Influence of Fault-Detection and Switching Mechanisms on the Reliability of Stand-By Systems

by

Jacques Losq

July 1975

Technical Report No. 75

This work was supported by National Science Foundation Grant GJ-40286 and l'Institut de Recherche en Informatique et Automatique (IRIA, France).

DIGITAL SYSTEMS LABORATORY

STANFORD ELECTRONICS LABORATORIES

STANFORD UNIVERSITY . STANFORD, CALIFORNIA

INFLUENCE OF FAULT-DETECTION AND SWITCHING MECHANISMS ON THE RELIABILITY OF STAND-BY SYSTEMS

by

Jacques Losq

July 1975

Technical Report No. 75

Digital Systems Laboratory
Department of Electrical Engineering   Department of Computer Science
Stanford University
Stanford, California

This work was supported by National Science Foundation Grant GJ-40286 and **l'Institut** de Recherche en Informatique et Automatique (IRIA, France).

Paper submitted to a special issue on fault-tolerant computing of IEEE Tansactions on Computers.

Digital Systems Laboratory
Department of Electrical Engineering   Department of Computer Science
Stanford University
Stanford, California

Technical Report No. 75

July 1975

INFLUENCE OF FAULT-DETECTION AND SWITCHING MECHANISMS ON THE RELIABILITY OF STAND-BY SYSTEMS

Jacques Losq

ABSTRACT

This paper concerns the reliability of stand-by systems when switch reliability is taken into account. It is assumed that failures obey a Poisson distribution for modules and switches. A very detailed method is given to model stand-by systems. Several cases are investigated: ideal systems, real systems with fault-detection mechanisms that can detect any module error and systems for which the fault-detection mechanisms detect only sane of the module errors. The reliability versus time curves are determined for each value of the number of spares. It is shown that the best number of spares increases as the length of the mission increases. . -Systems with extremely short mission time have the best reliability when they have only one spare. The limit when the number of spares increases is the reliability obtained with simplex systems. Whatever the number of spares is, the reliability of stand-by systems goes to zero as time goes to infinity. For a given mission time, it is possible to determine the best number of spares and the best possible reliability. For a given reliability, it is possible to compute the number of spares that gives the longest mission time. These models can be used to determine whether or not there exists a stand-by system that meets the requirements of a given reliability and a given mission time. If such stand-by system exists, its characteristics (minimum number of spares and reliability) can be derived.

Index terms: Reliability modeling, stand-by redundancy, switches and fault-detection mechanisms, dormancy factor, coverage factor, reliability, mission time.

A - INTRODUCTION

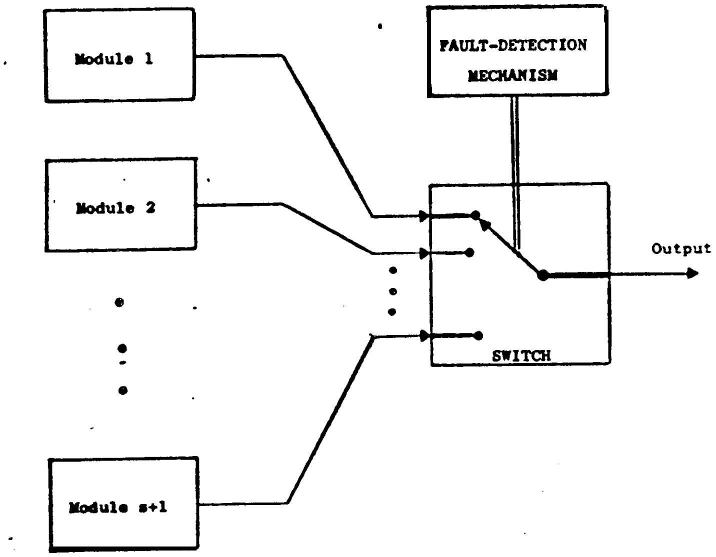
Many physical systems are provided with spare parts to replace failed parts.. The use of spares is called Stand-by or Sparing Redundancy, [1,7] Spares need not be exact replicas of the parts they replace . The equivalence need only be **functionnal** .

Systems using spares need a mechanism to detect the occurrence of errors . in the active parts . They also need a mechanism to implement the replacement process . These mechanisms are called error-detection and switching mechanisms (often referred to simply as switches) . Replacement processes for stand-by systems are simple . As soon as an error is detected at the output of an active module, this module is switched off and replaced by a spare . If the spare is faulty, it will be switched off immediately after its activation and replaced by another spare . There is no need for roll-back if the spares are active (or if the modules are combinational machines) and if error are detected as soon as they occur .

Stand-by redundancy is used to increase the reliability of systems . If spares have the same reliability, R, as the active module, stand-by systems with s spares (Fig. 1) have a reliability $R' = 1 - (1-R)^{s+1}$. This reliability function is obtained under the assumption that fault-detection and switching mechanisms are perfect . The reliability of such stand-by systems is always greater than the reliability of simplex systems $(R' > R)$. The reliability R' is an increasing function of the number of spares (Fig. 2) . As the number of spares increases, the reliability approaches 1 . When spare failure rates are less than active failure rates, stand-by reliability is even greater than R' .

However, fault-detection and switching mechanisms are not fault-free . The goal of this study is to determine the exact effects of failures inside fault-detection and switching mechanisms on the reliability of systems using spares .

In order to evaluate the effects of failures in the switches, a very detailed analysis of stand-by systems will be made . First, the method that has been introduced by Carter et al. [4] will be shortly reviewed . Then, using detailed analysis, theoretical limitations of stand-by systems will be derived . Application of the model to real systems will permit the determination of the relation between reliability, mission time and best number of spares .



1. Stand-by system with s spares ,

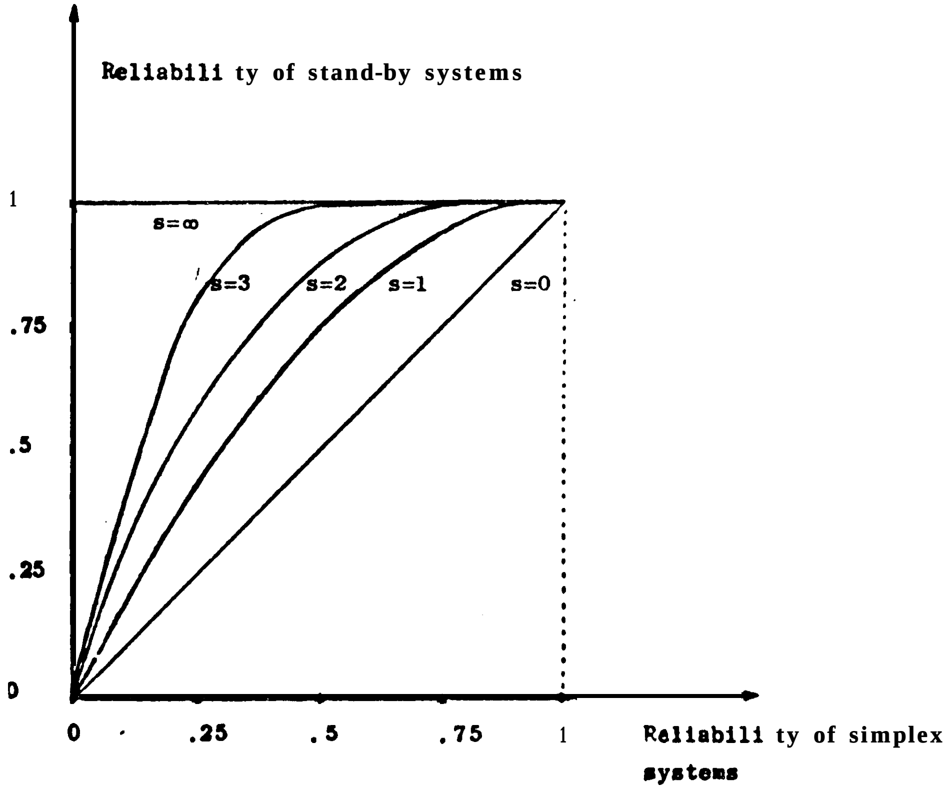


Fig. 2 . Stand-by system reliability as a function of simplex reliability .

A-l MULTIPLE OUTPUT STAND-BY SYSTEMS

Fig. 1 represents a stand-by system with only one output . However, most of the actual I.C. chips realize multiple output functions . The major problem with application of redundancy to multiple output systems arises when sparing is used . In this case, it is necessary to define more precisely the word **"spare"** . Physically, spares will always be modules . However, for the switching mechanisms, spares can be seen as modules (multiple output functions) or as parts of modules (the parts that realize single output functions) . So, there are basically two types of sparing redundancy for multiple output systems . In the first type, referred as Type I, fault-detection is done at the level of modules and a faulty module is replaced by a spare module (Fig. 3) . This solution is the simplest one and also the less reliable because modules with only one faulty output lead will be disconnected and replaced by spares . In the second type, referred as Type II, detection of faults is done at the level of single output functions and only single output functions (not modules as in Type I) are replaced (Fig. 4) . This solution provides the maximum increase in reliability, but switching mechanisms are more complex .

Modeling multiple output stand-by systems is analogous to modeling single output stand-by systems . Type I systems perform correctly as long as there is one fault-free module . Type II systems fail only when every module is subject to a failure that affects the same output function in each of the modules . So, Type I systems can be modeled as single output stand-by systems while Type II systems with n output leads are modeled as n parallel single output stand-by systems . However, corrections must be made to take care of the interdependence between the reliability of the different output leads of a module (for example, gate sharing between single output function realizations) .

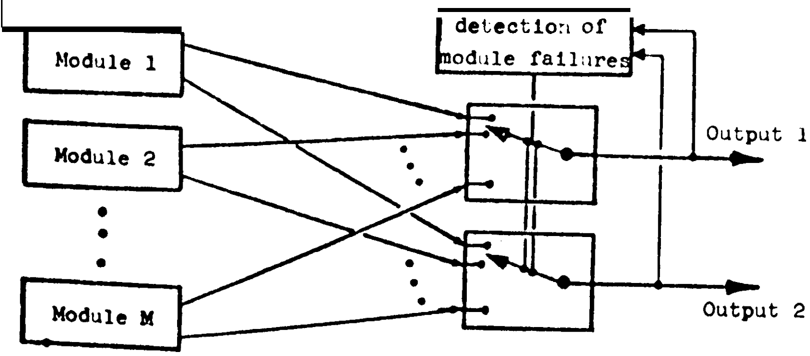


Fig. 3 . Two **output** rtand-by ● yrtem of **type I** .

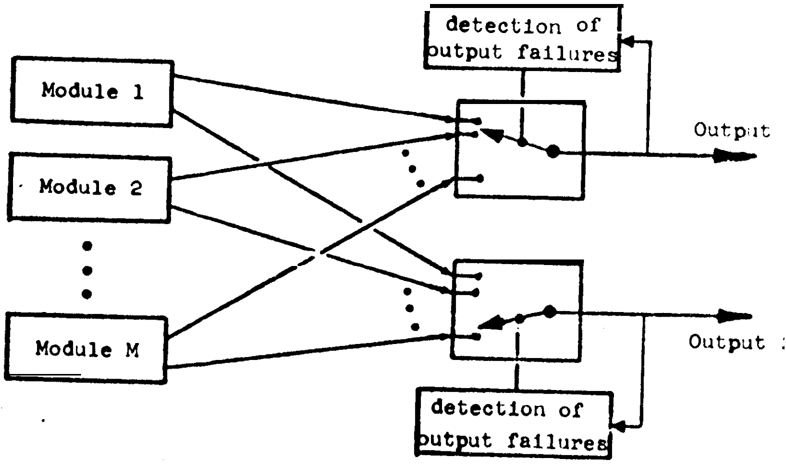


Fig. 4 ., Two output rtand-by **systems of type II** .

B - COVERAGE FACTORS - CARTER ET AL. METHOD

B-l Introduction

The notion of coverage was introduced by W.G. Bouricius, W.C. Carter and P.R. Schneider,[4] , and has been developed by several authors [5], [6] .

The coverage factor of a redundant system using spares is defined as the probability that the system recovers from a failure given that a failure exists . Coverage factors are usually denoted by the letter c :

c = Probability (the system recovers | a failure occurs)

In the method developed by Carter et al., stand-by systems are modeled by a renewal process with a fixedprobability, c, of success associated with each replacement of a failed module by a spare . This leads to the basic equation :

$$ {}_{c}R_{s}^{q}(\lambda,\mu,T) = {}_{c}R_{s-1}^{q}(\lambda,\mu,T) + \int_{0}^{T} -\frac{\partial({}_{1}R_{s-1}^{q}(\lambda,\mu,u))}{\partial u} .c^{s}.\exp(-\mu.u) $$

$$.\exp(-q.\lambda.(T-u)).du $$

in which : ${}_{c}R_{s}^{q}(\lambda,\mu,T)$ is the reliability, at time T, of systems with q+s modules (q active modules and s spares),

$\exp(-\mu.T)$ is the reliability, at time T, of a spare, [9]

$\exp(-\lambda.T)$ is the reliability, at time T, of an active module .

This equation can be solved by induction on s :

$$ {}_{c}R_{s}^{q}(\lambda,\mu,T) = \exp(-q.\lambda.T). \sum_{k=0}^{s} \binom{\frac{q.\lambda}{\mu} +k-1}{k} .c^{k}.\left[1-\exp(-\mu.T)\right]^{k} $$

B-2 Failure rate λ independent of the number of spares

If the failure rates λ and μ are fixed(independent of the parameter s), the reliability of stand-by systems is always an increasing function of the number of spares, However, even with an infinite number of spares, the reliability is still **stricly** less than 1 on the time range $\left]0,\infty\right]$ if the coverage factor, c, is less than 1 :

$$\underset{s\to\infty}{\text{Limit}}\ {}_{c}R^{q}_{s}(\lambda,\mu,T) = \exp(-q.\lambda{:}T)\ .\ \left[1 - c.\left(1-\exp(-\mu.T)\right)\right]^{\frac{-q.\lambda}{\mu}}$$

$${}_{c}R^{q}_{s}(\lambda,\mu,T) < \exp(-q.\lambda.T)\ .\ \Big[\exp(-\mu.T)_{\mathrm{I}}^{\frac{-q.\lambda}{\mu}} \quad \text{if } c<1\ .$$

B-3 Failure rate Adependent upon the number of spares

The complexity of the witching mechanism increases with the number of spares . In order to take into account this increase, it is possible to consider that the failure rate λ, **increases** as the number of spares increases . Another possibility is to consider that the coverage factor decreases as the number of spares increases . The first alternative corresponds to :

$$\frac{\partial\lambda}{\partial s} > 0$$

Carter-et al. have **shown**, [2], that there exists a finite best number of spares if the coverage factors are less than 1 and if the derivative of A with respect to **s** is positive (or if c=l and if $\underset{s\to\infty}{\text{Limit}}\ (s+1).T.\frac{\partial\lambda}{\partial s}$ is less or equal to one **)** . Reliability is always limited and the best number of spares, when the mission time approaches zero, is one .

B-4 Coverage factor dependent upon the number of spares

The second alternative to take into account the increase in complexity of the switches is to assume that the coverage factor decreases as the number of spares increases :

$$\frac{\partial c}{\partial s} < 0$$

For every time T there exists a best number of spares (Appendix I) . Systems with very short mission time have the best reliability when they have only one spare .

B-5 Conclusions

This model shows that the reliability of stand-by systems is always limited . It was shown that there exists a best number of spares when one takes into account the dependence between switch complexity and number of spares . However, these last results have been obtained using artificial methods (introducing a dependence between module failure rate and number of spares or between coverage factor and number of spares) . In practice, using this model, it may be extremely difficult to determine the best system for given requirements (uncertainty of $c, \frac{\partial c}{\partial s}$ and $\frac{\partial \lambda}{\partial s}$) . In order to get a more detailed insight for stand-by systems, a more accurate modeling of stand-by systems will be made .

C - DETAILED ANALYSIS OF STAND-BY SYSTEMS

C-l Introduction

Failures inside switches and fault-detection mechanisms should be classified according to the effects they have on systems . Fault-detection mechanisms perform the following function : detection of every occurrence of an error at the outputs of modules . So, failures in fault-detection mechanisms may have two different results . Either the modules are declared faulty when, in fact, they are fault-free, or occurrence of errors won't be detected . The same classification exists for switch failures . Switches deactivate failed modules and activate spares upon command from fault-detection mechanisms . A failure inside a switch will result in a replacement of an active module without command from the fault-detection mechanism or in a no-fulfillment of such a command when it is issued .

It is possible, depending upon practical realizations, for some other classes of failures **to** exist . For example, some failures can cause a spare to be activated when it should not be . However, the two functions realized by switches are very similar. A module is switched off when and only when a spare is switched on . So, it is possible to design switches such that these two functions (activation and deactivation) are performed by the same hardware . In this case, it is very likely that every switch failure will affect both functions .

Because of the similarity between the effects of switch failures and the effects of fault-detector failures, it is possible to lump these failures together and to partition them into two classes . The class of fail-safe failures consists of failures that result in discarding a fault-free module but replacing it by a spare . The failure rate associated with this class will be assumed to be a constant ν_0 . The second class corresponds to the set of unsafe failures . Unsafe failures are the failures which cause a module error to go undetected (or which result in a error being detected but without repair) . The failure rate corresponding to the set of unsafe failures will be assumed to be a constant ν_1 . All the modules will be assumed to have identical error **rate**, λ , when powered (active modules) and μ if kept power-off (inactive spares) .

C-2 Theoretical limitations of stand-by systems

This part is focused on the characteristics of ideal stand-by systems . Failure rate of power-off elements is zero . Power switching is used . Only a very small portion of the complete switch is powered . A design for such stand-by systems is given in Fig. 5 . Each module has its own switch and fault-detection mechanism . This increases reliability because when a module is switched on, its fault-detection mechanism, which is fault-free, is also switched on . The switching strategy is as follows : when the fault-detection mechanism of the active module detects an error, the switch is ordered to switch on the next spare, its switch and fault-detection mechanism and to switch off the faulty module, its fault-detection mechanism and itself . This corresponds to use stand-by redundancy on modules, switches and fault-detection mechanisms . The internal realization of fault-detection mechanisms will not be considered but it will be assumed that fault-detection mechanisms are designed such that they can detect the occurrence of any module error .

The module outputs should be OR-tied to the bus whenever possible . Because this part treats only ideal systems, it will be considered that the modules are OR-tied to the bus (or that the module-bus connection is perfect) . Also, no roll-back will be considered . Switches do not perform any logical operation, they only implement the power switching .

Such stand-by systems can be modeled using Markoff chains (Fig. 6) . The first subscript in the state notation indicates the initial number of spares, while the second subscript indicates the present number of available fault-free spares . States $_sP_i$ correspond to stand-by systems for which no unsafe failure has occurred in the switches and fault-detection mechanisms . The states $_sQ_j$ correspond to stand-by systems for which the active module is fault-free, but its corresponding switch has been subject to an unsafe failure which cancels any subsequent repair of the system . The state $_sF$ corresponds to the failed state .

Laplace transform is very useful to solve such Markoff chains[10$_3$. The Laplace transform of the probability of failure of such a stand-by system with s spares is (Appendix II) :

$$_sF(z) = \frac{\lambda}{z}\left[\frac{\nu_1}{z+\lambda}\sum_{k=1}^{s}\frac{(\lambda+\nu_0)^{k-1}}{(z+\lambda+\nu_0+\nu_1)^k} + \frac{(\lambda+\nu_0)^s}{(z+\lambda).(z+\lambda+\nu_0+\nu_1)^s}\right]$$

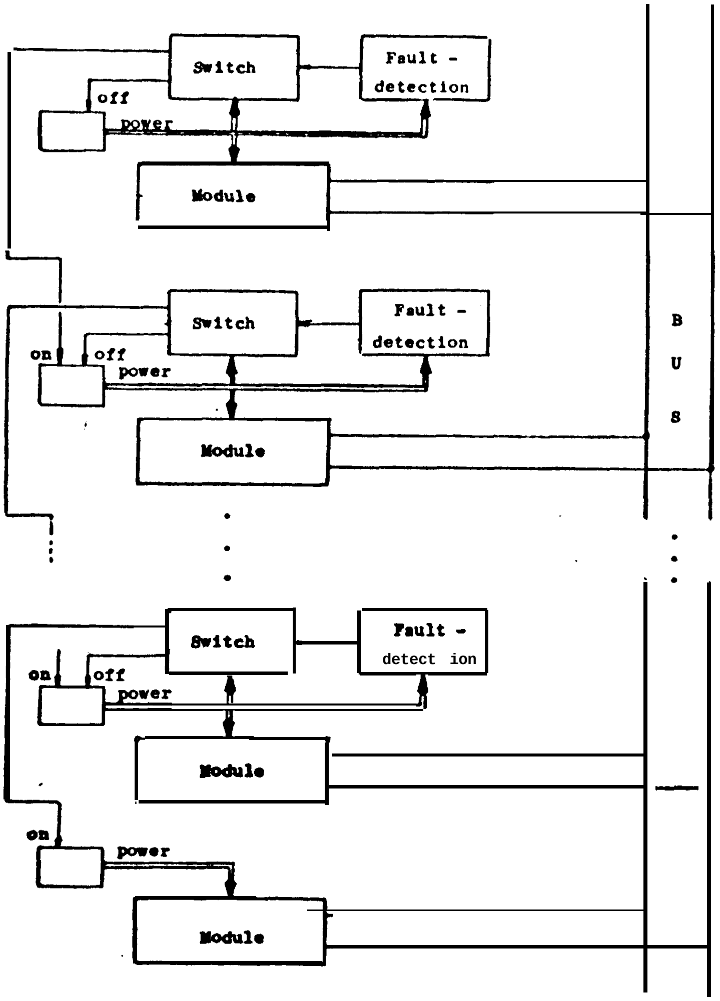


Fig. 5 . Stand-by system with power switching (for modules and switches)

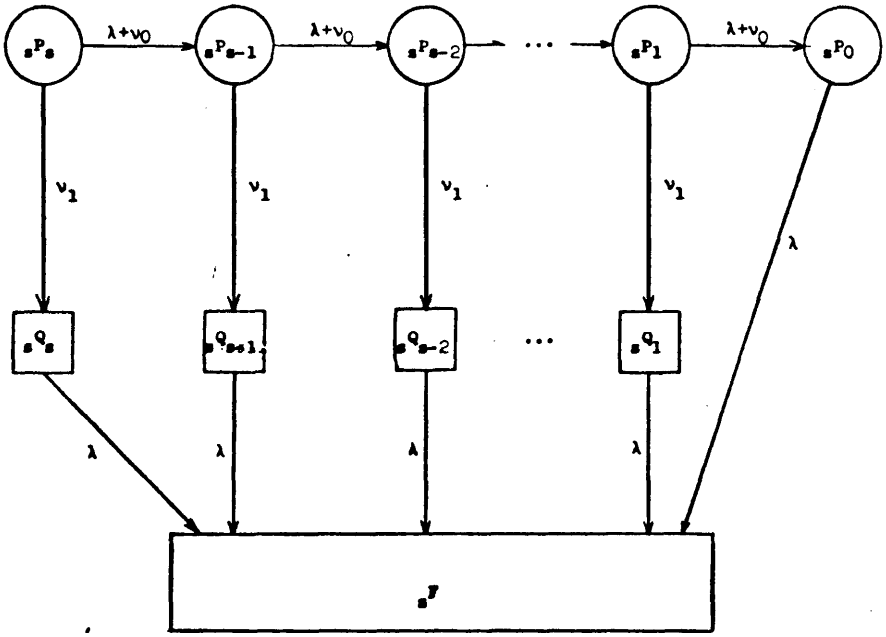


Fig. 6 , Markoff chain for s stand-by system with S pprfect spares , The probability of failure decreases as the number of spares increases :

$$ {}_{s}F(z) - {}_{s+1}F(z) = \frac{\lambda}{z} \cdot \frac{1}{z+\lambda} \cdot \frac{(\lambda+\nu_0)^s}{z+\lambda+\nu_0+\nu_1)^s} \cdot \frac{z}{z+\lambda+\nu_0+\nu_1} $$

The inverse **Laplace** transform of this equation is laways positive because it corresponds to a convolution of positive function in the range $]0,\infty[$.

The **limit of** the reliability of stand-by systems when the number of spares approaches infinity is :

$$ R^*(T) = \frac{1}{\lambda-\nu_1}\left[\lambda.\exp(-\nu_1.T) - \nu_1.\exp(-\lambda.T)\right] $$

This reliability, R*(T), is always less than one for T greater than zero and approaches 0 as T goes to infinity (Fig. 7) . The reliability difference between a stand-by system with infinite number of spares and a stand-by system with **s** spares is :

$$ R^*(T) - {}_{s}R(T) = \frac{1}{(s+1)!} \cdot (\lambda+\nu_0) \cdot \left[\left[\frac{3.F^*(T)}{\lambda.\nu_1}\right]^{\frac{1}{2}}\right]^{s+1} $$

$R+(T) - - {}_{s}R(T)$ of the order of $\dfrac{\left[F^*(T)\right]^{\frac{s+1}{2}}}{(s+1)!}$.

This shows that stand-by systems with small number of spares perform as well as (or very close to) stand-by systems with very large number of spares when they are used in applications requiring high reliability .

When all the switches and fault-detection mechanisms are fail-safe, then reliability approaches one over the whole time range $[0,\infty]$ **as** the number of spares approaches infinity :

$$ {}_{s}R(T) = 1 - \mathcal{L}^{-1}\left[\frac{1}{z} \cdot \frac{\lambda}{z+\lambda} \cdot \frac{(\lambda+\nu_0)^s}{(z+\lambda+\nu_0)^s}\right] > 1 - \frac{\lambda.(\lambda+\nu_0)^s}{(s+1)!} \bullet T^{s+1} \xrightarrow[s\to\infty]{} 1 $$

So, it is possible to state the major limitations inherent to stand-by redundancy . Stand-by systems have always a limited reliability (completely fail-safe switches can not be realized) . For ideal systems, reliability increases as the number of spares increases but the marginal cost of reliability increase is very high .

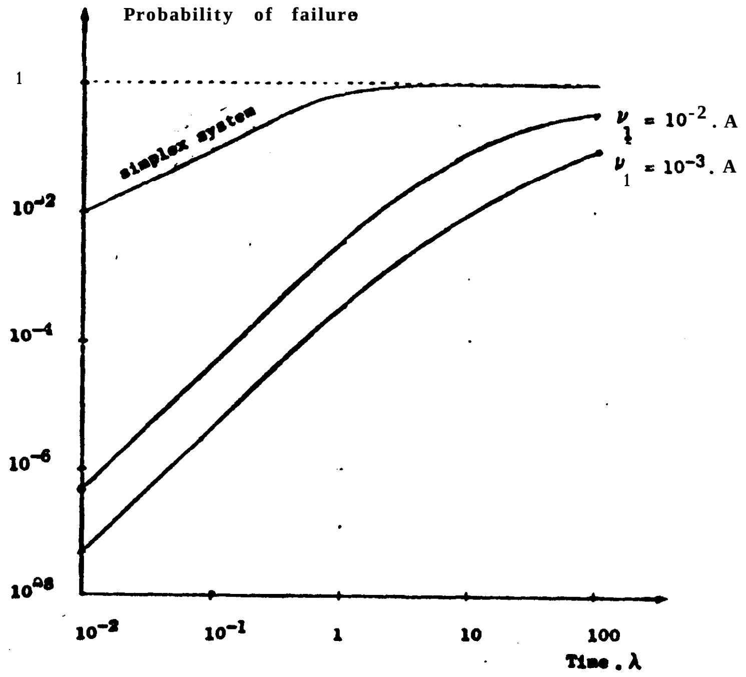


Fig. 7. Probsbllity of failure of stand-by systems with infinite [illegible]

C-3 Characteristics of real stand-by systems

C-3-l Description

The previous section was concerned with ideal systems . This section focuses on more common stand-by systems . The failure rate of unpowered components is generally different from zero . In what follows, it will be assumed that the failure rate of unpowered modules is constant and equal to μ . The ratio of active failure rate to inactive failure rate is called the dormancy factor and will be denoted by k .

Some stand-by systems have only one fault-detection mechanism (Fig. 8) . The major problem that arises in the modeling of such stand-by systems is to determine the interdependence between the reliabilities of the outputs of the fault-detection mechanism . When this interdependence is not known, it is impossible to accurately model these systems . Multiple output fault-detection mechanisms may be such that its outputs are either all correct or all faulty . Stand-by systems with such a fault-detection mechanism perform poorly . Any failure inside the fault-detection mechanism resultsin a system error . For fault-detection with multiple output, interdependence between the output reliabilities decreases the overall system reliability . Thus, it is important to carefully design fault-detection mechanisms to avoid such interdependence . If all the outputs have the same reliability and are independent, then stand-by systems with one multiple output fault-detection mechanism (Fig. 8) are equivalent (on the basis of reliability) to stand-by systems with one fault-detection mechanism for each module (Fig. 9) .

Only stand-by systems with one fault-detection mechanism for each module will be analysed They are equivalent to the most efficient sytems with only one fault-detection mechanism . Furthermore, they are simple, straightforward and the only ones for which detailed analysis is possible .

Power switching will be assumed . The model can be adapted to systems with logic switching (spares are kept powered) . The modules should be OR-tied to the bus whenever possible . When this is not possible, each module bus connection should be controlled by the corresponding fault-detection mechanism . This introduces additional causes of system error.. However, these system failures may be lumped with those introduced by the fault-detection mechanisms . All the switches and fault-detection mechanisms are kept powered at all times . So, a fault-detection mechanismorswitch may fail even after the corresponding module

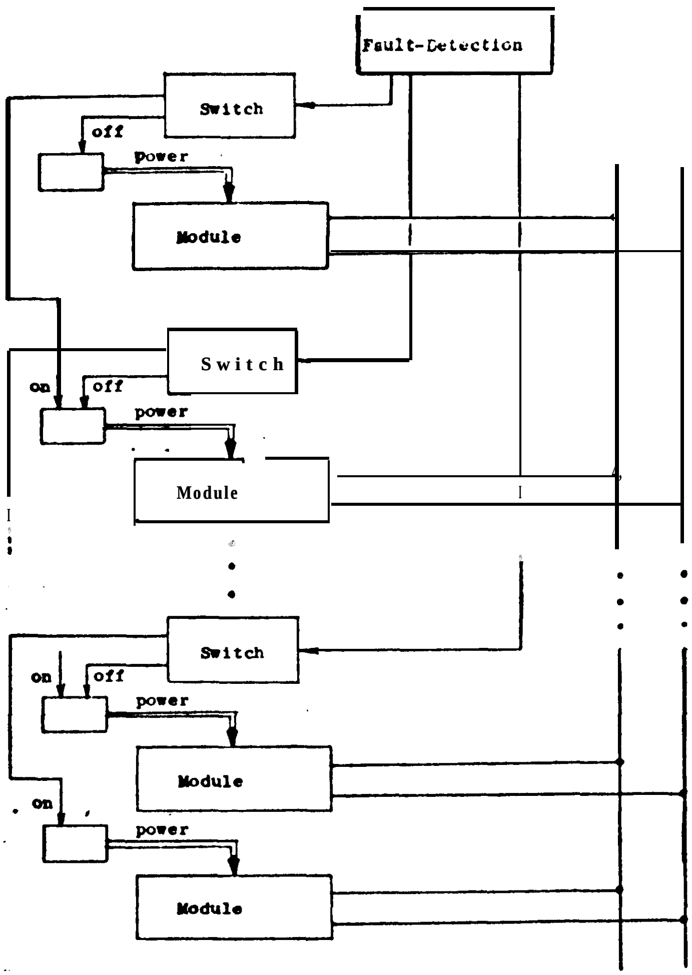


Fig. 8 . Stand-by system with only one fault-detection mechanism

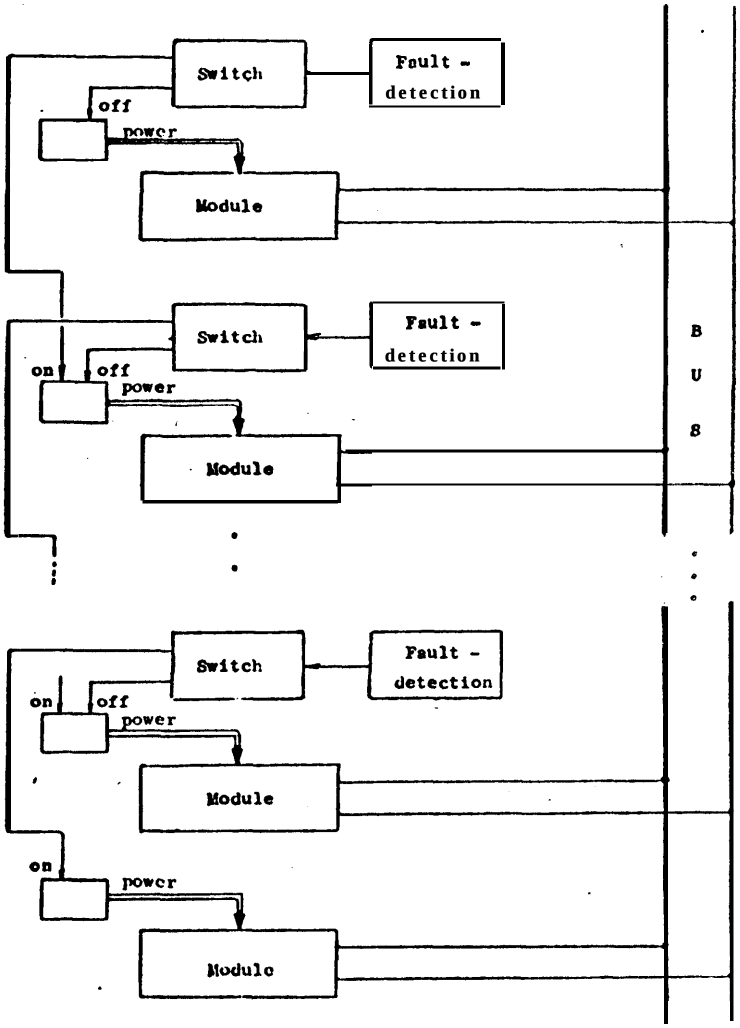


Fig. 9 . Stand-by system with one fault-detection unit for each module .

has been removed . Some of these failures may cause a faulty module to be switched back on . This case of system failure (that can also happen in the module - bus connection) will be taken into account .

C-3-2 Model for real stand-by systems (complete error detection capability)

Stand-by systems as shown in Fig. 9 can be modeled using Markoff chains . The rate of safe (unsafe) failures for each set.switch - fault-detection mechanism is ν_0 (ν_1) . In this part it will be considered that fault-detection mechanisms can detect all the module errors . In a second part, the effect of partial fault-detection will be taken into account .

The states of stand-by systems can be divided into two classes ; the class of states ${}_sP_i$ for which no unsafe failure has occured in the switches, fault-detectors and module-bus connections and the class of states ${}_sQ_i$ for which unsafe failures have occured . The effect of an unsafe failure in the switch of the active module is equivalent to a cancellation of subsequent module-error detection (or repair) . Unsafe failures in switches of fault-free spares result in establishing an uncontrolled module-bus connection . Any subsequent failure of the module will result in a system failure . Unsafe failures in the switches of failed modules result in reestablishing a module-bus connection which causes' immediate system failure . Safe failures are equivalent to module failures followed by proper repair . The effect of safe switch failures can be reduced to a decrease of the number of fault-free available spares .

The Markoff chain for real stand-by systems with complete fault-detection capability is given in Fig. 10 . The states ${}_sF_1$, ${}_sF_2$ and ${}_sF_3$ represent the failed states . ${}_sF_1$ corresponds to system failures due to spare exhaustion . ${}_sF_2$ corresponds to system failures due to occurrence of a failure in a module with a failed switch (unsafe switch failure) . State ${}_sF_3$ regroups the failures due to occurence of unsafe failures in the switches of failed modules .

The transition probability between state ${}_sP_{i+1}$ and state ${}_sP_i$ is equal to $\lambda+(i+1)\mu+(i+1)\nu_0$ (the last spare does not have a spare) . The transition probability between state ${}_sP_i$ and state ${}_sQ_i$ is equal to $i.\nu_1$ (probability of unsafe failure in switches corresponding to fault-free modules) . The transition probability between state ${}_sP_i$ and state ${}_sF_3$is equal to $(s-i).\nu_1$ (unsafe failures in switches corresponding to failed modules) . The transition probability between state ${}_sQ_i$ and state ${}_sF_2$ is λ (probability of an error in a module that has a failed switch) .

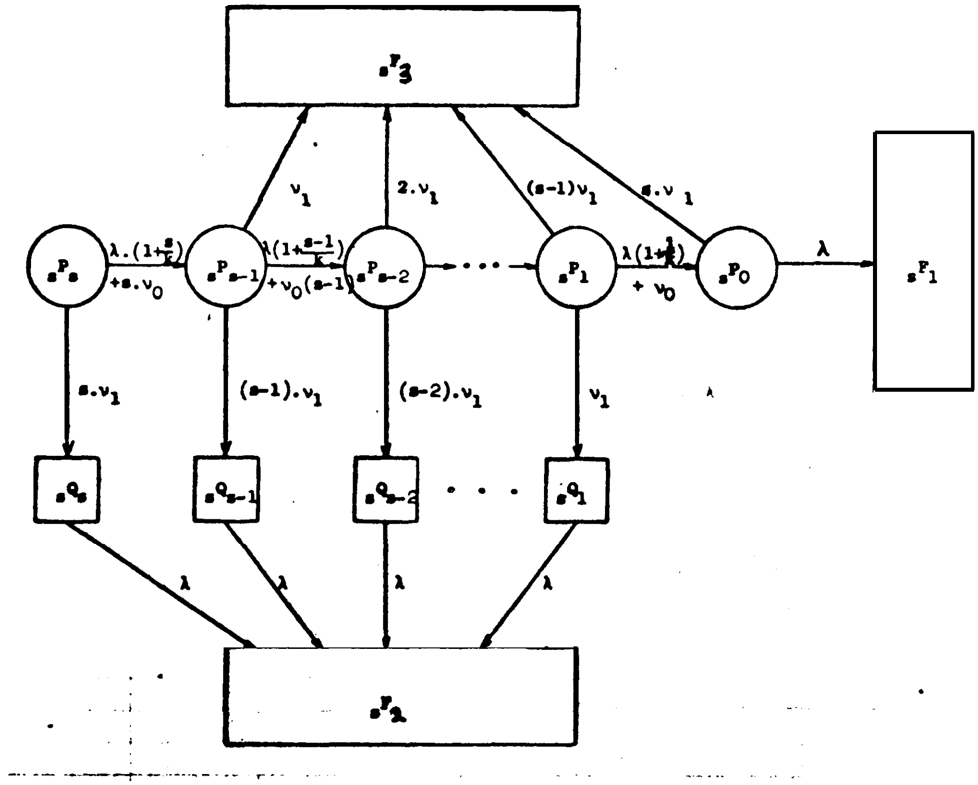


Fig. . 10 . Markoff chain for • ● tread-by system with S spares

(power switching only for modules) .

The **Laplace** transform of the reliability function is (Appendix III) :

$$_{s}R(z) = \frac{1}{z+s.\nu_1} + \frac{\nu_1}{z+\lambda} . \frac{1}{z+s.\nu_1+\nu_0+\frac{\lambda}{k}} . \left[s - \frac{A}{z+s.\nu_1} 7 \right]$$

$$- \lambda ._{s}P_0(z) \left[\frac{1}{z+s.\nu_1} - \left(1 + \frac{\lambda}{z+s.\nu_1} \right) . \frac{1}{z+\lambda} . \frac{\nu_1}{z+s.\nu_1+\nu_0+\frac{\lambda}{k}} \right]$$

The term $_{s}P_0(z)$ is equal to :

$$_{s}P_0(z) = \left| \prod_{i=0}^{s-l} \frac{A+(i+1).(\frac{\lambda}{k}+\nu_0)}{z+s.\nu_1+\lambda+i.(\frac{\lambda}{k}+\nu_0)} 4 \right| . \frac{1}{z+s.\nu_1+s.(\frac{\lambda}{k}+\nu_0)} \lambda .$$

When the number of spares is large, a good approximation of the reliability is :

$$ {}_s\hat{R}(T) = \left[1 - \frac{\lambda.\nu_1}{(\lambda - s.\nu_1).(\frac{\lambda}{k} + \nu_0)}\right] \exp(-s.\nu_1.T) $$

$$ + \frac{\nu_1}{s.\nu_1+\nu_0+\frac{\lambda}{k}+\lambda} . \left[s - \frac{\lambda}{s.\nu_1-\lambda}\right] . \exp(-\lambda.T) $$

$$ - \frac{\nu_1}{s.\nu_1+\nu_0+\frac{\lambda}{k}-\lambda} . \left[s + \frac{\lambda}{\nu_0+\frac{\lambda}{k}}\right] . \exp(-(s.\nu_1+\nu_0+\frac{\lambda}{k}).T) \cdot , $$

When the number of spares goes to infinity, the limit, R*(T), of the reliability function is :

$$ \hat{R}^*(T) = \exp(-\lambda.T) \quad . $$

So, when the number of spares approaches infinity, the reliability of stand-by systems approaches the reliability of simplex systems . This clearly indicates that the best number of spares is not infinite (simplex systems perform as well as systems with infinite redundancy and they cost infinitely less) .A stronger remark can **be made** . Maximum redundancy is equivalent to no redundancy at all .

However, when all the switches are fail-safe **(ν_1=0)**, the reliability of stand-by systems approaches 1 as the number of spares goes to infinity . This clearly shows the importance of careful design for switches and fault-detection mechanisms .

C-3-3 Stand-by systems versus simplex systems

Stand-by systems with infinite number of spares have the same reliability as simplex systems . The question that immediately arises is : is redundancy useful or harmful ?

Any stand-by system is more reliable than a simplex system for a short mission time . When the mission time is small compared to the simplex mean-life, simplex systems have a probability of failure proportional to time, while stand-by systems have a probability of failure proportional to time square . For short missions, stand-by systems achieve very high reliability gain over simplex systems .

Given a redundant system, it is interesting to know whether or not it is always more reliable than a simplex system (and if it is not, over what time range it is more reliable) . When time is much larger than the simplex mean life, the reliability of stand-by systems is approximated by :

$$ {}_{s}R(T) = \left[1 + \frac{b}{s.b+1-a} \left(\frac{a-1}{b} - \frac{a}{s.b-a} \left[1 - \frac{\binom{s+a}{s}}{\binom{s+s.b}{s}} \right] \right) \right] \exp(-\lambda.T) \quad , $$

$$ \text{with : } a = \frac{\lambda}{\nu_0 + \frac{\lambda}{k}} \qquad b = \frac{\nu_1}{\nu_0 + \frac{\lambda}{k}} \quad . $$

If a is less than 1 (dormancy factor equal to one), ${}_{s}R(T)$ is always less than ${}_{0}R(T)$ (Appendix IV) . So, every stand-by system with a dormancy factor of one will be less reliable than a simplex system if it is used for a long time . When the dormancy factor is large, for every value of the parameters λ, ν_0, ν_1, μ there exists a number S_0 such that systems with more than S_0 spares are always more reliable than simplex systems . Fig. 11 indicates if a system with s spares is more reliable than its modules . For large dormancy factor, almost every stand-by system is more reliable than a simplex system . Table 1 gives the limit on the mission time after which stand-by systems are less reliable than simplex systems .

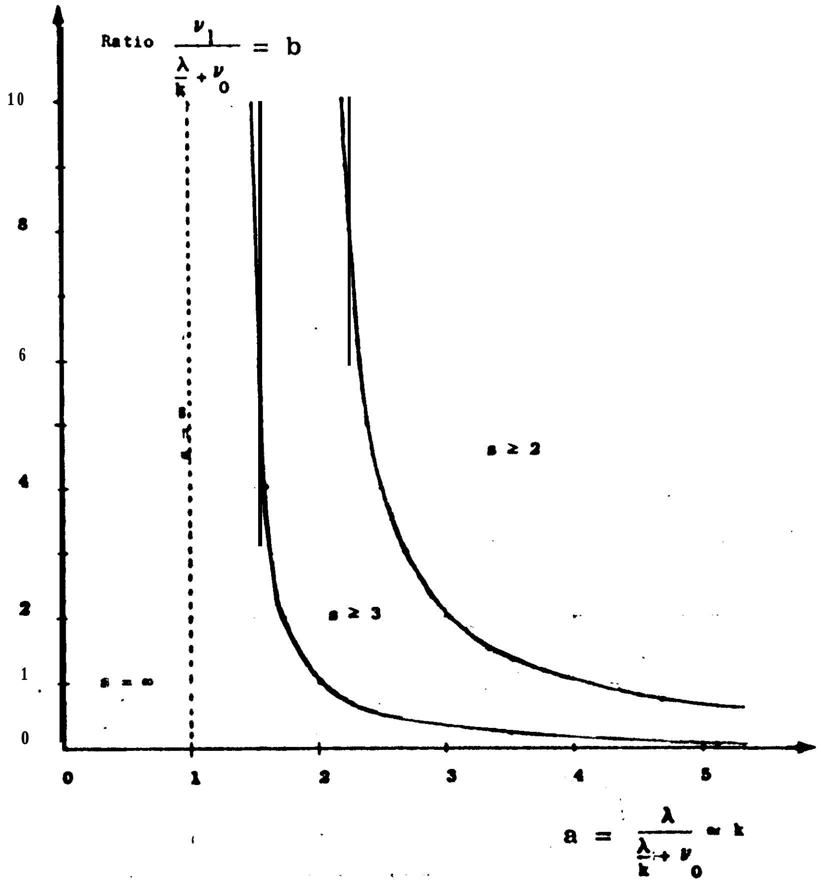


Fig. 11. Determination of the minimum number of spares much that ● tread-by systems are always more reliable than simplex ● y8teU .

Characteristics	Number of ● p8r.m									
	1	2	3	4	5	6	7	8	9	10
λ=μ= 1, ν_0= ν_1=.1	7.6	6.3	3.7	4.6	4.7	4.3	4	3.8	3.6	3.4
λ=μ= 1 ν_0=.1, ν_1=.01	65	62	43	36	34	30	26	26	24	21
λ=μ= 1 ν_0=.1, ν_1=.001	>100	>100	>100	>100	>100	>100	>100	>100	>100	>100

Table 1. Time● ♦ which● rend-by● ☐♦♏○○ becomelessreliablethansimplex ● ptr8 .

C-3-4 Reliability curves

Stand-by systems have a reliability very close to one for short mission time and very close to zero for long mission time . Systems with large number of spares and fail-safe switches have a probability of failure that approximates the step function $U(T-\tau)$:

$$ {}_{s}R(T) \cong 1-U(T-\tau) = \begin{cases} 1 \text{ if } T < \tau \\ 0 \text{ if } T > \tau \end{cases} $$

$$ \tau = \frac{1}{\mu + \nu_0} \sum_{i=0}^{s} \frac{1}{i+a} \cong \frac{1}{\lambda} \, . \, k \, . \, \text{Log} \, \frac{s+k}{k-1} \qquad \text{if } a \cong k \text{ and } k \gg 1 $$

$$ \cong \frac{k}{\lambda} \, . \left[\text{Log}(s+1) + C \right] \text{ if a is close to 1} $$

C is the Euler constant (Appendix V) . When the switches and fault-detection mechanisms are **not** fail-safe, the reliability of stand-by systems approaches :

$$ {}_{s}R(T) \simeq (s+l) . \frac{\nu_1}{s.\nu_1+\nu_0+\mu-\lambda} \left[\exp(-\lambda.T) - \exp(-(s.\nu_1+\nu_0+\mu).T) \right] $$

$$ + \left[\delta(T) - \exp(-s.\nu_1.\tau).\delta(T-\tau) \right] * \left[(1 - \frac{\lambda}{\lambda-s.\nu_1} \frac{\nu_1}{\mu+\nu_0}).\exp(-s.\nu_1 T) \right. $$

$$ - \frac{\nu_1}{s.\nu_1+\nu_0+\mu-\lambda} \left(1 + \frac{\lambda}{s.\nu_1-\lambda} \right) \exp(-\lambda.T) $$

$$ \left. \frac{\nu_1}{s.\nu_1+\nu_0+\mu-\lambda} \left(\frac{\lambda}{\nu_0+\mu} - 1 \right) \exp(-(s.\nu_1+\nu_0+\mu).T) \right] $$

with : $\delta(T-x) * f(T) = f(T-x)$ if $T > x$ and $= 0$ if $T < x$.

These approximations show that stand-by systems have good reliability when they are used for mission times less than $\frac{1}{A}$ and very low reliability for longer mfssioh times (Fig. 12) . For very small mission times, a simpler approximation can be obtained easily . Stand-by system probability of failure is close to the probability of unsafe switch failures .

Because of this special characteristics, stand-by systems are very. interesting for application with a given mission time (space application for example) , Stand-by systems are very reliable up to a certain point in time (f), then, after that, the reliability drops very -quickly . Table 2 lists the mean-life for some stand-by systems .

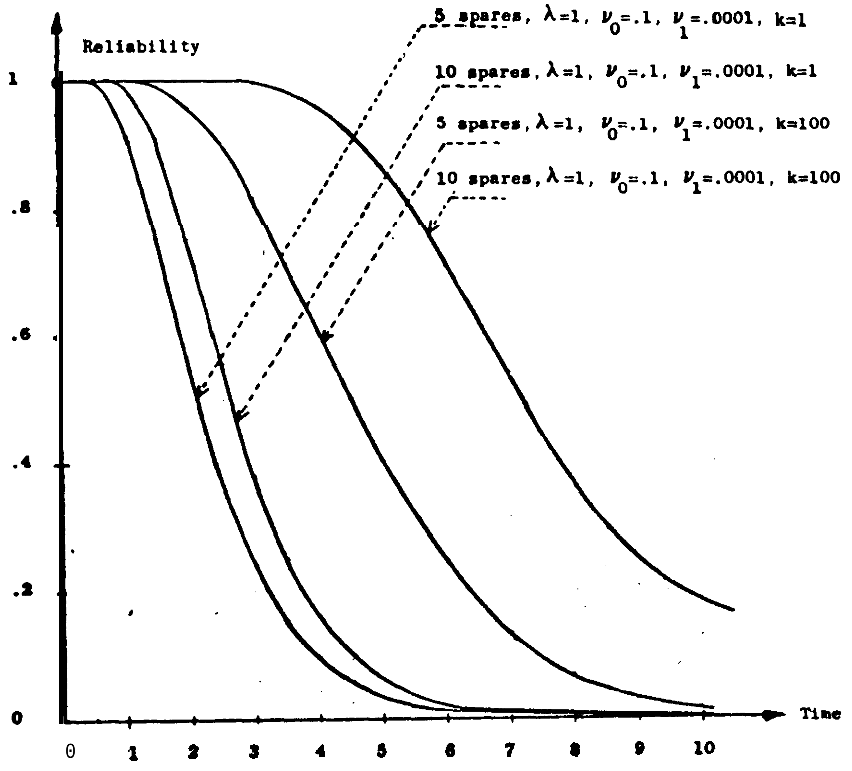


Fig. I2 . Reliability of stand-by ● yatem8 .

	v_l = .1 k - l	v_I = .1 k = 100	ν_1 =.0001 k = 1	v_1 =.0001 k = 100
s = 1	1.367	1.743	1.476	1.900
r - 3	1.570	a.349	2.020	3.470
s = 5	1.544	2.291	2.358	4.806
s = 10	1.344	1.808	3.880	7.462

Table 2 . Mean life of rtand-by systems (λ= 1 and $\nu_0 = \nu_1$) .

C-3-5 Best number of snares

When the number of spares is larger than one, the first terms of the Taylor expansion are :

$${}_sR(T) \simeq 1 - \nu_1\left[s.(\lambda+\nu_0+\mu) + A_I . \frac{T2}{2}\right.$$

$${}_sF(T) \simeq \nu_1\left[\lambda + s.(\lambda+\nu_0+\mu)\right].\frac{T^2}{2}$$

(cf. Appendix IV) . When the number of spares is one, the first term of the probability of failure is :

$${}_sF(T) \simeq \left[\nu_1.(2.\lambda+\nu_0+\mu) - \lambda.(\lambda+\nu_0+\mu)\right] , \frac{T^2}{2}$$

So, as time approaches zero, the probability of failure of stand-by systems with s spares is **lessthan** the probability of failure of systems with s+l spares . Stand-by systems with only one spare are the most reliable .

When time goes to infinity, the approximation for reliability is :

$${}_sR(T) = \left[1 + \frac{b}{s.b+1-a}\left[\frac{a-1}{b} - \frac{a}{s.b-a}\left[1 - \frac{\binom{s+a}{s}}{\binom{s+s.b}{s}}\right]\right]\right] \exp(-\lambda.T)$$

$$\text{with: } a = \frac{\lambda}{\nu_0+\mu} , \quad b = \frac{\nu_1}{\nu_0+\mu}$$

(cf. Appendix VI) . If a is greater than.one, this function decreases towards $\exp(-\lambda.T)$ as s goes to infinity . So, there is a number of spares, S_m, which gives the best reliability . S_m depends upon the failure fates, and is large in general,. However, when that many spares are needed in order to provide the best reliability, the reliability obtained is very small . In the useful range of utilisation, one can say that the best number of spares increases (and is less than S_m) as the mission time increases (Fig. 13) .

When a is less than one, the reliability function increases towards $\exp(-\lambda.T)$ as the mission time goes to infinity . So, the best number of spares goes to infinity as the mission time approaches infinity .

Fig. 13 shows the best number of spares for real systems . It increases as the dormancy factor increases or as the rate of unsafe failures decreases .

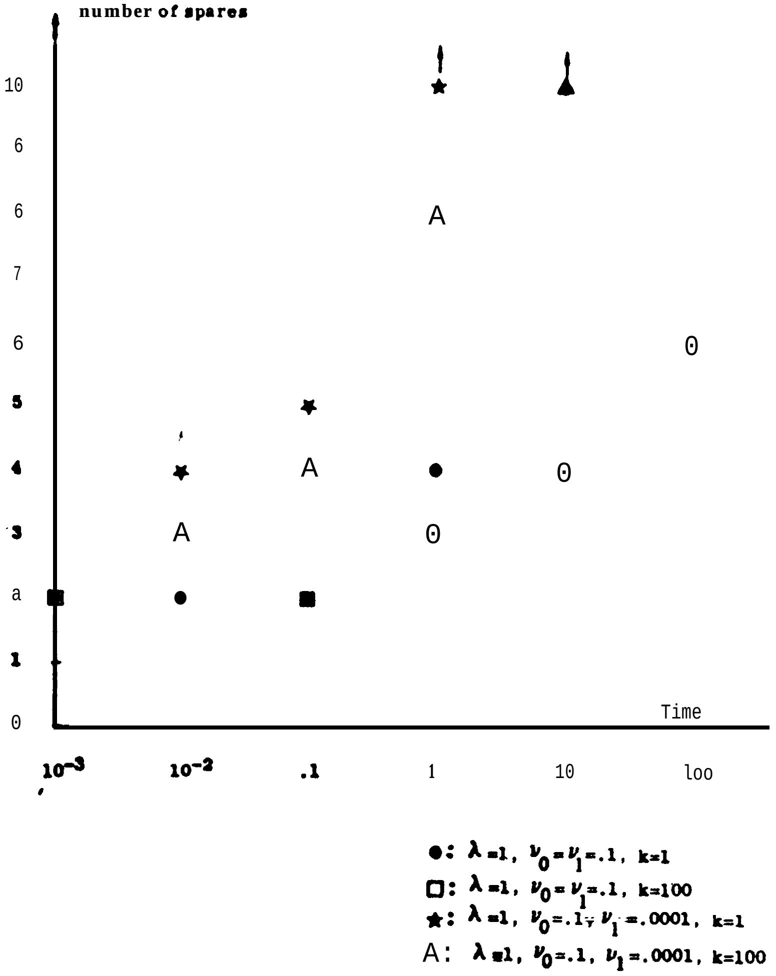


Fig. 13 . Best number of spare8 a8 a function of time .

When all the switches and fault-detection mechanisms are fail-safe, the difference between the reliability of a system with s spares and the reliability of a system with s-l spares is :

$$ {}_{s}R(T) - {}_{s-1}R(T) = \mathcal{L}^{-1}\left(\left(\prod_{i=0}^{s-1} \frac{\lambda+i.(\nu_0+\frac{\lambda}{k})}{z+\lambda+i.(\nu_0+\frac{\lambda}{k})}\right) \cdot \left[\frac{1}{z+\lambda+s.(\nu_0+\frac{\lambda}{k})}\right]\right) . $$

This difference is **always** positive . It corresponds to a convolution of positive functions . Stand-by systems with one spare are always more reliable than simplex if switches are fail-safe . So, any stand-by system with a fail-safe switch has a larger reliability than simplex systems and addition of spares always increases the reliability (which approaches one as the number of spares goes to infinity) .

C-3-5 Effect of incomplete error detection capability

The previous results were found assuming than fault-detection mechanisms were able to detect any module error that could occur . However, such an assumption is not always valid . If fault-detection mechanisms can detect only part of the possible module errors, some errors in the active module may not be detected. If l-c is the probability that an error in the active module goes undetected, the Markoff chain is given in Fig. 14 . The Laplace transform of the reliability, ${}_sR_c^\lambda(T)$, of a system with s spares (module failure rate = λ) is :

$$
{}_sR_c^\lambda(z) = \frac{1}{z+(1-c).\lambda+s.\nu_1} + \frac{\nu_1}{z+\lambda}.\frac{1}{z+(1-c).\lambda+s.\nu_1+\nu_0+\mu}\left[s - \frac{c.\lambda}{z+(1-c).\lambda+s.\nu_1}\right]
$$

$$
+ c.\lambda.{}_sP_0(z)\left[\frac{1}{z+(1-c).\lambda+s.\nu_1} - \frac{\nu_1}{z+\lambda}\,\frac{1}{z+(1-c).\lambda+s.\nu_1+\nu_0+\mu}\left[1+\frac{c.\lambda}{z+(1-c).\lambda+s.\nu_1}\right]\right]
$$

The term $c.\lambda.{}_sP_0(z)$ is equal to (Appendix VI.) :

$$
c.\lambda.{}_sP_0(z) = \prod_{j=0}^{s}\left[\frac{c.\lambda+j.(\nu_0+\mu)}{z+\lambda+s.\nu_1+j.(\nu_0+\mu)}\right]
$$

It can be easily seen that ${}_sR_c^\lambda(z)$ is equal to ${}_sR_{c=1}^{c.\lambda}(z+(1-c).\lambda)$. So, ${}_sR_c^\lambda(T)$ is equal to $\exp(-\lambda(1-c).T).{}_sR_{c=1}^{c.\lambda}(T)$. This relation gives a way to obtain all the results directly from the study of systems with complete fault-detection capability .

$$
{}_sR_c^\lambda(T) = \exp(-\lambda(1-c).T).{}_sR_{c=1}^{c.\lambda}(T) .
$$

If $c.\lambda$ is less than $\nu_0+\mu$, stand-by systems are always less reliable than simplex systems in the long run . If the relation is not true, then for every set of parameters λ, μ, ν_0,ν_1 and c, there exists a number S_0 such that stand-by systems with more than S_0 spares are always more reliable than simplex systems . The number S_0 can be found directly from Fig. 11 .

Reliability curves can be obtained from the study of systems with complete error detection capability . The cut-off point, τ, is the one obtained in C-3-4 if λ is replaced by $c.\lambda$. For a given mission time, the best number of spares for a system with incomplete error detection and a failure rate of λ for active modulesis equal to the best number of spares for a system with complete error detection and a failure rate of $c.\lambda$ for active module .

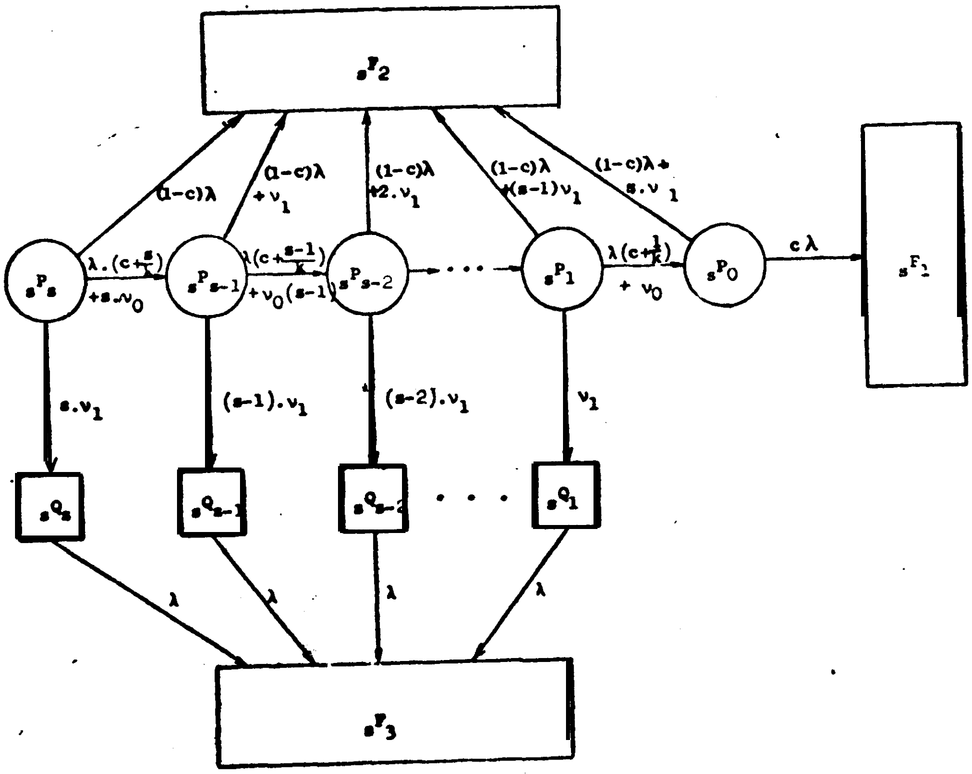


Fig. 14 . **Markoff** dhain for stand-by systems with s spares (incomplete fault-detection) .

D - CONCLUSIONS

Stand-by redundancy appears, on first approach, to be a very promising method to improve reliability . However, the use of stand-by redundancy, gives limited results . It is impossible, whatever the cost one may wish to pay, to get high reliability for long mission time . Stand-by systems with infinite number of spares perform as poorly as simplex systems . For every stand-by system, there exists a best number of spares which is increasing with mission time . Systems with one spare are the best for very short mission time . The best number of spares is surprising small (five or less for most systems when the duration of the mission time is less than one tenth of the simplex mean-life) .

Even when the number of spares is chosen to maximize the probability of success of the mission, the success probability approaches zero when the duration of the mission goes to infinity . Given a stand-by system, with a reasonably small number of spares, its reliability is very close to one for missions that last less than a certain limit τ, then drops very quickly to zero . The limit, τ, which defines the useful life of stand-by systems, increases as the logarithm of the number of modules (number of spares plus one) . As the number of spares gets large, this property tends to disappear and stand-by system characteristics approach simplex system characteristics .

The effect of the dormancy factor is very important . If power-off components do not fail, it may be possible to design ideal stand-by systems such that addition of spares always increases reliability . However, even with infinite redundancy, the probability of failure increases towards one as the mission time increases . When the spares have the same failure rate as the actives modules (dormancy factor of one or logical switching), any stand-by system becomes' less reliable than simplex systems if it is used for too long . When the dormancy is greater than one but finite, some stand-by systems are always more reliable than simplex systems .

If the fault-detection mechanisms are designed to catch only a fraction, c, of all possible module errors, performances decreases . A simple relation between the reliability of systems with incomplete fault-detection and systems with complete fault-detection has been obtained . The best number of spares for a system with coverage c and k gates per module is equal to the best number of spares for a system with c.k gates per module and complete error detection, but the best reliability that can be achieved is much lower .

In summary, one can say that stand-by redundancy may be very useful when it is properly used . Stand-by redundancy should be used to increase the reliability at the end of mission time, rather than to increase the mission time for a given reliability.. Stand-by redundancy, because of the step shape of reliability, is very useful for application with fixed mission duration . However, very careful modeling is necessary . The use of too many spares may decrease significantly, or even negate, the reliability gain obtained over simplex systems .

Appendix I

Assume that there does not exist a finite best number of spares . Then the reliability is monotonicly increasing with the number of spares . But :

$$\lim_{s \to \infty} \Bigl[{}_{c(s+1)}R^{q}_{s+1}(\lambda,\mu,T) - {}_{c(s)}R^{q}_{s}(\lambda,\mu,T) \Bigr]^{S} \Bigl[c(s+1)-c(s) \Bigr\} .$$

$$\Bigl[{}_{c(s)}R^{q}(\lambda,\mu,T) - \Bigl(\frac{q.\lambda}{\mu} - 1 \Bigr) . \Bigl(1-\exp(-\mu.T) \Bigr)^{0} \Bigr] \leqslant 0 \quad .$$

So, for every time T, there exists a number S such that systems with more than S spares have, at time T, a reliability less than the reliability of systems with S spares . .

Appendix II

Reliability of' ideal stand-by systems

$$ {}_sR(T) = \sum_{i=0}^{s} {}_sP_i(T) + \sum_{j=1}^{s} {}_sQ_j(T) $$

$$ \frac{d\ {}_sP_s(T)}{dT} = -(\lambda + \nu_0 + \nu_1) \cdot {}_sP_s\ (T) $$

$$ \frac{d\ {}_sP_i(T)}{dT} = -(\lambda + \nu_0 + \nu_1) \cdot {}_sP_i(T) + (\lambda + \nu_0) \cdot {}_sP_{i+1}\ (T) $$

$$ \frac{d\ {}_sQ_j(T)}{dT} \quad - \lambda . {}_sQ_j(T) \quad \nu_1 \cdot \ {}_sP_j(T) $$

$$ {}_sP_s(T{=}0) = 1 \qquad {}_sP_i(T{=}0) = 0 \text{ for } i \in \left\{0,1,2,\ldots,s-1\right\} $$

$$ {}_sQ_j(T{=}0) = 0 $$

$$ {}_sR(z) = \int_0^{\infty} \exp(-z.T) \ . \ {}_sR(T).dT = \frac{1}{z} - \frac{\nu_1}{z} \cdot \frac{\lambda}{z+\lambda} \cdot \sum_{k=1}^{s} \frac{(A+\nu_0)^{k-1}}{(z+\lambda+\nu_0+\nu_1)^k} + $$

$$ \frac{\lambda}{z} \cdot \frac{(\lambda+\nu_0)^s}{(z+\lambda).(z+\lambda+\nu_0+\nu_I)^s} $$

$$ \lim_{s\to\infty} {}_sR(T) = \lim_{s\to\infty} \left[\mathfrak{L}^{-1}\ {}_sR(z) \right] = \mathfrak{L}^{-1} \left[\lim_{s\to\infty} \ {}_sR(z) \right] = \mathfrak{L}^{-1} \left[\frac{1}{z} - \frac{1}{z} \frac{\lambda}{z+\lambda} \frac{\nu_1}{z+\nu_1} \right] $$

$$ = \frac{1}{\lambda-\nu_1} \left| \lambda.\exp(-\nu_1.T) - \nu_1.\exp(-\lambda.T) \right| $$

Appendix I II

Reliability of real stand-by systems

$${}_sP_s(T=0) = 1$$

$$\frac{d\,{}_sP_s(T)}{dT} = -\left[\lambda(1+\frac{s}{k}) + s(\nu_0+\nu_1)\right] \cdot {}_sP_s(T)$$

$$\frac{d\,{}_sP_i(T)}{dT} = -\left[X(1+\frac{i}{k}) + s.\nu_1 + i.\nu_0\right] \cdot {}_sP_i(T) + \left[\lambda(1+\frac{i+1}{k}) + (i+1).\nu_{0_3} \bullet \quad \text{sPi+l(T)}\right.$$

$$\frac{d\,{}_sQ_j(T)}{dT} = -\lambda . {}_sQ_j(T) + j.\nu_1 . {}_sP_j(T)$$

Using Laplace transform and combinatorial formula [11]:

$$\sum_{i=0}^{s} {}_sP_i(z) = \frac{1}{z+s.\nu_1}\left[1 - \lambda . {}_sP_0(z)\right._3$$

$$\sum_{i=1}^{s-l} \frac{d\,{}_sQ_i(T)}{dT} = \nu_1 \sum_{i=0}^{s-l} i . {}_sP_j(T) - \lambda \sum_{i=0}^{s-l} {}_sQ_i(T)$$

$$\sum_{i=0}^{s} i . {}_sP_i(z) = \frac{1}{z+s.\nu_1+\nu_0+\frac{\lambda}{k}}\left[s - \frac{\lambda}{z+s.\nu_1} . (1-\lambda . {}_sP_0(z)) + \lambda . {}_sP_0(z)\right]$$

$${}_sR(z) = \frac{1}{z+s.\nu_1} + \frac{\nu_1}{z+\lambda} . \frac{1}{z+s.\nu_1+\nu_0+\frac{\lambda}{k}} . \left[s - \frac{\lambda}{z+s.\nu_1}\right]$$

$$- \lambda . {}_sP_0(z)\left[\frac{1}{z+s.\nu_1} - \left(1 + \frac{\lambda}{z+s.\nu_1}\right) . \frac{1}{z+\lambda} . \frac{\nu_1}{z+s.\nu_1+\nu_0+\frac{\lambda}{k}}\right]$$

$${}_sP_0(z) = \left[\prod_{i=0}^{s-l} \frac{A+(i+1).(\frac{\lambda}{k}+\nu_0)}{z+s.\nu + \lambda + i.(\frac{\lambda}{k} + \nu_0)}\right] . \frac{1}{z+s.\nu \quad (\frac{\lambda}{k}+\nu_0)+\lambda}$$

Appendix IV

Poles and residues of ${}_sR(z)$:

Residue for the pole $-\nu_1 = 0$

Residue for the pole $-(\nu_0+\nu_1+\frac{\lambda}{k}) = 0$

Residue for the pole $-\lambda = r = 1 + \frac{b}{s.b+1-a}\left[\frac{a-1}{b} - \frac{a}{s.b-a}\left[1 - \frac{\binom{s+a}{s}}{\binom{s+s.b}{s}}\right]\right]$

with : $a = \dfrac{\lambda}{\nu_0 + \frac{\lambda}{k}}$ $\qquad b = \dfrac{\nu_1}{\nu_0 + \overset{A}{ii}}$

Residue for pole $-(\lambda+s.\nu_1+j(\nu_0+\mu)) = (-1)^j\left[\dfrac{\prod_{i=0}^{s}(i+a)}{j!\ (s-j)!}\,\dfrac{1}{a+j}\left[1+j.\dfrac{b}{s.b+j}\,\dfrac{1}{a+j-1}\right]\right]$

Theorem:

If a is less than one, **r,** the residue for the pole **$-\lambda$ is** always less than one . If a is equal to one, r is less than one for s **finite** and equal one for s infinite . If a is greater than one, **r** approaches one (decreasing towards one) as s goes to infinity . So, for every value **of** b, if a is greater than one, there exists **a** number S_0 such that s greater than S_0 **implies** r greater than one .

Proof';

$$\frac{-a}{s.b-a}\left[1 - \frac{\binom{s+a}{s}}{\binom{s+s.b}{s}}\right]$$ is always negative for **a,** b positive

So, **If a is** less than one, r is always less than one for every s .

If a is equal to one, r is less than one except if s Is Infinite . If s Is Infinite, r is equal to one .

Formal derivation of Gamma functions is not very easy . So, formal derivation of r with respect to s will not be made . However, as s goes to infinity, r approaches one (In decreasing) :

$$\underset{s\to\infty}{\text{Limit}}\left[1 - \frac{\binom{s+a}{s}}{\binom{s+s.b}{s}}\right] = 1 \quad ,$$

$$\underset{s\to\infty}{\text{Limit}}\left[\frac{a-1}{b} - \frac{a}{s.b-a}\left[1 - \frac{\binom{s+a}{s}}{\binom{s.b+s}{s}}\right]\right] = \frac{a-1}{b} > 0 \quad \text{if } a > 1$$

$$\underset{s\to\infty}{\text{Limit}}\ r = \underset{s\to\infty}{\text{Limit}}\left[1 + \frac{b}{s\ b+1\ a} . \frac{a-1}{b}\right] = 1^{+}$$

So, as s goes to infinity, the residue r **approches** one but is bigger than one for finite s . This implies than there Is a value s_0 such that, If s larger than s_0, the residue s is larger than one . The residue for **s=1** Is less than one for every value of a and b . So, s_0 is always bigger than one . Exact values for s_0 as a function of a and b are given in Fig. 13 . Curves show that, if s is less than s_0, the residue r is less than one .

Mean-life

$$\text{Mean-life} = \text{M.L.} = \int_0^{\infty} {}_sR(t).dt = {}_sR(z=0)$$

$$\textbf{If } \nu_1=0, \text{ then M.L.} = \sum_{i=0}^{s} \frac{1}{\lambda+i.\alpha} = T_0$$

If $\nu_1 \neq 0$, then M.L. **is** less than T_0 . **Any** cause of failure which exists in systems with perfect switches exists also in systems with Imperfect switches . Furthermore, systems with unsafe switches have other kinds of failures . Similarly, the mean-life decreases as the failure rates of modules, switches and fault-detectors increase .

Appendix V

Approximation of reliability by Dirac function

If $\nu_1 = 0$ then $${}_sR(z) = \frac{1}{z}\left[1 - \lambda . {}_sP_0(z)\right]$$

$$= \frac{1}{z}\left[1 - \frac{1}{\prod_{j=0}^{s}\left[1 + \frac{z}{\lambda + i.\alpha}\right]}\right]$$

with $\alpha = \frac{\lambda}{k} + \nu_0$

$${}_sR(z) \simeq \frac{1}{z}\left[1 - \frac{1}{\sum_{j=0}^{s}\left[z.\sum_{i=0}^{s}\frac{1}{\lambda+i.\alpha}\right]^j}\right] \simeq \frac{1}{z}\left[1 - \exp(- z \,.\, \sum_{i=0}^{s}\frac{1}{\lambda+i.\alpha})\right|$$

$${}_sR(T) \simeq 1 - U(T-\tau)$$

$$\tau = \sum_{i=0}^{8}\frac{1}{\lambda+i.\alpha} = \left[\sum_{i=0}^{s}\frac{1}{i+a}\right| \frac{1}{\alpha}$$

$\tau \simeq \frac{a}{\lambda}.\left[\text{Log}(s+1) + C\right]$ if $a \simeq 1$, C is Euler constant, C=.57721

$\tau \simeq \frac{a}{\lambda} . \text{Log}\,\frac{s+a}{a-1}$ If $a \gg 1$

if $\nu_1 \neq 0$ then $${}_sP_0(z) \simeq \exp(- \frac{z+s.\nu_1}{\alpha} . \sum_{i=0}^{s}\frac{1}{i+a})$$

$${}_sR(T) \begin{cases} = f(T) - t\, g(T) = {}_s\hat{R}(T) & \text{if } T < \tau \\ = f(T) + g(T) - \exp(-s.\nu_1.\tau).g(T-\tau) & \text{if } T > \tau \end{cases}$$

with $$\begin{cases} f(T) = (s+1).\,\mathcal{L}^{-1}\left(\frac{1}{z+\lambda}.\frac{\nu_1}{z+s.\,\nu_1+\nu_0+\mu}\right) \\ g(T) = \mathcal{L}^{-1}\left(\frac{1}{z+s.\nu_1} - \frac{1}{z+\lambda}.\frac{\nu_1}{z+s.\,\nu_1+\nu_0+\mu}\left[1 + \frac{\lambda}{z+s.\nu_1}\right]\right) \end{cases}$$

Appendix VI

Reliabili ty of real stand-by systems (incomplete fault-detection)

$${}_sP_s(T{=}0) = 1$$

$$\frac{d_sP_s(T)}{dT} = -\left[\lambda\left(1+\frac{s}{k}\right) + s(\nu_0+\nu_1)\right] . {}_sP_s(T)$$

$$\frac{d_sP_i(T)}{dT} = -\left[\lambda\left(1+\frac{i}{k}\right) + s.\nu_1 + i.\nu_0\right] \bullet \ \mathrm{sPi(T)} + \left[\lambda\left(c+\frac{i+1}{k}\right) \boxed{\equiv} \ (i+1).\nu_{0_3} \right.$$

$$\frac{d_sQ_j(T)}{dT} = -\lambda . {}_sQ_j(T) + j.\nu_1 . {}_sP_j(T)$$

Using Laplace transform :

$$\sum_{i=0}^{s} {}_sP_i(z) = \frac{1}{z+c\lambda+s\nu_1}\left[1-c.\lambda.{}_sP_0(z)\right._3$$

$$\sum_{151}^{s-l} \frac{d_sQ_i(T)}{dT} = \nu_1 \sum_{i=0}^{s-l} i.{}_sP_j(T) - \lambda \sum_{i=0}^{s-l} {}_sQ_i(T)$$

$${}_sR_c^{\lambda}(z) = \frac{1}{z+(1-c).\lambda+s.\nu_1} + \frac{\nu_1}{z+\lambda}.\frac{1}{z+(1-c).\lambda+s.\nu_1+\nu_0+\mu}\left[s - \frac{c.\lambda}{z+(1-c).\lambda+s.\nu_1}\right]$$
$$+ c.\lambda.{}_sP_0(z)\left[\frac{1}{z+(1-c).\lambda+s.\nu_1} - \frac{\nu_1}{z+\lambda}\frac{1}{z+(1-c).\lambda+s.\nu_1+\nu_0+\mu}\left[1+\frac{c.\lambda}{z+(1-c).\lambda+s.\nu_1}\right]\right]$$

The term $c.\lambda.{}_sP_0(z)$ is equal to (Appendix VII) :

$$c.\lambda.{}_sP_0(z) = \prod_{j=0}^{8}\left[\frac{c.\lambda+j.(\nu_0+\mu)}{z+\lambda+s.\nu_1+j.(\nu_0+\mu)}\right]$$

$${}_sR_c^{\lambda}(T) = {}_sR_1^{c.\lambda}(T) . \exp(-(1-c).T)$$

REFERENCES

1. A. Avizienis, "Design of Fault-Tolerant Computers', FJCC, Vol. 31, pp. 733-743, 1967 .

'2 W. G. Bouricius, W. C. Carter, D. C. Jessep, P. R. Schneider, and A. B. Wadia, 'Reliability modeling for fault-tolerant computers', IEEE Trans. on Computers, Vol. C-20, No. 11, November 1971,pp. 1306-1311.

3. J. Goldberg, K. N. Levitt, and R. A. Short, "Techniques for realization of ultra-reliable spaceborn computers', Final Report, Phase I, SRI project 5580, Stanford Research Institute, Menlo Park, California, September 1966.

4. W. G. Bouricius, W. C. Carter, and P. R. Schneider, "Reliability modeling 'techniques for self-repairing computer systems", Proc. ACM 1969 Annual Conference, pp. 295-305, also IBM Rep. RC-2378.

5. T. F. Arnold, 'The concept of coverage and its effect on the reliability model of a repairable system', IEEE Trans. on Computers, Vol. C-22, No. 3, March 1973, pp. 251-254, also in Proc. from the International Symposium on Fault-Tolerant Computing, Newton, Mass., June 19-21, 1972.

6. D. A. Rennels and A. Avizlenis, 'RMS: A reliability modeling system for self-repairing computers', Proc. of the Third International Symposium on Fault-Tolerant Computing, June 21-22, 1973, Palo Alto, California, pp. 131-135.

7. J.P. Roth, W.G. Bouricius, W.C. Carter and R.P. Schneider "Phase II of an architectural study for a self-repairing computer", SAMSO TR67-106, November, 1967 .

8. W.S. Feller, 'An Introduction to Probability Theory and its Applications", Volume I, Wiley, New-york, 1957 .

9. P.O. Nerber, "Power Off Time Impact On Reliability Estimates", IEEE Int. Convention Rec., Part 10, pp. 1-5, March 22-26, 1965, New-york .

10. G.A. Korn and T.M. Korn, "Mathematical Handbook for Scientists and Engineers", McGraw-Hill, New-York, 1961

11. D.E. Knuth, "The Art of Computer Programming", Vol. 1, "Fundamental Algorithms",Adison-Wesley Publishing Company, New-York, 1969 .