a non-Markovian problem from scratch, the method relies on finding an equivalent Markov model with the same asymptotic behavior.

Let us consider a fleet of systems (*i.e.,* aircraft, windmills, computer servers, etc.) and focus on evaluating the expected fleetwide frequency of system failures. In safety-critical systems, there might be a regulation stipulating an allowable limit on such a frequency. *E.g.,* in civil aviation the regulating authority uses this quantity as opposed to a specific risk associated with a particular system [1]. For Markov processes with n states and continuous time the governing system of (Chapman-Kolmogorov) differential equations can be written as follows:

$$\frac{dP(t)}{dt} = Q \cdot P(t), \quad Q_{ii} = -\sum_{j \neq i}^{n} Q_{ji} \quad Q_{in} = 0 \tag{1}$$

Here are $P_i(t)$, $i = 1 \dots n$ the probabilities of being in state S_i: $P_i(t) = P\{X = S_i\}$, and Q is the transition rate matrix with the diagonal terms

compensating for the off-diagonal terms in each column and the last zero column representing the absorbing state. The systems' hazard rate (i.e., the probability that the system will fail given that it has not failed yet) is an absolute value of the second largest (Perron-Frobenius) eigenvalue of the matrix Q (see [6] and [3]). Indeed, using the Perron-Frobenius theorem, one can show that there is a unique largest negative eigenvalue $-k$ for the transition rate matrix Q. In addition, there is a zero eigenvalue due to the absorbing state. As a result, as time $t \to \infty$, only the contribution from the two largest eigenvalues can be retained.The other eigenvalues are negative with absolute values larger than k. Here c_i and v_i are components of the first two eigenvectors, and A and B are the corresponding constants with A uniquely defined because F is an absorbing state:

$$P\{X = F\}(t) \approx Ac_n + Bv_{n+1}e^{-kt} = 1 - Bv_{n+1}e^{-kt}$$
$$P\{X = U_i\}(t) \approx Ac_i + Bv_ie^{-kt} = Bv_ie^{-kt}$$

The system hazard rate is therefore $h(t) = dF/dt/(1 - F(t)) = k$.

1.1. *Dual Redundancy: Markov model*

Let us consider a system consisting of two identical redundant components, so that operation of only one component is required for system operation. The failure and repair rates for each component are λ and μ, respectively. The transition rate matrix Q has the following form:

$$Q = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -\lambda - \mu & 0 \\ 0 & \lambda & 0 \end{pmatrix} \tag{2}$$

For this system the absolute value of smallest (negative) root is

$$k_1 = \frac{3\lambda + \mu - \sqrt{(3\lambda + \mu)^2 - 8\lambda^2}}{2} \tag{3}$$

An alternative calculation is based on the solution of the renewable process equation, following Birolini [7][a]. The method relies on the solution of the integral equations of the renewal process using Laplace transforms. As a result, for any up state U_i mean time to failure (MTTF) m_i can be calculated using the following system of the linear algebraic equations:

$$\tilde{q}_i m_i = 1 + \sum_{j=1, j\neq i}^{n} q_{ji} m_j \tag{4}$$

[a] See Appendix A.7.5.3.2 in an excellent A. Birolini book [7].

For the considered double redundant system, this yields the following solutions:

$$m_1 = \frac{3\lambda + \mu}{2\lambda^2} \quad m_2 = \frac{2\lambda + \mu}{2\lambda^2} \tag{5}$$

As expected, m_i does not depend on the last column of the matrix Q (*i.e.,* on the transitions from the failed state—but at least one of those transitions must be present for the analysis to be valid to avoid absorbing states). However, the steady-state probabilities for each state do depend on recovery from the failed state. Let us adopt a standard method [1,2] where upon failure the system returns to the "fully up" state U_1. In fact, the introduction of such an "artificial" transition allows an even simpler approach to estimating the system hazard rate: once the probabilities for the resulting steady state are established, we can evaluate the conditional probabilities of being in an up state given the fact that the system has not failed $\bar{P}_i = P\{X = U_i | X \neq F\}$, and use those probability to weight-average the rates of direct transitions to the failed state:

$$k_s = \sum_{i=1}^{n} \bar{P}_i q_{ni} \tag{6}$$

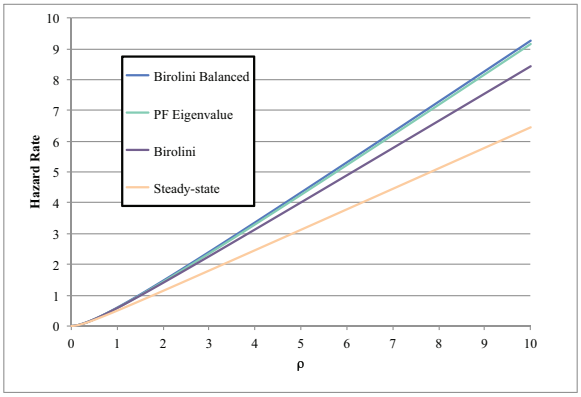

Figure 1. Comparing hazard rates of Markov models for a two-part system.

Figure 1 demonstrates the comparison of these approaches for different values of $\rho = \lambda/\mu$. in addition to the Perron-Frobenius eigenvalue, steady-state, and Birolini methods, there is a "Birolini Balanced" curve that is

obtained when the recovery from the failed state is arranged to match the asymptotic conditional probabilities $\bar{P}_i$ in the presence of the absorbing state (as calculated based on the eigenvalue analysis). While the differences can be observed when $\rho \approx 1$, for smaller values of ρ, all four curves converge. The rate of convergence to Perron-Frobenius values is different for the considered methods: the differences for "Birolini Balanced" are negligible even for very large values of $\rho = 10$. For $\rho = 1$ (and considering $\mu = 1$ for specificity, since all the values scale with μ) the steady state value is 0.5, while both the Perron-Frobenius and Birolini methods show very close results: 0.58579 and 0.58333, respectively.

1.2. *Fixed repair delays*

Let as turn to non-Markovian effects for this problem and consider fixed repairs with mean value of $\tau = 1/\mu$, and for specificity, consider $\tau = \mu = 1$. Using finite-difference method with a step of 6×10^{-4} and $10,000$ steps (the sojourn time distribution for repair is a part of the state description) leads to the value of the hazard rate 0.62513 (see details in [3]). This value differs significantly from the one for the exponential repair (0.58579).

Next, we calculate the asymptotic value using the method described in [3]. The method is based on the presence of the quasi-steady state after the initial transient phase Eq. 2. As a result, for any node of the state-space representation, the total inflow (regardless of the number of inflow transitions) has the same time dependency as the individual up states, *i.e.,* proportional to e^{-kt}, where k is the Perron-Frobenius eigenvalue. This allows us to infer the holding time distribution for this node, taking into the account the intensity of the outflow into other nodes (in our case, the failure of the system). For the fixed repair time, we can observe that the equivalent failure rate of the repair will be equal to

$$\hat{\mu} = \frac{\lambda - k}{e^{\tau(\lambda - k)} - 1} \tag{7}$$

At the same time Eq. 3 relates k to $\hat{\mu}$ and λ. Since k is monotonically decreasing with $\hat{\mu}$, a simple iteration requires only a few steps to reach the solution for both: $\hat{\mu} = 0.82427$ and $k = 0.62518$; comparing this value with the "brute force" methods demonstrates the accuracy of this approach.

2. FADEC system

Next, let us consider a simplified Full Authority Digital Electronics Control system (FADEC) [2] as depicted in Figure 2B. This representation of failure

logic is referred to as a reliability block diagram, where each component is denoted with the block interrupting the path in the corresponding location if it fails. The system is operational as long as there is an uninterrupted path from the sink on the left to the source on the right.

FADEC has built-in high redundancy that leads to a very low probability of loss of control when all the components are fully functional. The high redundancy also leads to a large number of components comprising the system, so the chances of one of those components failing are relatively high. This renders impractical immediate replacements of components upon failure and leads to the need for operations with degraded redundancy.

Specific numeric values are taken from [2]: failure rates (per hour) are $\lambda_1 = 5.2\times10^{-5}$ and $\lambda_2 = 6.5\times10^{-5}$ for CPU units, and $\lambda_3 = 8.0\times10^{-5}$ and $\lambda_4 = 9.0 \times 10^{-5}$ for channel power. A cross-link is provided, so a working component from a different channel is used if the corresponding component from its own channel fails. The corresponding Markov diagram is shown in Figure 2A. No repairs are shown on the diagram for clarity's sake, but they are determined based on the policies described below.

There are two categories of time-limited dispatch applied after the failure of a single component: long- and short-term dispatch intervals (LTD and STD, respectively). LTD varies between 200 and 2,000 hours, and is applied when a CPU fails (represented by states B_1 and B_2); STD is 200 hours, and applied if a power unit fails (represented by states C_1 and C_2). Two failures result in a Do Not Dispatch (DND) policy (so the aircraft is grounded and repaired) within 5 hours (states D_i on the diagram).

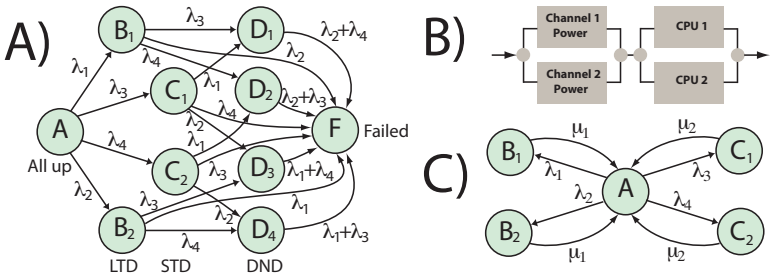

Figure 2. FADEC system: A) Full Markov state space B) RBD diagram C) Reduced Markov state space

The hazard rate, as calculated using the Perron-Frobenius eigenvalue varies slightly sublinearly, from 3.857×10^{-6} to 1.021×10^{-5} between the

LDT limits. Using this rate as a reference, the relative differences in rate predictions are shown in Figure 3. Four methods are used for exponentially distributed repair (equivalent repair rates μ_1, μ_2, and μ_3 are the respective inverses of TLD intervals LDT, SDT, DND). In addition to the full Markov steady-state method (shown in black), there are three approximate steady-state methods that rely on a reduced-state diagram, as shown in Figure 2C, to evaluate $\bar{P}_i$ for single failures only. These methods utilize Eq. 6 using the respective transition rates to the failure state. The Time-Weighted Average (TWA) method uses the repair rates shown in Figure 2C, while the Reduced Markov method corrects for the outflow to the failed state from each single failure state; so for example, for state B_1 the rate is corrected as follows: $\mu_1 \rightarrow \mu_1 + \lambda_2$. Both TWA and Reduced Markov are methods approved by the FAA [1], and the need to utilize reduced-state models is driven by the state-space size of real-world problems.

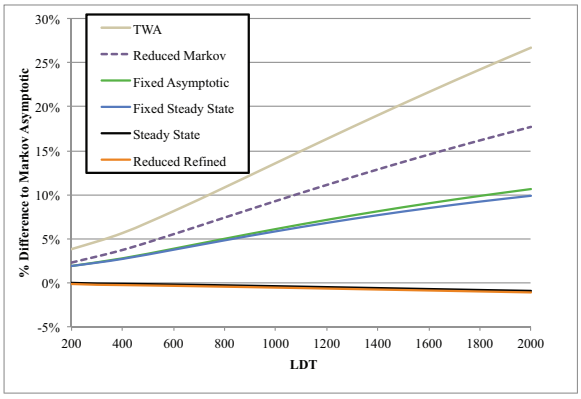

Figure 3. Comparing hazard rates for FADEC.

Instead of discarding the impact of dual failures that do not lead to system failure (D_i), one can note that a short duration of DND policy (and the resulting low risk of system failures from those states) implies that getting into those states is equivalent to recovery to the fully operational state. This leads to a refinement of the reduced Markov model, where the repair rates are further corrected to include failure of all other components (so for B_1, the rate is corrected as follows: $\mu_1 \rightarrow \mu_1 + \lambda_2 + \lambda_3 + \lambda_4$). As can be observed in Figure 3 (orange curve), the difference compared to the full Markov steady-state rate is negligible. Since the component failure

rates are at least two orders of magnitude smaller than the repair rates, the difference between the steady-state renewal process and the asymptotic rate is small (*cf.* $\rho = 0.01$ in the dual-redundant example, Figure 1).

The other two curves are obtained by applying corrections for the fixed delay. The green curve is based on the asymptotic rate correction (Eq. 7). The blue curve is based on the similar correction for the steady-state solution. The latter correction is even simpler to implement: k is set to zero in Eq. 7), and no iterations are required (see [3] for details). The difference between those two curves is small (just like for the corresponding cases with exponential repair). However, there is a sizable difference when fixed repair delays are compared to exponential repairs with the same mean (about 10% for the upper limit of the LDT range).

3. Conclusions

The paper demonstrates the relationships among different approaches for estimating the hazard rate of a redundant system with deferred maintenance policies. The accuracy of a refined reduced-state Markov model and the approximating fixed-repair delays with the equivalent Markov models [3] are demonstrated. The resulting models are relatively simple and scalable, so it is hoped that their use will be more widespread in the future.

References

[1] SAE ARP 5107, *Guidelines for Time-Limited-Dispatch (TLD) analysis for electronic engine control systems. Revision B.* SAE Intenational, 2006.

[2] D. Prescott and J. D. Andrews. A comparison of modelling approaches for the Time-Limited Dispatch (TLD) of aircraft. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 220, 9-20, 2006.

[3] V. Volovoi. Correcting for non-Markovian asymptotic effects using Markovian representation. *ArXiv* 1705.01070 [cs.CE], 2017.

[4] D. R. Cox. The analysis of non-Markovian stochastic processes by the inclusion of supplementary variables. *Proceedings of the Cambridge Philosophical Society* 51, 433-441, 1955.

[5] S. Distefano and K. S. Trivedi. Non-Markovian state-space models in dependability evaluation. *Quality and Reliability Engineering International* 29, 225-239, 2012.

[6] M. Boussemart, T. Bickard, and N. Limnios. Markov decision processes with a constraint on the asymptotic failure rate. *Methodology and Computing in Applied Probability* 3, 199-214, 2001.

[7] A. Birolini, *Reliability Engineering: Theory and Practice*, 5th ed. Berlin Heidelberg: Springer-Verlag, 2007.