CHAPTER 6

PROBABILISTIC R&M PARAMETERS AND REDUNDANCY CALCULATIONS

CONTENTS

1 INTRODUCTION

1.1 This chapter provides a basic introduction to the range of R&M parameters available and the arithmetic for their manipulation. Chapters 2, 3 and 4 discuss the various parameters that can be used, their nature and application. Chapters 5 onwards provide formulae and methods for calculating system R&M parameters given the relevant parameter values for the elements of the system.

1.2 The Reliability Block Diagram (RBD) technique is used throughout this chapter to illustrate the combination of system elements. Readers who are not familiar with this representation are referred to PtCCh30.

1.3 All formulae in this section assume that the system elements are *completely independent in every way*, except for the relationships indicated in the Reliability Block Diagram (RBD). If this is not the case then an equivalent network must be constructed with the dependent aspects separated out. For example consider an exam candidate who takes two pocket calculators of the same design into in an examination. A level of redundancy exists in that there are two items. However a systematic error in the design (hardware or software) will affect both calculators when asked to perform the same calculation. To evaluate the system parameters it is necessary to regard the dependent failures in series (in RBD terms) with the two independent items in parallel.

1.4 Formulae are provided for various categories of system / mission profile. The main division is between operation without repair and operation with repair. For systems without repair the parameters of interest are the system reliability (probability of operating for the whole mission / survival) and the Mean Time To [first] Failure (MTTF). Systems that are repaired during a mission are considered in the steady state (it is assumed that the system has been deployed for a sufficient period so that any dependency of its Availability or MTBF on time has been passed). In this case the parameters of interest are the System Availability, the Mean Time Between Failures (MTBF) and the Mean Time To Repair (MTTR), or other maintainability parameter.

1.5 In general, all items are assumed to be active. That is, operating unless failed. The exception is standby redundancy; this is best handled by computer simulation, but where a simple analytical result is available it has been given.

1.6 The results in this leaflet are based on two fundamental rules for combining probabilities:

a) if A and B are two independent events with probabilities P(A) and P(B) of occurring, then the probability P(AB) that both events will occur is the product:

$$P(AB) = P(A).P(B)$$

b) if two events A and B are mutually exclusive so that when one occurs the other cannot occur, the probability that either A or B will occur is:

$$P(AB) = P(A) + P(B)$$

Clearly these may be extended to any number of events.

1.7 The following particular notations and terminology are used in this leaflet:

a) $\prod_{1}^{N} y_i$ is used to denote $y_1 . y_2 . y_3 . \ldots . y_N$

b) M/N is used to denote that in a redundant group of N items, at least M items must be failure free for the group to be considered up.

c) The descriptor 'Equal Blocks' denotes that all relevant parameters (e.g. failure rate) used in the calculations are identical for each item or block in a group. 'Unequal Blocks' means that each item has its own different values.

2 RELIABILITY PARAMETERS

2.1 Reliability can either be defined as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to perform under given conditions for a given time interval whilst as a performance measure it is the probability of being able to perform as required under given conditions for the time interval.

2.2 Various levels of reliability can be defined for an item to cover differing levels of degradation in performance. Failure that renders the item inoperable or non mission worthy are typically defined as mission reliability whereas failure that renders only minor degradation to performance but which will require a maintenance action to be performed at some point in the future are typically defined as basic reliability. It would be usual to expect that a mission reliability requirement would be much higher than a basic reliability requirement.

2.3 To put this into context, the failure of an interior light on a family motor car may be considered a minor nuisance by the user, particularly when getting in and out of the car in the dark but would not render the car inoperable and would most likely be considered a basic failure. However failure of the fuel or water pump would render the car inoperable and would thus most likely be considered as a mission failure.

2.4 Mission and Basic are two of the descriptors that can be applied to reliability, but many others exist too, including, but not limited to Storage, Dormant, Major, and Critical. Whatever descriptors are chosen to be applied for the item that is under consideration it is imperative that the level of degradation or definition(s) of those failure descriptors are included within the specification to ensure everyone associated with that item has a clear and unambiguous understanding of the term.

2.5 Reliability can be specified in a number of different ways and whilst no one way can be considered as best to cover any circumstance, some methods can be less appropriate than others under certain conditions.

2.6 The most common, and probably most recognised, method of specifying reliability is to quote it as a mean value using a term such as MTBF for a repairable item or MTTF for a non repairable item. The values specified should be those that achieve the users' minimum operating requirement and should be commensurate with any availability requirement that has been defined. It is important to recognise that any requirement specified in this way is only a mean value and it should be expected that significant numbers of the population will fail before the mean time is reached, thus specifying a 200 hour MTBF to support an operating requirement of 200 hours will result in failure. It should also be noted that that specifying a mean value without any supporting information is of no benefit to the items being purchased. Consideration must be given to whether the ‘time’ is based on hours of operation, calendar time or some transformation based on known factors such as take offs and landings for an aircraft, distance for a vehicle or number of firings for a gun. It is also necessary to ensure that any mean value is clearly supported by a usage profile.

2.7 Reliability can also be specified as a probability of success, with or without an associated specified operating time. The requirement for a one shot device, typically a missile, would be specified as a probability of success without a time qualification as the user wants assurance that when that item is used it will operate successfully against its predefined usage profile. An item that would be expected to repeat similar or differing usage profiles many times, a vehicle for example, would be specified with a time qualification where the time qualification is equal to the length of the mission.

2.8 All of the example requirements above are of a quantitative nature, i.e. can be specified and measured in a numerical way, but it is also possible to specify requirements in a qualitative way, i.e. relating to the quality of the item. For reliability this type of requirement often relates to the design of the item, examples of which are below:

a. Single Point of Failure - The item shall be designed such that no single fault can cause a mission or safety critical failure within it.

b. Path Separation – The item shall be designed such that redundant parts within the item are kept independent by ensuring that cables, power supplies and signal routes have well defined separate paths.

2.9 However reliability is specified, it is imperative that failure definitions relevant to each level of reliability are included.

2.10 As described in the section on availability later, it is important to remember that a separate reliability requirement may be required when contracting for availability or capability.

2.11 Reliability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly where the technology and design solution of the final item are not known. In these instances care must be taken to ensure that if a reliability requirement is set it does not dictate the design solution or constrain the design such that innovation or taking advantage of emerging but unproven technology is not considered.

3 MAINTAINABILITY PARAMETERS

3.1 Maintainability can either be defined as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance whilst as a performance measure it is the probability that a given maintenance action, performed under stated conditions and using specified procedures and resources, can be completed within the time interval ($t1$, $t2$) given that the action started at $t = 0$. For the purposes of setting meaningful requirements maintainability is taken to be a performance measure.

3.2 The user is interested in understanding how long it will take to bring an item back to a fully operational condition following any incident. The time will be dependant on two factors: the physical time it takes to diagnose and undertake the repair and the time to obtain the required spares, tools and a maintainer capable of undertaking the work, this later time being referred to as logistic delay and which is mostly outside of the influence or control of the item designer. In order to differentiate between these two differing times it is normal for the diagnose and repair time to be referred to as Active Repair Time (ART) and the time including logistic delay to be referred to as Time To Repair (TTR).

3.3 If every recovery task applicable to the item was timed and plotted then a unique distribution would be generated which could then be defined by a fixed number of points. When setting maintainability requirements it is points on this distribution that the user is required to define, either based on historical knowledge of similar items, expectation of current technology or on the perceived time the user can accept the item not being available. It is usual to specify more than one point on the distribution in order to bound its shape, typical measures being the Mean, Median or percentage points.

3.4 The most common, and probably most readily recognised, method of specifying maintainability is through the use of a mean time, either as a Mean Active Repair Time (MART) or a MTTR. As stated above, simply specifying a mean on its own has very little influence on the design of the item thus it is considered best practice to include at least one percentage point in addition to the mean.

3.5 Specifying two or more percentage point times for maintainability requirements requires the item designers to consider such things as access to cabinets, ease of removal of parts and ability to diagnose a malfunctioning item in a reasonable time. It is normal to specify a percentage point towards the top end of the distribution such that either 90% or 95% of all repairs shall be completed by the specified time. In conjunction with either a Mean time, or possibly a time for 50% of all repairs to be complete this defines the approximate shape of the repair time distribution. If the item is heavily dependant on software then it may be applicable to set a lower percentage point time within which all software restarts shall be accomplished.

3.6 There are occasions, particularly in a performance based contract, where it may be applicable to set a maximum time by which all actions or activities shall be completed. Contractual penalties may then be applied to any activity that is not completed by the required time. Care needs to be taken in setting such limits to ensure that it is not so wide that it has an adverse effect on operation of the item and that is not so narrow that the supplier has very little chance of meeting the time.

3.7 Maintainability requirements if set during the early stages of the life cycle can be used to influence the design in terms of its maintainability before design decisions have been made. This would be done to ensure that that the distribution relating to any of the mean values outlined above are not adversely skewed by a single, or group of repair activities. This would typically be done by setting a maximum time (M_{Max}) which no repair should be expected to exceed under normal circumstances taking account only of those factors which are under the control of the designer.

3.8 As an example consider an item, housed in a container and mounted on a large structure, access to which is gained by removing one of the covers of that container. How the covers are attached can have a significant influence on the time it takes to carry out any repair activity that is required by the item. If it is held on by 25 non captive bolts that have to be removed and replaced using only a spanner, the time taken to gain access to the container will be significantly longer than if it is held on by a similar number of captive bolts or quick release fastenings.

3.9 In this instance an M_{Max} requirement could influence the choice of fittings that are used, although the time requirement may have to considered and possibly traded off against the cost of the fastening devices and the requirement for any special tools to operate them.

3.10 The requirements defined above are all of a quantitative nature, but maintainability can also be defined in a qualitative way. Some examples of qualitative requirements are given below:

a. The item shall not contain any fixing device that can not be removed using a number 2 cross head screw driver available from any commercial tool stockist.

b. The item shall be designed such that any operator can conduct the regular checks required without specialist knowledge or training.

c. The item shall be such that all items the user is required to inspect or top up on a regular basis shall be immediately obvious.

3.11 Maintainability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly where the technology and design solution of the final item are not known. In these instances care must be taken to ensure that if a maintainability requirement is set it does not dictate the design such that innovation or taking advantage of emerging but unproven technology is not considered.

4 AVAILABILITY PARAMETERS

4.1 Availability is defined as ‘ability to be in a state to perform as required’ and is a measure of the time the item is in an operable state when compared to elapsed calendar time so in its simplest form can be represented mathematically by the formula

$$\frac{Uptime}{Totaltime} \quad \text{or} \quad \frac{Uptime}{Uptime + Downtime}$$

4.2 As defence contracting moves from the traditional approach using organic support towards performance based contracts, Availability is becoming the most commonly used characteristic when defining dependability requirements. As will be shown later on there are differing types of availability, some of which are easy to define and calculate values for and others which, whilst easy to define, are much harder to calculate or measure values for. There are also many ways to break down and specify availability be it for an individual part within an item, the whole item or a number of items either at the fleet level or at some operational unit level.

4.3 Care must be taken when specifying availability to ensure that the achieved level of availability actually delivers the capability that the user anticipated. No availability requirement can ever be 100% as failure will always occur at some point in time and whilst the design can be such that most failures can be mitigated through redundancy or alternate methods of service provision, the cost of mitigating against those 1 in 100,000 events soon rises to unacceptable levels, thus it is normal to have to accept some downtime, however small that may be. To ensure that capability is not compromised to an unacceptable level during these outages, the down time should be bounded by specifying the length of time the capability can be unavailable for and how often the capability can be unavailable in a calendar period.

4.4 Taking the provision of a 'network' as an example, the user has specified that it has to be available for 99.8% of the time. In a calendar year of 365 days this allows for the network to be unavailable for 17.5 hours but the requirement as it stands puts no constraints around how that down time is accrued. At one extreme the network could be down for 17.5 hours once during the calendar year which for a communication network would have serious consequences. At the other extreme it could be unavailable for close to 3 minutes every day, which could erode user confidence in the network far more than the one off occurrence previously referred to. In either case the demonstrated level of availability is the same and meets the 99.8% requirement as specified. To get around this it is recommended that the user defines the maximum number of times it is acceptable to have any down time during the year, and when the network is down the maximum time it can take before it is back on line. This would typically be done by setting reliability and maintainability requirements that are commensurate with the availability requirement.

4.5 Having considered the generic concept of availability there are a number of standard definitions that are used depending on what is included within the measured downtime:

a. **Intrinsic availability** is a measure of the availability of the item under ideal conditions, i.e. assuming that a trained maintainer, the spare parts, the tools and test equipment required to undertake corrective maintenance action are all to hand immediately. It is the most common metric that is included in a contract as it only includes the down time associated with carrying out corrective maintenance action activity which is within the control of the design authority and it focuses attention on ensuring that down time due to design is optimised. If intrinsic availability is used within a specification, care must be taken to manage expectations as it is very unlikely that it can be achieved in service because there will always be some logistic delays that will need to be included.

b. **Operational availability** gives a more realistic view of the levels of availability that can be achieved in service because it includes logistic delays but it is more difficult to measure and thus gain a figure that is agreeable to everyone. What truly constitutes logistic delay is a much debated topic with no clear answer and no clear rules that can be applied to every corrective maintenance action. If the piece of test equipment or tool that is required has not been returned to its 'correct location' following a previous activity and it takes 30 minutes to locate it, can this be counted as logistic delay against the item? Putting an operational availability requirement into a contract highlights this type of issue and requires many rules to be written to ensure the requirement is clear and unambiguous.

4.6 Availability requirements for an item can be specified at a number of levels depending on what is required. If the item is part of a fleet it may be appropriate to set an availability requirement for the whole fleet or for differing parts of the fleet, for example vehicles are often split into operational and training fleets with the operational fleet having a higher availability requirement than the training fleet. It may be that the item itself has an availability requirement or it may be beneficial to set an availability requirement for a part of the item, for example the diesel generators in a ship may have an availability requirement as well as the ship itself. Care needs to be taken to ensure that the requirements are commensurate with each other such that the level of availability requested for the higher assembly is not in excess of that which is possible given the lower level availabilities.

4.7 Contracting methods have for some years been moving away from the traditional organic support solutions towards performance based contracts where specified levels of availability or capability are included. In such situations it is necessary to ensure that the data needed to measure the success, or otherwise, of the metrics is specified and a method of collecting it is included. It may be necessary, or preferable, for the collected data to be fed into an agreed model for the assessment against the requirements particularly if provision is wide spread or against a large number of assets.

4.8 Whatever the requirement, it is imperative to ensure that what is offered / contracted for is fully understood and commensurate with what is required. It is not uncommon in a performance based contract for there to be a number / range of exclusions which, if not fully understood, can have significant impact on what the user is expecting. As an example, when contracting for an air vehicle, the engines are often part of a separate contract as can be such things as wheels and tyres, certain electronic items and even spare parts which have not been demanded in the preceding few years. Similarly failure modes and mechanisms that have not, or can not be, predicted such as corrosion or tyre puncture are often outside of the contractual terms and will require to be costed and contracted for separately.

4.9 Availability can be a good parameter to define at any stage of procurement from early pre-concept up to and including utilisation and support. As has been shown in the preceding paragraphs care should be taken to ensure that the characteristics which have the greatest impact on availability are also more closely defined as the item matures. In pre-concept and concept stages it may be reasonable to only specify a top level availability requirement to ensure that operational needs can be met, but as the design matures, and the usage requirements become clearer, it becomes more and more important to ensure that downtime is bounded so that it does not have a significant impact on operational requirements.

5 RELIABILITY CALCULATIONS FOR MISSIONS WITHOUT REPAIR

5.1 General

5.1.1 This Section addresses the calculation of the system reliability (R_S) where the reliability of each element is known. The i^{th} item in the system is assumed to have known reliability R_i.

5.1.2 The expressions addressed in this paragraph are summarised in Tables 1 and 2.

5.1.3 In principle, these expressions can be used where the failure of elements is not constant with time or the Reliability relates to different periods of time. Where constancy with time can not be assumed then much care is needed to ensure that appropriate values, or values relating to consistent periods of time, are combined.

5.2 Series System

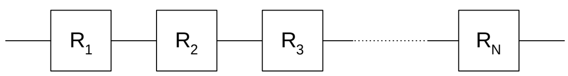


Figure 1: RBD for a Series System of n Items

5.2.1 The probability of survival of the system is the probability that all items survive.

Thus: $R_S = R_1 \cdot R_2 \cdot R_3 \cdot \ldots \cdot R_N$

$$R_S = \prod_{1}^{N} R_i \qquad \text{Equation 1}$$

When the R_i are all equal (to R say), then:

$$R_S = R^N \qquad \text{Equation 2}$$

5.3 Active Parallel Redundancy

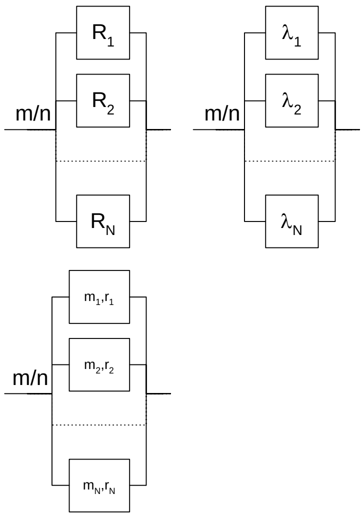


Figure 2: RBD for an Active Parallel Redundancy System of n Items

5.3.1 The redundant group is considered up when at least m out of the n items are up. In general, it is simpler to analyse this system on the basis of probability of system failure (P_f); R_s is then obtained as $1 – P_f$. This is illustrated in the following paragraphs.

5.3.2 When M = 1. The system is only failed when all items are failed. The probability of an individual item failing is $(1 - R_i)$, so that P_f, the probability that all fail, is:

$$P_f = \prod_{1}^{N} (1 - R_i)$$

Since $R_S = 1 – P_f$:

$$R_S = 1 - \prod_{1}^{N} (1 - R_i) \qquad \text{Equation 3}$$

When all the R_i are equal (to R say) then:

$$R_S = 1 – (1 – R_i)^N \qquad \text{Equation 4}$$

5.3.3 When M ≠ 1. To analyse this situation it is necessary to list all possible up (or down) states of the system, calculate the probability of occurrence of each state, and sum these to produce R_S (or P_f). If $m > ½(n+1)$ there are fewer down states than up states and it is therefore more convenient to calculate R_s as $1 – P_f$; otherwise calculating R_s directly is easier.

5.3.4 When M = 2, N = 3. The process is illustrated below for m = 2, n = 3, the simplest possible case. Since m is not less than ½(n+1), R_S will be calculated.

The system survives when:

either (i) items 1 and 2 and 3 survive;

or (ii) items 1 and 2 survive and 3 fails;

or (iii) items 1 and 3 survive and 2 fails;

or (iv) items 2 and 3 survive and 1 fails.

If the probability of (i) occurring is denoted by P(i), etc, then:

$P(i) = R_1 . R_2 . R_3$

$P(ii) = R_1 . R_2 . (1 - R_3)$.

$P(iii) = R_1 . R_3 . (1 - R_2)$.

$P(iv) = R_2 . R_3 . (1 - R_1)$.

Since none of these four 'events' can occur at the same time, that is they are mutually exclusive, they may be summed to provide the probability of system survival.

Thus: $R_S = P(i) + P(ii) + P(iii) + P(iv)$

Therefore, for M = 2, N = 3:

$$R_S = R_1R_2R_3 + R_1R_2(1 - R_3) + R_1R_3(1 - R_2) + R_2R_3(1 - R_1) \qquad \text{Equation 5}$$

5.3.5 Clearly, if M and N are large the expression for R_S will become extremely cumbersome. In these cases computer assistance is desirable and programs do exist for such analyses.

5.3.6 When all R_i are equal to R say, the situation is simpler. The above example reduces to:

$$R_S = R^3 + 3R^2(1 - R) \qquad \text{Equation 6}$$

5.3.7 For General M, N and Equal Blocks. For general M and N, but equal R_i, the expression for R_S is the sum of the first (N + 1 - M) terms of the Binomial expansion of $(R - Q)^N$, where Q = 1 - R. (Alternatively it is 1 minus the last M terms of this expansion.). This is because each term in the Binomial expansion gives the probability of a particular up (or down) state of the system.

Thus: $$R_S = \sum_{0}^{N-M} {}_N C_i R^{(N-i)}(1-R)^i \qquad \text{Equation 7}$$

where: $${}_n C_i = \frac{n!}{(n-1)!.i!}$$

Alternatively, calculate R_S as $1 - P_f$ (P_f is given by the last M terms of the expansion), as follows:

$$R_S = 1 - \sum_{N-M+1}^{N} {}_N C_i R^{(N-i)}(1-R)^i \qquad \text{Equation 8}$$

This equation has fewer terms than the previous equation when M < ½(n + 1).

5.4 Standby Redundancy

5.4.1 Reliability expressions for Standby Redundancy rapidly become cumbersome as the number of items increase and readers are referred to Basovsky[1] for a fuller discussion. However, expressions are quoted in Table 1 for the condition when:

a) Active failure rates are assumed to be constant; and

b) Passive and switching failure rates are assumed to be zero.

5.5 Systems with both Series and Redundant Items

5.5.1 In general a system will comprise a mixture of items in series and redundancy configurations. This poses no problems in cases where the items can be formed into independent groups, each of which is soluble using the formulae given in Sections 5.2 to 5.4. The reliability of each can be calculated using the methods described previously, and the groups are then further grouped successively until finally R_S can be calculated. The process is best explained by means of an example, see Leaflet 2.

5.6 Systems with Complex Redundancy

5.6.1 Not all systems will consist of groups of series items or active parallel items. For example, consider the RBD below:

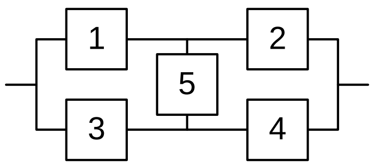


Figure 3: Complex Redundancy Group

An indication of how this system can be tackled is given in the next paragraph, but in general it is recommended that the analysis of systems like this, and more complex ones, should not be attempted without the aid of a computer program or a specialist mathematician.

5.6.2 The Reliability (R_S) of the RBD in Figure 3 can be calculated with the aid of a modified version of Bayes theorem. This states that:

$$P(B) = P(A) \,.\, P(B \mid A) + P(\overline{A}) \,.\, P(B \mid \overline{A}) \qquad \text{Equation 9}$$

Where: P(x) means 'the probability of event x';

P(x | y) means 'the probability of event x given event y';

B is the desired event (system survives in this case);

$\overline{A}$ means event A does not occur.

5.6.3 To solve Figure 3, choose event A to be 'block 5 survives'.

If block 5 survives it is required that the group below survives for the system to survive.

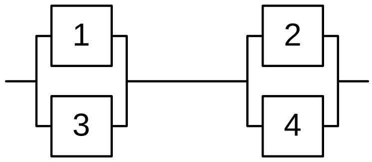


Figure 4: RBD with Block 5 Up

The probability of survival, say R_α, is calculable using previous methods.

5.6.4 If block 5 fails it is required that the group below survives for the system to survive.

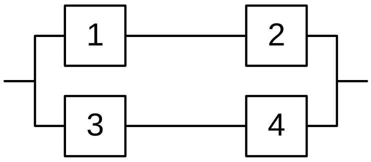


Figure 5: RBD with Block 5 Down

Again this reliability, say R_β, is calculable using previous methods.

5.6.5 Now put

$$P(B) = R_s,\ P(A) = R_5, \text{ and } P(\overline{A}) = 1 - R_5,$$

Thus: $R_S = R_5 . R_\alpha + (1 - R_5) . R_\beta$ Equation 10

5.6.6 Other types of RBD configuration can be analysed by suitable choice of 'event A' in the Bayes theorem.

5.6.7 In principle a diagram of any complexity can be analysed. For example, if Figure 4 or Figure 5 could not have been analysed using previous methods, further application of the Bayes Theorem to this sub-group could have been made. The process can be repeated indefinitely.

6 MTTF CALCULATIONS FOR MISSIONS WITHOUT REPAIR

6.1 General

6.1.1 The formulae presented in this Section, unlike those in the previous Section, apply only to items with constant failure rate, i.e. where the probability of failure by a given time is described by the negative exponential distribution. Where this is not so, it will usually be necessary to use models to analyse the system, or numerical methods of integration.

6.1.2 Thus it will be assumed throughout this Section that the reliability function for item i is of the form:

$$R_i(t) = e^{-\lambda_i t}$$

6.1.3 It is stated here, without proof, that the Mean Time To Failure (MTTF) of a system whose reliability function is $R_S(t)$ is:

$$MTTF = \int_0^\infty R(t).dt \qquad \text{Equation 11}$$

and $$MTTF_i = \frac{1}{\lambda_s} \qquad \text{Equation 12}$$

6.1.4 The expressions derived in this Section are summarised in Tables 3 and 4.

6.2 Series System

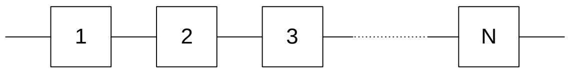


Figure 6: RBD for a Series System of n Items

From Equation 1 (and being explicit that R is time related):

$$R_S(t) = \prod_{i=1}^{N} R_i(t)$$
$$= \prod_{i=1}^{N} e^{-\lambda_i t}$$
$$= e^{-(\lambda_1 + \lambda_2 + \ldots + \lambda_N)}$$

□ $R_S(t) = e^{-\lambda_S t}$ where $\lambda_S = \sum_1^N \lambda_i$

From Equation 12:

$$\text{System MTTF} = \frac{1}{\lambda_S} = \frac{1}{\sum_1^N \lambda_i}$$ Equation 13

6.3 Active Parallel Redundancy

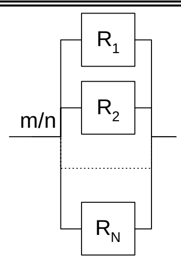


Figure 7: RBD for an Active Parallel Redundancy System of n Items

6.3.1 To obtain system MTTF in this case it is necessary to apply the Equation 11 to Equations 3 to 8. It is not proposed to attempt this in general terms here as expressions will become cumbersome. The technique will be demonstrated by applying it to a particular example for each equation.

6.3.2 For m = 1, Non-Identical Items

From Equation 3:

$$R_S(t) = 1 - \prod_{1}^{N} (1 - R_i(t))$$

If n = 2, $R_S(t) = 1 - ((1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t}))$

$$= e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t} \qquad \text{Equation 14}$$

Using Equations 11 and 12:

$$\text{System MTTF} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_1 + \lambda_2} \qquad \text{Equation 15}$$

It should be noted that it is *not* possible to express Equation 14 in the form $R_S(t) = e^{-\lambda_s t}$, where λ_S is some function of only λ_1 and λ_2. Thus, the system times to failure do *not* comply with the negative exponential distribution, and this is true for all parallel redundant groups, not just the 1/2 group discussed here.

If N = 3, $R_S(t) = 1 - ((1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t})(1 - e^{-\lambda_3 t}))$

$$= e^{-\lambda_1 t} + e^{-\lambda_2 t} + e^{-\lambda_3 t} - e^{-(\lambda_1 + \lambda_2)t} - e^{-(\lambda_2 + \lambda_3)t} - e^{-(\lambda_3 + \lambda_1)t} + e^{-(\lambda_1 + \lambda_2 + \lambda_3)t}$$

$$\text{System MTTF} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} - \frac{1}{\lambda_2 + \lambda_3} - \frac{1}{\lambda_3 + \lambda_1} + \frac{1}{\lambda_1 + \lambda_2 + \lambda_3} \qquad \text{Equation 16}$$

6.3.3 When M = 2, N = 3, Non-Identical Items

From Equation 5:

$$R_S(t) = R_1R_2R_3 + R_1R_2 - R_1R_2R_3 + R_1R_3 - R_1R_2R_3 + R_2R_3 - R_1R_2R_3$$

$$= R_1R2 + R_1R_3 + R_2R_3 - 2R_1R_2R_3$$

It is not necessary to write out the exponential form of the equation each time. Clearly, applying the integral (Equation 11) to a product of reliabilities simply results in the reciprocal of the sum of the λ's in the product.

Thus: $$\text{System MTTF} = \frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_2 + \lambda_3} + \frac{1}{\lambda_3 + \lambda_1} - \frac{2}{\lambda_1 + \lambda_2 + \lambda_3} \qquad \text{Equation 17}$$

6.3.4 Table 4 provides the expressions for System MTTF for some of the more common redundancy groups, assuming identical items in the group, derived in a similar manner to the above, but using Equations 7 and 8. For example, with N = 3 and M = 2.

From Equation 7:

$$R_S = R^3 + 3R^2(1-R)$$

and Equation 11:

$$\lambda_S = \int_0^\infty R_S.dt$$

Then: $$\lambda_S = \int_0^\infty R^3 + 3R^2(1-R).dt$$

$$\lambda_S = \int_0^\infty R^3 + 3R^2(1-R).dt$$

$$= \int_0^\infty e^{-3\lambda t} + 3e^{-2\lambda t}\left(1 - e^{-\lambda t}\right).dt$$

$$= \int_0^\infty \left(3e^{-2\lambda t} - 2e^{-3\lambda t}\right)dt$$

$$= \left[-\frac{3e^{-2\lambda t}}{2\lambda} + \frac{2e^{-3\lambda t}}{3\lambda}\right]_0^\infty$$

$$= -0 + 0 + \frac{3}{2\lambda} - \frac{2}{3\lambda}$$

$$= \frac{5}{6\lambda}$$

6.3.5 It is interesting to note from Table 4 that the cost effectiveness of active redundancy falls off rapidly as n is increased, for non-repairable systems. For example, the MTTF for the 1/2 case is $1.5/\lambda$, whereas for the 1/6 case MTTF only increases to $2.45/\lambda$.

6.4 Standby Redundancy

6.4.1 Expressions are not derived here but Table 3 lists some of the simpler cases for situations where the switching failure rate and non-operating failure rates are zero. Where this is not the case then more detailed modelling is needed (see PtCCh30).

6.4.2 From Table 3, it can be seen that the cost effectiveness of standby redundancy is much better than for active redundancy in non-repairable systems.

6.5 MTTF for Complex Systems

6.5.1 The analysis cannot easily be extended to more complex groupings, as was done for reliability in Sections 5.5 and 5.6, because a redundancy group does not exhibit a constant failure rate (see Section 6.3.2). Therefore, successive groupings cannot be made, as the basic assumption of constant failure rates of items in a group will then be violated. In such circumstances computer models are recommended.

7 Availability Of Repairable Systems In The Steady State

7.1 General

7.1.1 For this analysis it is assumed that an availability (A_i) can be associated with the i^{th} block of the system, and that system availability is A_S. The main constraining assumption in the analysis of repairable systems in this chapter is that there is no queuing for repair.

7.1.2 Availability can be thought of as the probability that an item or system is up at any random instant in time. (The probability that it is down is 1 minus the availability.) Like reliability it is a probability, and it can be manipulated in the same way as reliabilities were in Section 5. For example, the availability of a system comprising N series items is the probability that all are up at any time.

Thus: $$A_S = \prod_{i=1}^{N} A_i$$ Equation 18

7.1.3 For a 1/N active redundant group, the group is unavailable when all items are unavailable.

Thus: $$A_S = 1 - \prod_{i=1}^{N} (1 - A_i)$$ Equation 19

7.1.4 Therefore, with the exception of the standby redundancy analysis in 5.4, Steady State Availability analysis is identical to the Reliability analysis in Section 5. It is only necessary to replace R_S with A_S, and R_i with A_i.

7.2 Standby Redundancy

7.2.1 To calculate the availability of a standby redundancy group it will normally be necessary to use computer models. However, for the 1/N case where: items are identical, passive and switching failure rates are zero, and item failures are distributed exponentially with respect to their active time, then A_S can be calculated from:

$$A_s = \frac{m_S}{m_S + r_S}$$ Equation 20

where: m_S is system MTBF as given in Table 5, and

r_S is system MTTR as given in Table 7.

8 MTBF And MTTR Of Repairable Systems In The Steady State

8.1 General

8.1.1 In Section 8 the symbols m and r will be used to denote the Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) respectively. It is *not* necessary to assume that time between failure and time to repair are distributed exponentially for the results to be valid, although it *is* assumed that m and r are constant in the sense that they do not vary with time. Steady State Availability is related to m and r by the expression:

$$A = \frac{m}{m + r} \qquad \text{Equation 21}$$

Some expressions are simpler if the notation $\lambda = 1/m$, $\mu = 1/r$ is adopted.

8.1.2 Because the distributions of failure and repair times do not affect the calculation, the method of successive groupings described in Section 5.6 may be applied to complex systems[2].

8.1.3 Expressions for system MTBF and MTTR are derived similarly to those in previous sections. The results are summarised in Tables 5 to 7.

8.2 System MTBF

8.2.1 Series Items

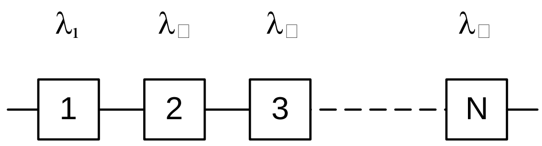


Figure 8: RBD for Series Items

8.2.2 The situation here is exactly similar to the case discussed in 6.2. Repair is not relevant to the system MTBF since the system goes down when any of the blocks go down.

Thus: $\lambda_S = \lambda_1 + \lambda_2 + \lambda_3 + \ldots + \lambda_N$

i.e. $$\text{System MTBF}(m_S) = \frac{1}{\sum_{1}^{N} \lambda_i} \qquad \text{Equation 22}$$

(cf Equation 13)

8.2.3 Active and Standby Redundancy. Expressions are quoted in Table 5 for most situations that will arise in practice. Also, to facilitate calculations for active redundancy, Table 6 lists the expressions for m_s for various values of M and N when items are identical.

8.3 System MTTR

8.3.1 Expressions for computing system MTTR are given in Table 7. Care is needed in using these expressions. The user needs to be clear what each term is referring to. Use of the nomenclature ‘mean time to restore’ or ‘mean down time’ is more correct than ‘mean time to repair’ at the system level. Repairs to specific items of equipment take just as long as in a non-redundant system. However, with redundancy, the systems only fails when a second (or higher numbered) item fails while the first fault is being repaired (or awaiting repair).

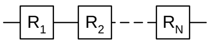
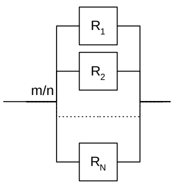
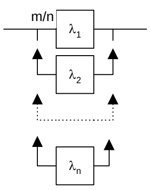
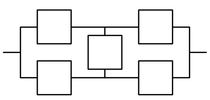
Reliability Block Diagram	**System Reliability (R_S)**	**Conditions**
 Series System	$R_S = R1.R2.R3.....R_N = \prod_1^N R_i$	N Unequal Blocks
	$R_S = R^N$	N Equal Blocks
 Active Redundancy	$R_S = 1 - \prod_{i=1}^{N} (1 - R_i)$	Unequal Blocks M = 1, N general
	$R_S = R_1R_2R_3 + R_1R_2(1-R_3) + R_2R_3(1-R_1) + R_3R_1(1-R_2)$	Unequal Blocks M = 2, N = 3
	For M and N general, Section 5.3.3 to 5.3.5	Unequal Blocks
	$R_S = (1-R)^N$	Equal Blocks M = 1, N general
	$R_S = \sum_{i=0}^{N-M} {}_NC_i R^{(N-i)}(1-R)^i$ or alternatively $R_S = 1 - P_F$ $= 1 - \sum_{i=N-M}^{N} {}_NC_i R^{(N-i)}(1-R)^i$ where: ${}_NC_i = \frac{N!}{i!(N-i)!i!}$	Equal Blocks M & N general see also Table 2 for N □6.
 Standby Redundancy	For Standby Redundancy: $R_s(t)$ is probability of system surviving time t. Block active times to failure are negative exponentially distributed. Passive failure rates & switching failure rates are assumed to be zero.	
	$R_s(t) = \frac{\lambda_2 e^{-\lambda_1 t}}{\lambda_2 - \lambda_1} + \frac{\lambda_1 e^{-\lambda_2 t}}{\lambda_1 - \lambda_2}$	Unequal Blocks M = 1, N = 2
	$R_s(t) = \frac{\lambda_2\lambda_3 e^{-\lambda_1 t}}{(\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1)} + \frac{\lambda_1\lambda_3 e^{-\lambda_2 t}}{(\lambda_1 - \lambda_2)(\lambda_3 - \lambda_2)} + \frac{\lambda_1\lambda_2 e^{-\lambda_3 t}}{(\lambda_1 - \lambda_3)(\lambda_2 - \lambda_3)}$	Unequal Blocks M = 1, N = 3
	$R_s = e^{-M\lambda t} \sum_{i=0}^{N-M} \frac{(M\lambda t)^i}{i}$	Equal Blocks M & N general
	For systems like this, and others which are not like the above, see Section 5.6.	
The reliability of systems which have RBDs which comprise combinations of the above block groups may be calculated by successive groupings, as explained in Section 5.6..		

Table 1: Reliability Expressions for Missions Without Repair

N \ M	1	2	3	4	5
2	$1 - Q^2$				
3	$1 - Q^3$	$R^3 + 3R^2Q$			
4	$1 - Q^4$	$1 – (4RQ^3 + Q^4)$	$R^4 + 4R^3Q$		
5	$1 - Q^5$	$1 – (5RQ^4 + Q^5)$	$R^5 + 5R^4Q + 10R^3Q^2$	$R^5 + 5R^4Q$	
6	$1 - Q^6$	$1 – (6RQ^5 + Q^6)$	$1 – (15R^2Q^4 + 6RQ^5 + Q^6)$	$R^6 + 6R^5Q + 15R^4Q^2$	$R^6 + 6R^5Q$
$Q = 1 – R$. The above expressions contain the least possible number of terms					

Table 2: Reliability Expressions for M/N Active Redundancy (Equal Blocks, No Repair)

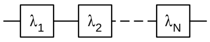
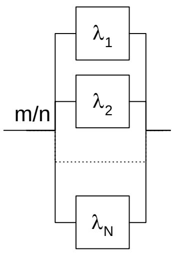
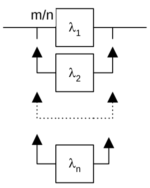
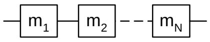
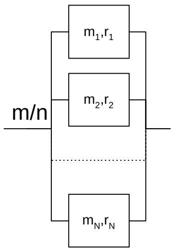
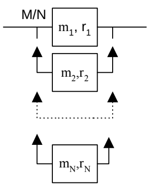
Reliability Block Diagram	System MTTF	Conditions
 Series System	$\text{MTTF} = \frac{1}{\lambda_S} = \frac{1}{\sum_1^N \lambda_i}$	N Unequal Blocks
	$\text{MTTF} = \frac{1}{\lambda_S} = \frac{1}{N\lambda}$	N Equal Blocks
 Active Redundancy	$\text{MTTF} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_1 + \lambda_2}$	Unequal Blocks M = 1, N = 2
	$\text{MTTF} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \frac{1}{\lambda_1 + \lambda_2} - \frac{1}{\lambda_2 + \lambda_3} - \frac{1}{\lambda_3 + \lambda_1} + \frac{1}{\lambda_1 + \lambda_2 + \lambda_3}$	Unequal Blocks M = 1, N = 3
	$\text{MTTF} = \frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \frac{1}{\lambda_2 + \lambda_3} - \frac{2}{\lambda_1 + \lambda_2 + \lambda_3}$	Unequal Blocks M = 2, N = 3
	$\text{MTTF} = \frac{1}{\lambda}\left(\frac{1}{N} + \frac{1}{N-1} + \frac{1}{N-2} \cdots \frac{1}{M}\right)$	Equal Blocks M & N general, see also Table 4 for N □6.
 Standby Redundancy	$\text{MTTF} = \sum_1^N \frac{1}{\lambda_i} = \sum_1^N m_i \qquad \left(m_i = \frac{1}{\lambda_i}\right)$	Unequal Blocks M = 1, N = general
	$\text{MTTF} = \frac{N}{\lambda} = Nm$	Equal Blocks, M = 1, N general Note 3
	$MTTF = \frac{(N - M + 1)}{M\lambda} = \frac{(N - M + 1)}{M} m$	Equal Blocks, M , N = general Note 1 & 2
	$\text{MTTF} = \frac{1}{\lambda_1 + \lambda_2}\left(1 + \frac{\lambda_1}{\lambda_2 + \lambda_3} + \frac{\lambda_2}{\lambda_1 + \lambda_3}\right)$	Equal Blocks, M , N = general Note 1 & 2.
	Standby Redundancy Notes: 1. Negative exponential distributions. 2. Passive failure rates & switching failure rates are assumed to be zero. 3. Any failure time distribution.	
For more complex groupings, successive groupings are not permitted in order to calculate system MTTF (cf Table 1), since the assumptions of constant failure rates will be violated when redundancy is involved, as explained in Section 6.5.		

Table 3 MTTF Expressions for Missions Without Repair (cont.)

N \ M	1	2	3	4	5
2	$\frac{3}{2\lambda}$				
3	$\frac{11}{6\lambda}$	$\frac{5}{6\lambda}$			
4	$\frac{25}{12\lambda}$	$\frac{13}{12\lambda}$	$\frac{7}{12\lambda}$		
5	$\frac{137}{60\lambda}$	$\frac{77}{60\lambda}$	$\frac{47}{60\lambda}$	$\frac{9}{20\lambda}$	
6	$\frac{147}{60\lambda}$	$\frac{29}{20\lambda}$	$\frac{57}{60\lambda}$	$\frac{37}{60\lambda}$	$\frac{11}{30\lambda}$

Table 4: MTTF Expressions for M/N Active Redundancy (Equal Blocks, No Repair)

Reliability Block Diagram	System MTBF (m_S)	Conditions
	$m_s = \dfrac{1}{\sum_{i=1}^{N} \lambda_i}$	N Unequal Blocks
Series System	$m_S = \dfrac{1}{N\lambda} = \dfrac{m}{N}$	N Equal Blocks, each with MTBF = m
	$m_s = \dfrac{A_s}{A_1 Q_2 \lambda_1 + A_2 Q_1 \lambda_2}$ $(Q = 1 - A)$	Unequal Blocks M = 1, N = 2
	$m_s = \dfrac{A_s}{Q_1 Q_2 A_3 \lambda_3 + Q_1 A_2 Q_3 \lambda_2 + A_1 Q_2 Q_3 \lambda_3}$	Unequal Blocks M = 1, N = 3
	$m_s = \dfrac{A_s}{K}$ where $K = A_1 A_2 Q_3 (\lambda_1 + \lambda_2) + A_1 A_3 Q_2 (\lambda_1 + \lambda_3) + A_2 A_3 Q_3 (\lambda_2 + \lambda_3)$	Unequal Blocks M = 2, N = 3
Active Redundancy	$m_S = \dfrac{A_S m}{M \, {}_N C_M A^M Q^{N-M}}$ $\left({}_N C_M = \dfrac{N!}{(N-M)!.M!} \right)$	Equal Blocks M & N general, see also Table 6 for N [illegible]6.
 Standby Redundancy	$m_S = \sum_{i=2}^{N} \dfrac{m^{i-1} (N-1)!}{r^{i-2} (N+1-i)!}$	Equal Blocks 1/N case, each block having exponential distributed active failure and repair times. Passive and switching failure rates assumed to be zero.

More complex systems than the above can be analysed using the successive grouping technique described in Section 5.6.

The distribution of failure and repair times is not constrained, except for Standby Redundancy.

Key: m and r denote MTBF and MTTR respectively.

$$\lambda = \frac{1}{m} \qquad \mu = \frac{1}{r}$$

Table 5: MTBF Expressions for Repairable Systems in the Steady State (cont.)

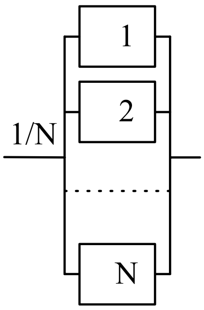
N \ M	1	2	3	4	5
2	$\frac{A_s m}{2AQ}$				
3	$\frac{A_s m}{3AQ^2}$	$\frac{A_s m}{6A^2Q}$			
4	$\frac{A_s m}{4AQ^3}$	$\frac{A_s m}{12A^2Q^2}$	$\frac{A_s m}{12A^3Q}$		
5	$\frac{A_s m}{5AQ^4}$	$\frac{A_s m}{20A^2Q^3}$	$\frac{A_s m}{30A^3Q^2}$	$\frac{A_s m}{20A^4Q}$	
6	$\frac{A_s m}{6AQ^5}$	$\frac{A_s m}{30A^2Q^4}$	$\frac{A_s m}{60A^3Q^3}$	$\frac{A_s m}{60A^4Q^2}$	$\frac{A_s m}{30A^5Q}$
Q = 1 – A. A calculated as in Section 7.					

Table 6: MTBF Expressions for M/N Active Redundancy (Equal Blocks, Repairable)

<table>
<tr><th>Reliability Block Diagram</th><th>System MTTR (r_s)</th><th>Condition</th></tr>
<tr><td colspan="3">In general it is recommended that System MTTR (r_S) be calculated from the expression:

$$r_S = \frac{m_S(1 - A_S)}{A_S}$$

where A_S and m_S are calculated as described in Section 7 and Table 5 respectively.

However, for 1/n active or standby redundancy r_S may be calculated as below:</td></tr>
<tr><td rowspan="2">

Active or Standby Redundancy</td><td>$$r_S = \frac{1}{\sum_{1}^{N} \frac{1}{r_i}}$$</td><td>Unequal Blocks,

MTTR of i^{th} block= r_i</td></tr>
<tr><td>$$r_S = \frac{r}{N}$$</td><td>Equal Block,
each with MTTR = r</td></tr>
</table>

Table 7: MTTR Expressions for Repairable Systems in the Steady State

LEAFLET 6/0

REFERENCES

1. Basovsky I: *Reliability Theory and Practice*. Prentice-Hall International

2. Mathew A E: *ANSAR – A Systems Analysis Design Tool, NRC 3/9*. National Reliability Conference 21-23 September 1977 at the University of Nottingham

3. Reliability, Maintainability & Availability Parameters taken from NATO Standard ADMP-01, Guidance for Developing Dependability Requirements, Edition 1, Version 1 dated December 2013

Intentional blank page

LEAFLET 6/1

EXAMPLE OF ACTIVE PARALLEL REDUNDANCY WITH N EQUAL BLOCKS

Problem: A missile launcher can hold 6 missiles. The probability that an individual missile is non-failed at missile launch is 90%. What is the probability (R_s) that at least 4 are non-failed when an operational demand occurs?

Solution: In this case m = 4, n = 6, R = 0.9.

Since m < ½(n+1) use

$$R_s = \sum_{i=0}^{n-m} {}_nC_i R^{(n-i)}(1-R)^i$$

Then $R_s = {}_6C_0R^6 + {}_6C_1R^5(1 - R) + {}_6C_2R^4(1 - R)^2$

$= (0.9)^6 + 6(0.9)^5(0.1) + 6 . 5 . ½ . (0.9)^4(0.1)^2$

(Note: $x^0 = 1$, $0! = 1$)

∴ $R_S = 0.531441 + 0.354294 + 0.098415$

$= 0.984$, or 98.4%.

To facilitate this type of calculation, Table 2 of PtDCh6 lists the expressions for R_s for various values of m and n when items have identical reliability (R).

Intentional blank page

LEAFLET 6/2

EXAMPLE WITH BOTH SERIES AND REDUNDANT ITEMS

Problem: Find R_S, the system reliability for the RBD in Figure 9.

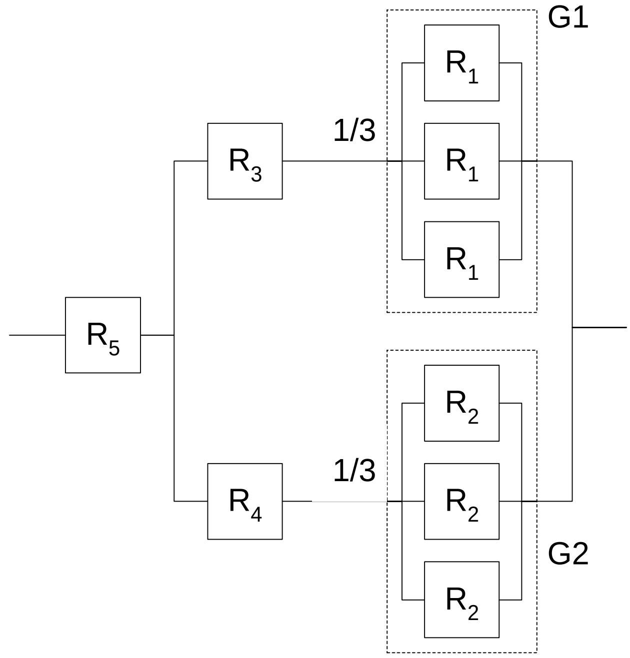


Figure 9: System RBD

Solution. Let Gi denote group i, and R_{Gi} denote the reliability of Group Gi.

Then: $R_{G1} = 1 - (1 - R_1)^3$

$R_{G2} = 1 - (1 - R_2)^3$

The system is now reduced to:

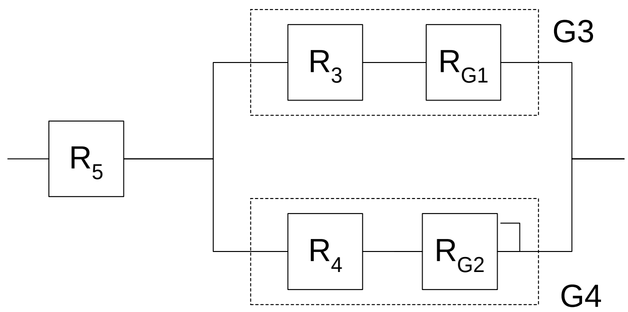


Figure 10: First Reduction

Then: $R_{G3} = R_3 . R_{G1}$

$R_{G4} = R_4 . R_{G2}$

The system is now reduced to:

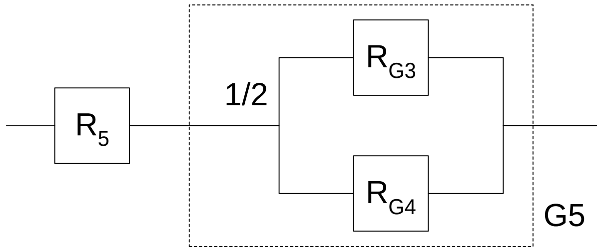


Figure 11: Second Reduction

Then: $R_{G5} = 1 - (1 - R_{G3})(1 - R_{G4})$

The system is now reduced to:

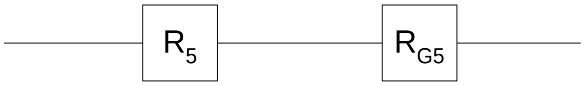


Figure 12: Third Reduction

Then: $R_s = R_5 . R_{G5}$

The reduction process could incorporate complex redundancy groups as described in section 5.6 of PDCh6. Block 5, for example, in the above RBD might itself be a complex group.

LEAFLET 6/3

MODELLING ADDITIONAL FUNCTIONALITY OF SYSTEMS

9 INTRODUCTION

9.1 This Leaflet provides a discussion of a process which may be performed in order to provide an indication of a System's Availability when additional functionality is added to a core system that has previously been analysed. The generic structure explained in this note for adding additional functionality to a model uses the example of a new function (System B), being added to the model of an existing System (System A).

9.2 The process defined is limited to situations where the additional functionality can be reasonably modelled as a separate serial element in the reliability block diagram for the new system. As such the following implicit assumptions are made:

a) No elements of the additional and existing systems are common to both systems;

b) The interface between the two systems does not involve any fusion of system elements or alteration to the internal configurations of the systems with respect to redundancy.

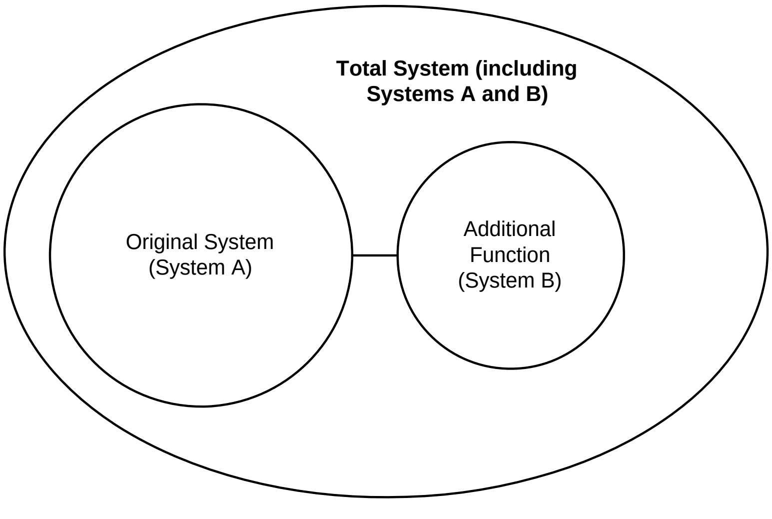


Figure 13: Additional Equipment Added to a System

10 DEFINITIONS

A_T = Availability of System - Availability of the total system (systems A and B above) including the original system and the additional function.

A_O = Availability of Original System - Availability of the old system (system A above) including the original system.

A_N = Availability of Additional Function - Availability of the additional function (system B above).

11 REQUIREMENTS OF A MODELLING STUDY

11.1 The requirements of a modelling study are generally to predict the effect on the System Availability upon the incorporation of an additional function, and compare the findings with those obtained for the initial study. Additionally it is often desirable to determine the Availability of the System (A_T) incorporating the additional function for differing Availabilities of the new function (A_N).

12 MODELLING BASICS

12.1 Modellers using availability modelling packages generally seek to predict the overall Operational Availability, Reliability and Maintainability (R&M) of a System. This may be performed for a previously modelled System which provides a new facility or function by the incorporation of Additional Equipment into the model.

12.2 Studies are often performed to provide an estimate of the likely system Availability for a given function of the System (e.g. transmission of a telecommunications signal from a specific point to another point).

12.3 Reports associated with a modelling study should include the following as precursory information for the System to be modelled.

a) Overview and project history/background - This should include a brief description or overview of the System being modelled and the current status of the project (feasibility, development etc.). The project description should state all of the sub systems/functions which comprise the system and should also identify the latest report issue covered by this description.

b) Additional function description - This should be compiled for each of the Additional Functions to be added to the Original System and should be defined including the Additional Function's composition, description and any assumptions concerning the Additional Function.

c) Assumed base Availability of the equipment supporting the Additional Function - R&M assumptions concerning the additional equipment or Additional Functions should be stated together with the sources of data, including any supporting information where appropriate.

d) Assumptions about the repairability of any element as it applies to restoration of the defined element. This should include details of any Maintenance policies or assumptions regarding the restoration of the element (e.g. spares, repair teams, Repairable at Sea/Non-Repairable at Sea etc.)

e) Any additional assumptions relating to the Total System.

f) Dependencies between the Additional Function and the Original System.

13 LIMITING THE DETAIL OF THE ASSUMPTIONS AND DATA

13.1 It is considered that the documentation should not replicate all of the assumptions, input data and outputs contained within the original report. Reasons to support this approach include:

a) The assumptions paper should primarily be a justification and discussion of the assumptions concerned with the Additional Function and its impact on the Original System.

b) If the documentation attempts to duplicate too much of the modelling input data, new assumptions and data may be overlooked and the report may become overly complex and hence will not be used properly, leading to it being of little value to the interested parties.

14 AIMS

14.1 The principal aims of an Availability Modelling study for the System are generally:

a) To compare the Availability of the Original System with that expected to be achieved by the Total System including the Additional Function;

b) Through a series of sensitivity studies, to predict the effect of the Additional Function on the whole System Availability for different R&M characteristics of the Additional Function.

15 ASSUMPTIONS

15.1 All additional assumptions should be noted and the expected impact of any Additional Function on the Original System investigated thoroughly.

15.2 Care should be taken in modelling the additional software and hardware of the system. In particular, the integration of additional software into the rest of the system should be examined. For example, if a failure of the Additional Function is isolated from the rest of the system, this may only result in a degraded service, whereas, if failure of any Additional Function reduces the Total System capability, the effects could be extensive.

15.3 A number of models should be run with differing failure details of those parts (hardware) and elements (software) of the system which contribute to provision of the Additional Function in order to assess the impact of the Additional Function's Availability on the Total System Availability.

16 BASE CASE MODEL

16.1 A Base Case model should be run for the Total System in order to predict the expected Availability. For this model the R&M data relating to the Additional Function should be estimated as accurately as possible. The Base Case scenario should be used to provide a general feel for the potential loss of Availability of the Total System, incorporating equipment performing the Additional Function, compared to the Availability of the Original System that did not including equipment performing the new function.

17 'SENSITIVITY' STUDIES

17.1 In order to provide the most effective solution, a series of sensitivity studies should be performed to analyse the change in Availability of the total System, with the change in Availability of the Additional Function.

17.2 The overall Availability of the System is dependent on the Availability of the initial System (without equipment performing the Additional Function) and upon the Additional Function (equipment performing the Additional Function). The Availability of the Total System including the Additional Function is given by:

$A_T = A_O * A_N$

where A_T = Availability of System

A_O = Availability of Original System

A_N = Availability of Additional Function

17.3 For any system comprising of Original System and Additional Function, assuming the Availability of the Original System is set, the Availability of the Total System will tend to a particular value depending on the relative Availabilities of the Original and Additional Functions (A_O and A_N) as shown below:

If $A_N >> A_O$ then $A_T \rightarrow A_O$

If $A_N << A_O$ then $A_T \rightarrow A_N$

If $A_N \cong A_O$ then $A_T \cong (A_O)^2$ or $(A_N)^2$

17.4 Figure 2 shows how the Availability of a System (A_T) may vary with the Availability of the Additional Equipment (A_N), assuming a constant Availability of the Original System (A_O).

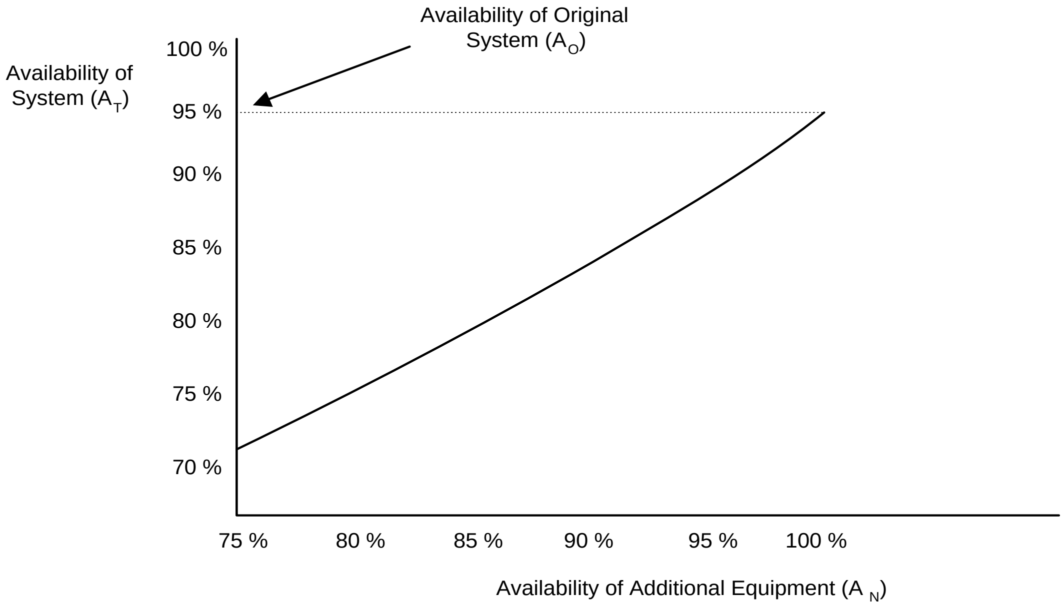


Figure 14: System Availability Against Additional Function Availability

17.5 The most cost effective solution will be given by the incorporation of the Additional Function that provides the lowest Total System Through Life Costs (TLC) that will still allow the Total System to meet the R&M requirements. It is therefore important that the requirements of the Additional Function are clearly defined and the Additional Function offers the most cost effective solution for a tolerable Availability of the Total System.

17.6 Generally, for a given function or system the initial cost of equipment increases with increased Availability or Reliability. However, equipment performing the Additional Function should be assessed on predicted Total Life Costs (TLC) in order to determine the 'real' cost of the equipment rather than just the initial purchase price of the equipment.

18 CONCLUSIONS

18.1 The report should focus on the change in Availability of the System for differing R&M characteristics of the Additional Function.

18.2 All assumptions regarding the integration of the new equipment should be highlighted in the report and the integration of additional software into the rest of the system should be examined, including compatibility with existing software.

18.3 The incorporation of any equipment added to the Original System should be assessed. Care should be taken to fully understand the effects of the integration of any Additional Equipment and its effects on the Original System.

18.4 Where possible the critical elements / function of the Additional Equipment should be identified, including non-repairable failures as these will have the biggest impact on the Availability of the Additional Function.

18.5 Planned additional software should be fully tested before implementation and the effects of software failure examined.

Intentionally blank page