X-560-70-323
PREPRINT

NASA TM X- 65309

RELIABILITY TECHNIQUES FOR FLIGHT SYSTEMS

PAUL HEFFNER

APRIL 1970

GSFC
GODDARD SPACE FLIGHT CENTER
GREENBELT, MARYLAND

Reproduced by
NATIONAL TECHNICAL
INFORMATION SERVICE
Springfield, Va. 22151

X-560-70-323

RELIABILITY TECHNIQUES
FOR FLIGHT SYSTEMS

by

Paul Heffner

April 1970

Information Processing Division

Tracking and Data Systems Directorate

Goddard Space Flight Center

Greenbelt, Maryland

CONTENTS

RELIABILITY TECHNIQUES FOR FLIGHT SYSTEMS

by

Paul Heffner

Goddard Space Flight Center

ABSTRACT

When high reliability is required for a spacecraft electronic system, it is desirable to have a good perspective of various approaches to redundancy during both conceptual and design phases. The intent of this document is to contribute to such a perspective. The document is divided into two parts. Part 1 is a result of a generalized study, and Part 2 is one of application to a real system.

In Part 1, three fundamental techniques of applying redundancy are discussed. The discussion for each technique leads to the development of resultant curves that show the improvement given by that technique over one that uses only a simplex system. Each of these curves is plotted against the number of additional circuits required to implement the redundancy. Finally, as a conclusion to Part 1, the three techniques are compared to each other by reviewing their mission-lifetime improvements, with consideration given to the implementation penalty of additional circuits. For the various techniques, certain general conditions had to be made and maintained throughout the discussions to allow for reasonable comparisons. The conditions used for these comparisons are included.

In Part 2, some application work involving improving the reliability of an existing system is given. The system is the On-Board Processor, a spacecraft computer for the Orbiting Astronomical Observatory. This part provides for a deviation from the generalized discussions of Part 1 and for further insight into the potential mission-lifetime benefits afforded by redundancy.

RELIABILITY TECHNIQUES FOR FLIGHT SYSTEMS

PART 1
COMPARING TECHNIQUES OF REDUNDANCY

INTRODUCTION

Redundancy techniques are investigated when a need develops to improve a given system's reliability, or, in other words, when a need develops for extending the lifetime of a system for a given degree of confidence. Initially, the elements that make up the system will have been selected with consideration of their individual failure rates, or, their mean-time-between-failures (MTBF). Tradeoffs among power, size, weight, utility, bandwidth, availability, cost, etc., will have been made along with reliability considerations during the selection of components, modules, parts, and assembly. Reliability then suffers because of other equally important factors. Therefore, it is not unusual for a simplex system to have a reliability that is less than desirable. *

When redundancy is considered, numerous tradeoffs require a perspective of the various techniques. This document considers three general redundancy techniques for improving system reliability: (1) paralleling, (2) subdividing, and (3) columnizing. These techniques will be discussed separately and

*The simplex system is defined to be a system in which any single-point failure will cause a failed system. In reality, many failures within a system will cause a degraded system rather than a useless system. For a given specified system, a great deal of qualification is required when this consideration is brought into discussion. When general techniques are compared, the simplex system condition given first is appropriate.

then compared. All three techniques may not be choices available to the designer for all types of systems.

Each technique can be divided into three categories: (1) "active" (or "hot") redundancy, (2) standby "tepid" redundancy, and (3) standby "cold" redundancy. A powered-on system in standby is said to be active, and its failure rate is the same whether it is "in the loop" or not. A tepid system, when powered off, has a smaller (but not zero) failure rate than its powered-on failure rate. A cold system has a failure rate of zero when powered off (an unrealistic case—yet a useful consideration). In the following discussions, all "in-the-loop" powered-on systems have elements with the same failure rate as the original main system (that failed).

Further, it is assumed (1) that the system is composed of homogeneous elements (so far as reliability is concerned), (2) that additions or modifications to the system to effect redundancy are made with elements of similar reliability, and (3) that these elements are equally distributed on each unit used in redundancy, including the main operating unit.* These assumptions are not wholly realistic, but they allow for reasonable comparisons between general approaches, as will be shown.

The word "unit", used throughout the discussions, could represent a system, subsystem, or a smaller functional unit. The word "circuit" is also used

*For the technique of columnizing, a further condition is stipulated. It is discussed in that section of the paper.

throughout the discussion; it could be any "element" such as a circuit chip and its average number of wiring contacts—again, as long as it can be assumed that all elements are alike regarding reliability.

All reliability calculations leading to the resultant curves were based on models whose elements have constant failure rates when powered on. A simplex system made up of such elements exhibits a reliability curve that is exponential with time.

PARALLEL REDUNDANCY

The first of the three techniques that will be discussed is parallel redundancy, as shown in Figure 1.

The original simplex unit, before being placed in parallel redundancy, contains n circuits ($k = 1$) and exhibits the familiar exponential reliability curve given by $R\ (t) = e^{-n\lambda t}$, with λ equal to the failure rate of each circuit (or element). The system failure rate is $n\lambda$, and the system MTBF is $1/n\,\lambda$. This

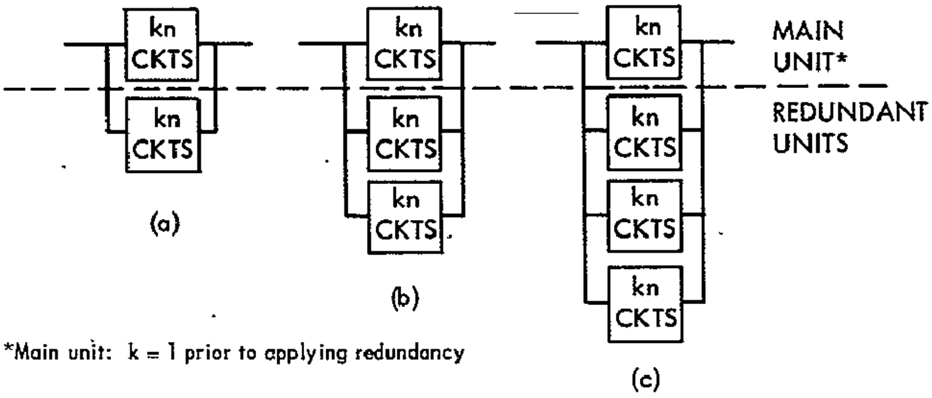


Figure 1—Parallel redundancy employing one, two, and three additional units.

curve is plotted in Figure 2, curve A. It conveys that there is only a 37-percent probability for the system to operate without failure for a period of time equal to the system's MTBF. The probability that the system will operate successfully for 0.11 times its MTBF is 0.9. For example, if a simplex system is to have a 90-percent probability of operating without failure for 1 year, it should have a MTBF of at least 9.1 years.

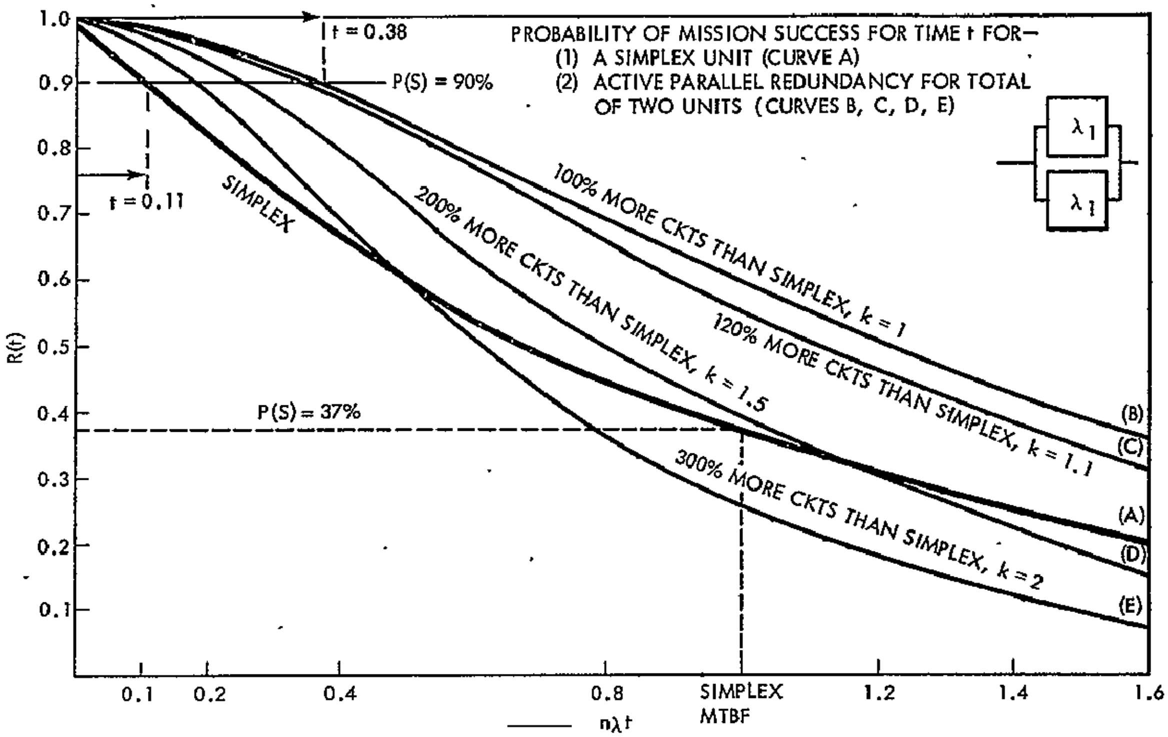


Figure 2—Active parallel redundancy for one unit in standby.

System reliability, when using one additional unit in active redundancy, for which there would be $2n$ circuits in all is given as

$$R(t) = 2e^{-k\tau} - e^{-2k\tau},$$

where

$$\tau = n\lambda t$$

and

k = ratio of the number of circuits in each unit for the redundant system, to the number of circuits in the original simplex unit.

A plot of this is given by curve B in Figure 2. Assuming the criterion for mission lifetime is based on a 90-percent probability of success [$P(S)$], the system will operate without failure for 0.38 of the simplex MTBF, thus providing a gain of 3.45 in mission lifetime.*

Realistically, there is a penalty in the way of additional circuits necessary to implement the total system so that more than precisely $2n$ circuits will be required. For a large unit, the percentage is likely to be small. Curve C gives the reliability of a system when each of the two parallel units contain 10 percent more circuits (k = 1.1) so that the total system has 120 percent more circuits than the simplex unit. Similarly, curve D gives the reliability for k = 1.5, or 200 percent more circuits than simplex. For a small simplex unit, the percentage of additional circuits is likely to be high. To apply redundancy to one logic gate, as an extreme example, may require three additional circuits, or a 300-percent increase over the simplex gate. Curve E is plotted for this case, where k = 2. The reliability return begins to diminish as the circuit penalty increases. From this small family of curves for active parallel redundancy when employing a total of two units, a more meaningful curve can be plotted.

In Figure 3, the total system gain in mission lifetime, relative to the simplex unit, where lifetime is based on the 90-percent probability of success,

*See Appendix A for a discussion of mission lifetime gain as a function of different choices of $P(S)$.

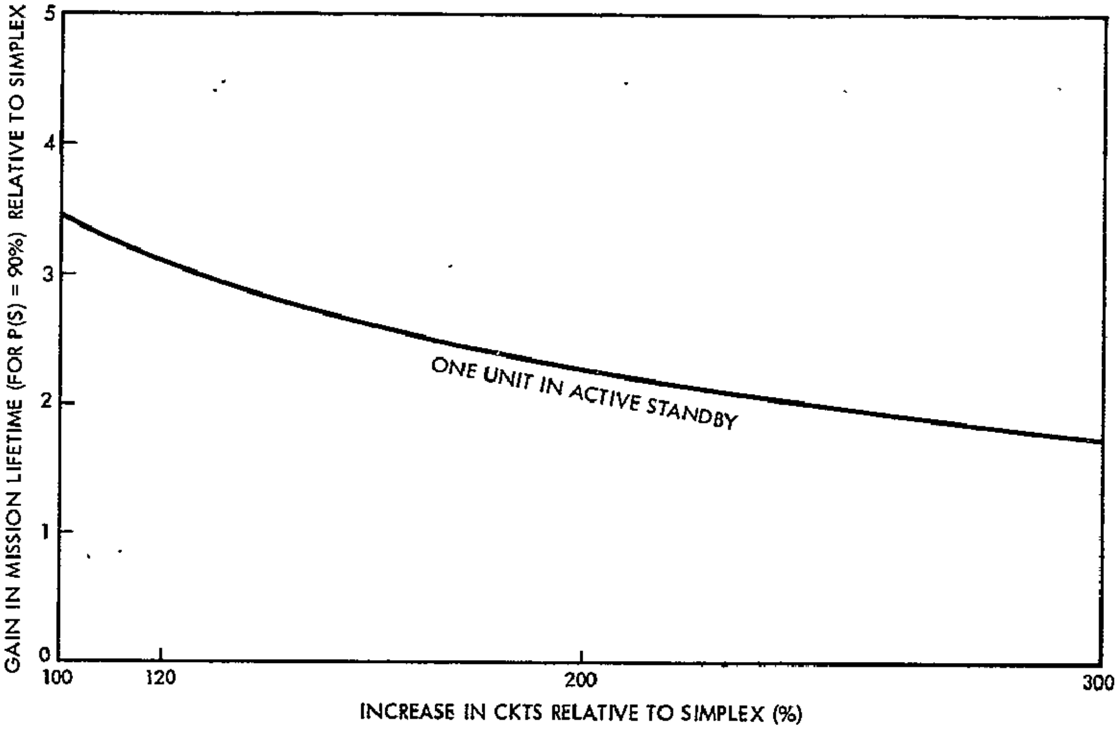


Figure 3–One unit in active standby.

is plotted against the percentage of additional circuits used to implement redundancy. For example, the mission lifetime can be increased threefold over that of the simplex unit if the implementation of one additional parallel and switchable unit does not require more than 125 percent more circuits.

An upper bound on reliability improvement through the use of spare units is provided by the same analysis but with the assumption of "cold redundancy." Here a unit is powered off when it is not in use, and its failure rate is assumed to be zero until turned on. When using one additional unit in cold standby, system reliability is expressed as

$$R(t) = e^{-kr}(1 + kr),$$

where

$\tau = n\lambda t$

and

k = ratio of the number of circuits in each unit for the redundant system, to the number of circuits in the original simplex unit.

A family of reliability curves for this case is shown in Figure 4. Four curves are given for k = 1, 1.1, 1.5, and 2. This represents a system increase in circuits of 100, 120, 200, and 300 percent, respectively. Figure 5 gives the mission lifetime gain relative to simplex for $P(S)$ = 90 percent.

For the more realistic case, where a powered-off unit does have some failure rate (but less than the powered-on unit), the relationship for "tepid

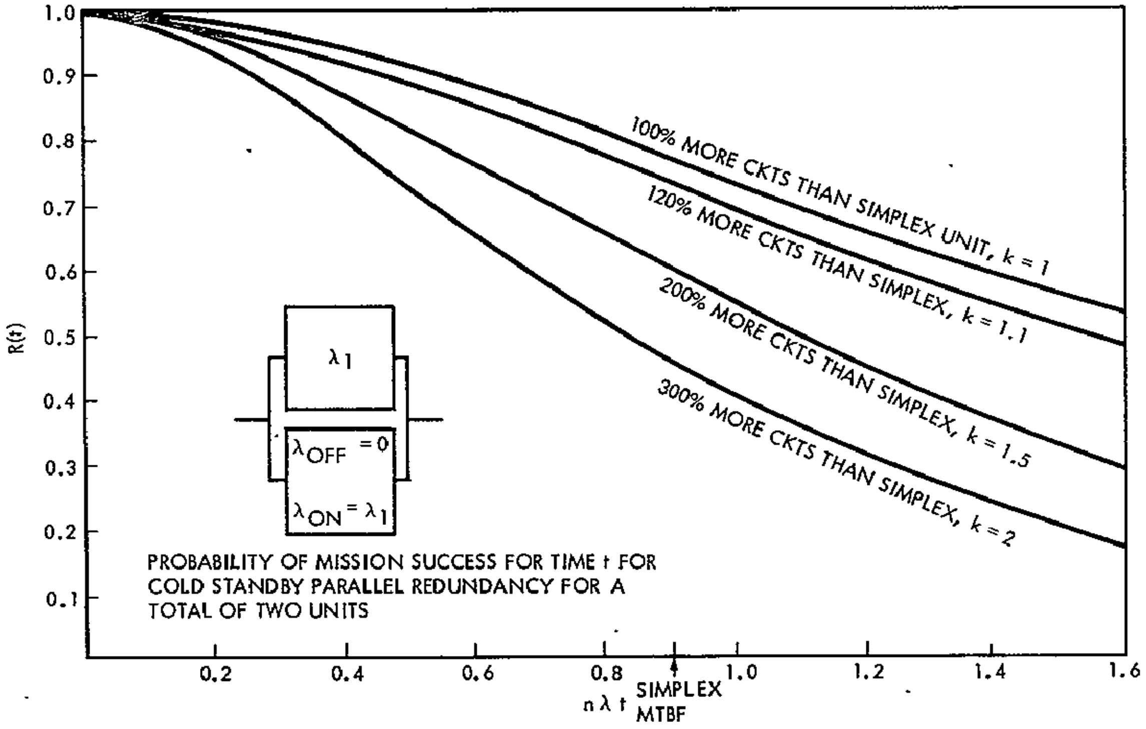


Figure 4–Cold parallel standby redundancy for one unit in standby.

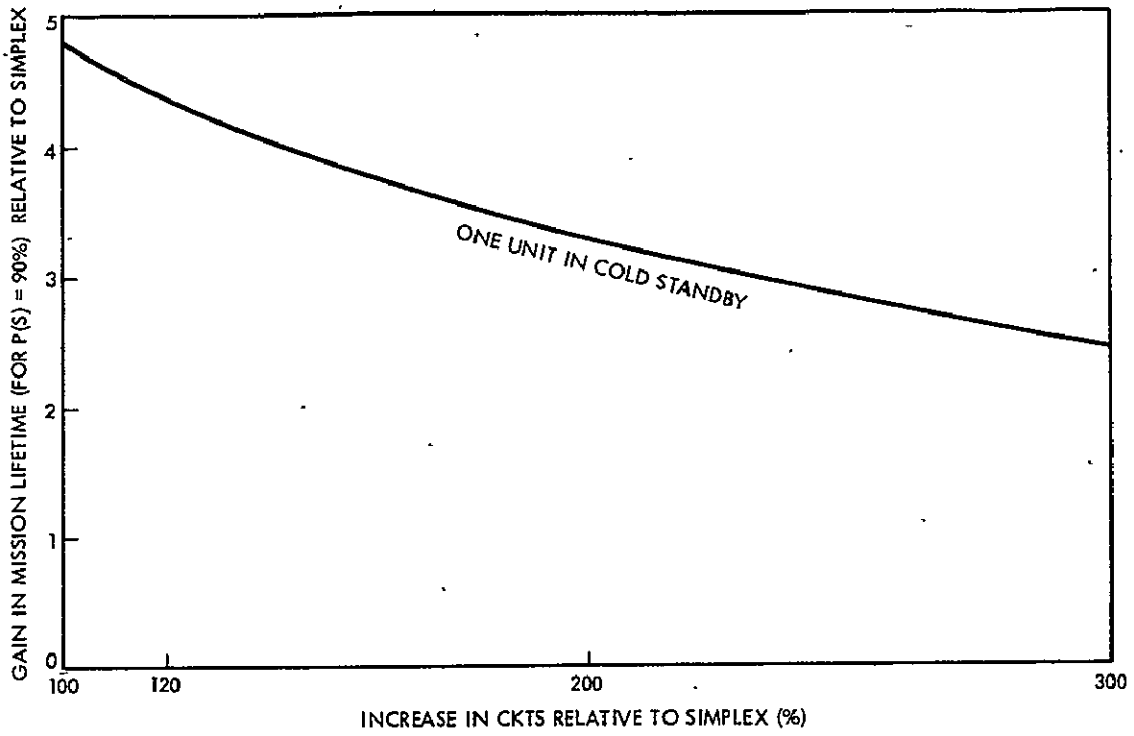


Figure 5–One unit in cold standby.

standby" is used. For a reasonable choice of powered-off failure rate being 1/5 that of the powered-on failure rate, the following expression can be used:

$$R(t) = e^{-k\tau} + 5\,(e^{-k\tau} - e^{-1.2k\tau}),$$

with the variables defined as given previously. The resulting family of reliability curves for $k = 1,\ 1.1,\ 1.5$, and 2 are given in Figure 6. From these, the mission lifetime gain for $P(S) = 90$ percent is plotted in Figure 7, curve C, with the curves for cold standby and active standby included for comparison. It can be observed from these plots that there is not a heavy penalty in the way of decreased lifetime gain as more circuits are used.

The discussion thus far has led to the generation of a set of curves for active, cold, and tepid standby where, in total, two units are used. For the case

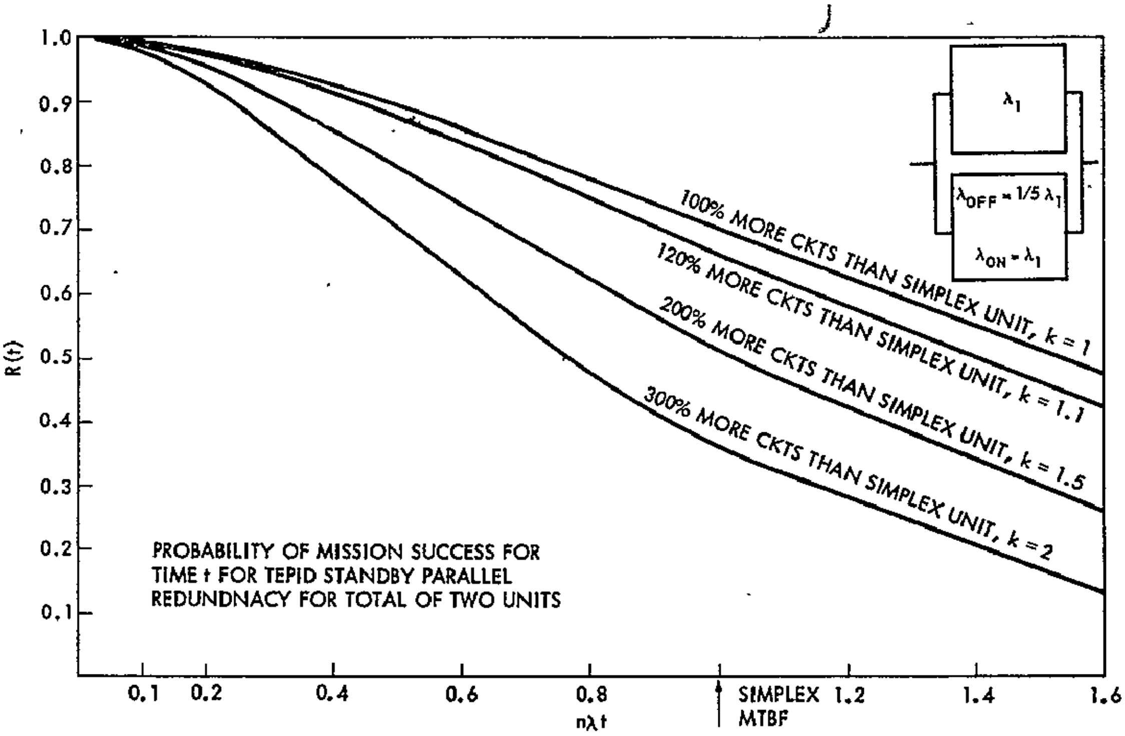


Figure 6–Tepid parallel redundancy for total of two units.

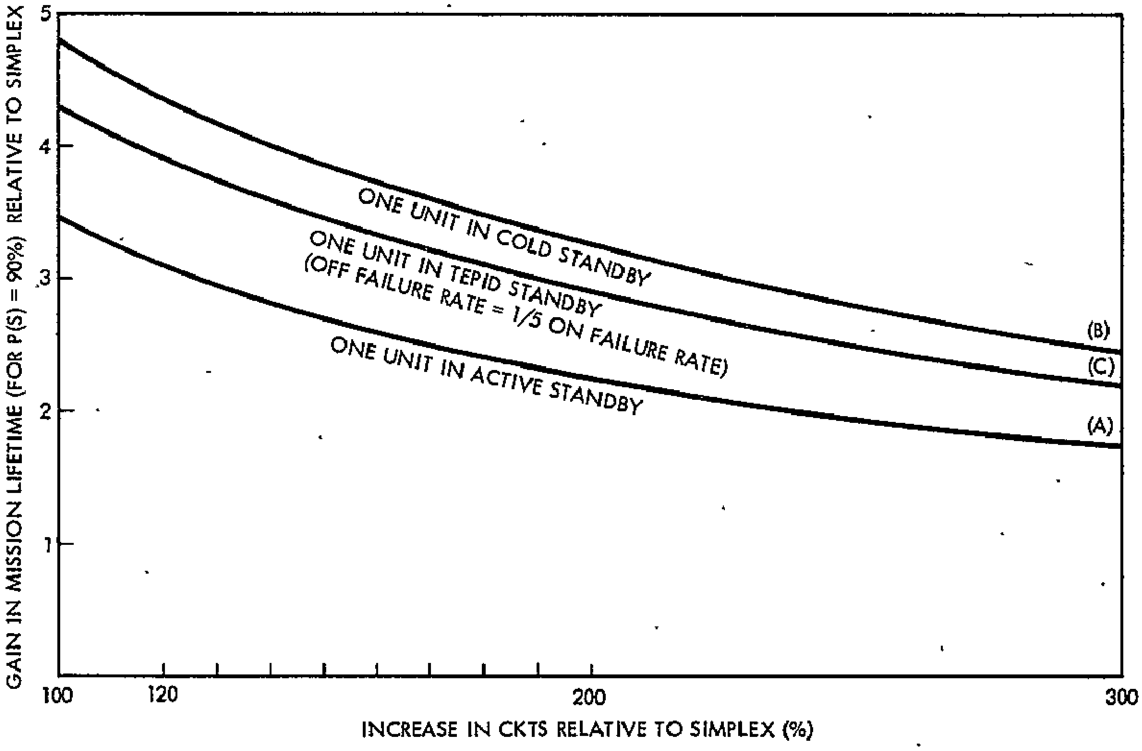


Figure 7–Tepid parallel redundancy for one unit in standby.

of two standby units, for which three units would be in parallel, another set of curves can be generated. The reliability curves that support the gain curves are included in Appendix B. Hereafter, all support curves will be included in this appendix. The following expressions for parallel redundancy of three units are then used:

For active standby,

$$R(t) = 1 - (1 - e^{-k\tau})^3.$$

For cold standby,

$$R(t) = e^{-k\tau}\left[1 + k\tau + \frac{(k\tau)^2}{2}\right].$$

For tepid standby where the off-failure rate is 1/5 of the on-failure rate,

$$R(t) = e^{-k\tau}\,[1 + 5(1 - e^{-0.2\,k\tau}) + 15(1 - e^{-0.2k\tau})^2\,].$$

Figure 8 gives the gain in mission lifetime relative to simplex for $P(S) = 90$ percent.

When three units are placed in standby with the first unit for a total of four units, the following set of expressions are employed:

For active standby,

$$R(t) = 1 - (1 - e^{-k\tau})^4.$$

For cold standby,

$$R(t) = e^{-k\tau}\left[1 + k\tau + \frac{(k\tau)^2}{2} + \frac{(k\tau)^3}{6}\right].$$

For tepid standby where off-to-on failure rate is 1/5,

$$R(t) = e^{-k\tau}\left[1 + 5(1 - e^{-0.2\,k\tau}) + 15(1 - e^{0.2k\tau})^2 + 35(1 - e^{-0.2k\tau})^3\right].$$

Gains in mission lifetime for this redundancy are shown in Figure 9.

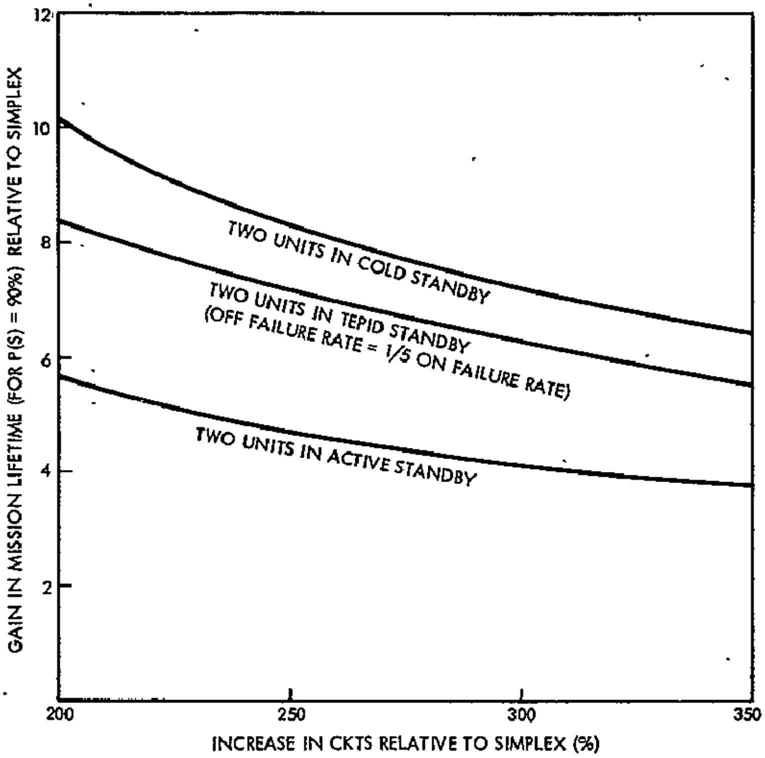


Figure 8–Parallel redundancy for a total of three units.

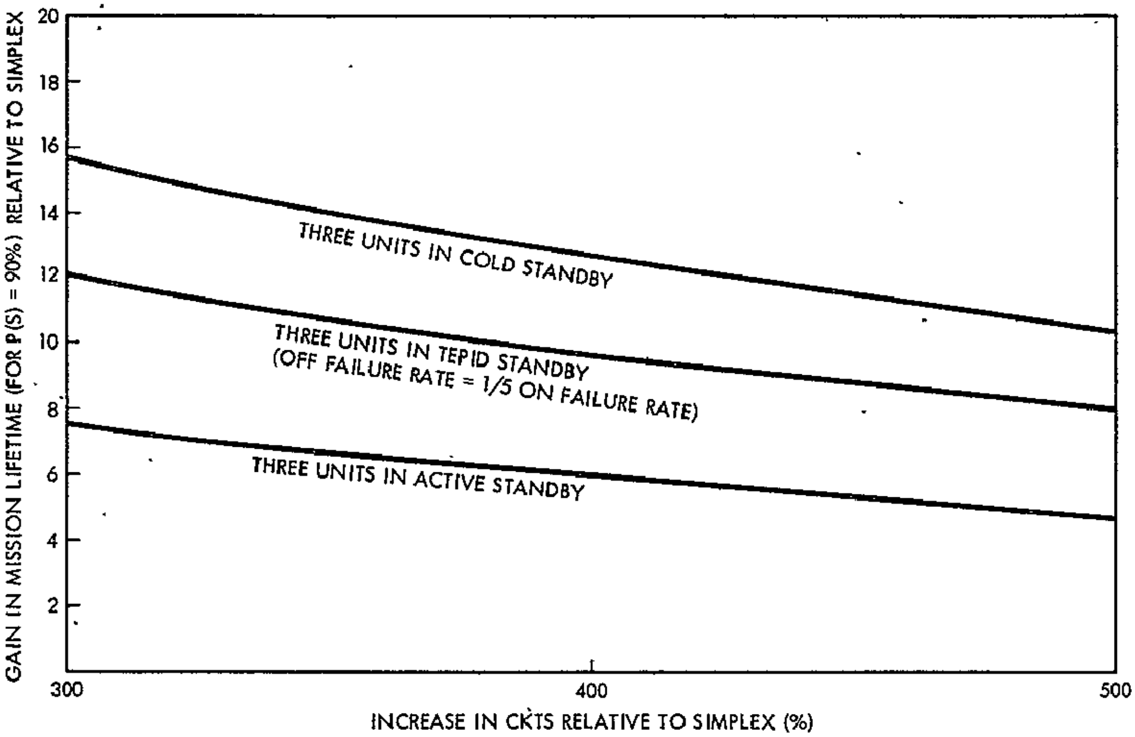


Figure 9–Parallel redundancy for a total of four units.

SUBDIVIDING

In the second technique, the simplex unit is subdivided. Each subdivision, or subunit, is made redundant by paralleling it with a like subunit. Again, for weighing advantages and disadvantages of such a technique, it is assumed that the original simplex unit can be divided into subunits where each subunit has an equal number of circuits (an unrealistic but informative approach). Figure 10 presents a block representation of a few such subdivisions. For example, in block E, the simplex unit is divided into four subunits, each having $n/4$ circuits, and each subunit is paralleled by an equivalent subunit. For this ideal case, a total of $2n$ circuits are employed. Realistically, a penalty of additional circuits will be required to implement the redundancy of each pair of subunits. This is shown in block F for the case of using 10 percent more circuits with each subunit, which would result in a 120-percent circuit increase over the original simplex unit.

In a like routine, a family of different numbers of subdivisions, each for several penalty percentages of additional circuits, are considered. To plot reliability as a function of time for such a system in which each paralleled subsystem comprises a redundant pair, the following expression was used to give resultant reliability for active redundancy:

$$R(t) = (2e^{-k\tau/P} - e^{-2k\tau/P})^P$$

where

$\tau = n\lambda t,$

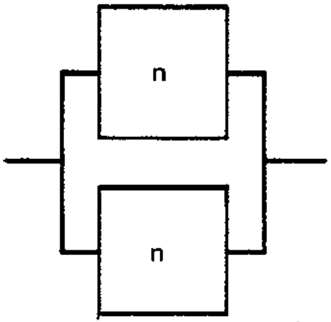
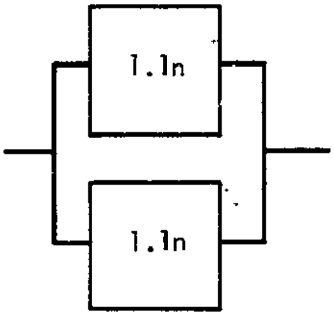
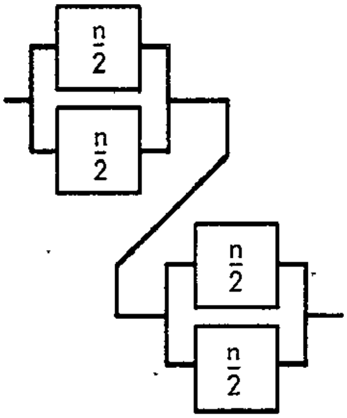
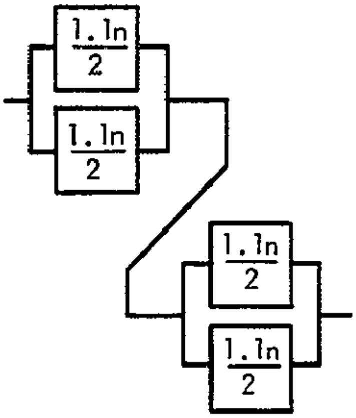
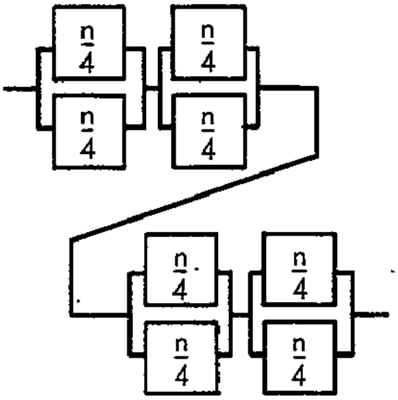
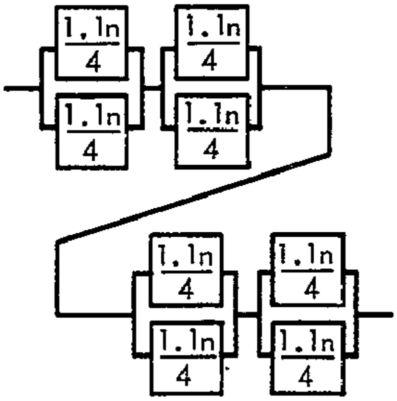
APPLICATION	100% MORE CKTS	120% MORE CKTS
Placing one unit in parallel with the original unit, as discussed in first technique.	 (a)	 (b)
Subdividing the unit into two subunits and applying redundancy to each subunit, for second technique.	 (c)	 (d)
Subdividing the unit into four subunits and applying redundancy to each subunit, for second technique.	 (e)	 1.1n/4 1.1n/4 1.1n/4 1.1n/4 1.1n/4 1.1n/4 1.1n/4 1.1n/4 (f)

Figure 10—Subdividing to achieve gain in mission lifetime.

k = ratio of number of circuits in each unit for the redundant system to the number of circuits in the original simplex unit,

and

P = number of subdivisions.

In Figure 11 a set of plots is given for subdividing the unit into 2, 4, 8, 16, and 32 subunits when each paralleled subunit is active. As in previous curves, the ordinate gives the gain in mission lifetime (for 90-percent probability of success) over that of the simplex unit. The supporting curves are given in Appendix B, from which similar data may be plotted for other probabilities of success. [Also see Appendix A for a discussion of mission lifetime gain as a function of different choices of $P(S)$.]

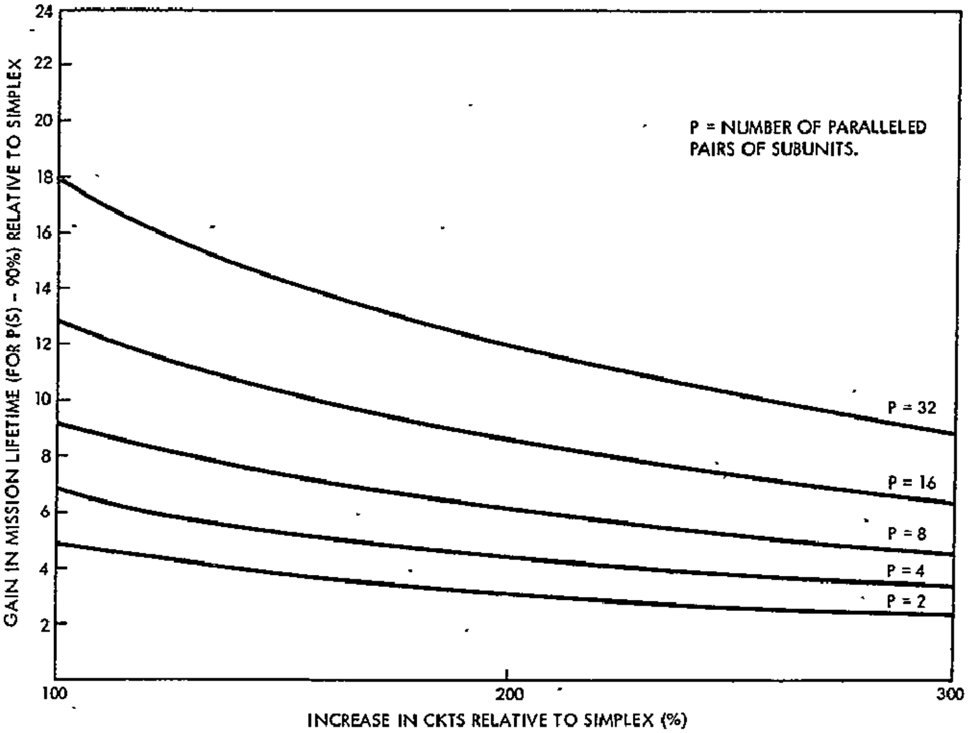


Figure 11–Subdividing and using active redundancy with each subunit.

For cold standby, the following expression gives system reliability:

$$R(t) = \left(e^{-k\tau/P} + \frac{k\tau}{P}e^{-k\tau/P}\right)^{P}.$$

A family of curves for 2, 4, 8, 16, and 32 subdivisions is given in Figure 12, and the supporting curves in Appendix B.

COLUMNIZING

The third and last technique in Part 1 is columnizing. Not all functional units lend themselves to this technique, especially to efficient columnizing. In this technique, a unit is divided into several columns. An ideal unit for this technique is one in which there is a large number of parallel operations and data transfers. Figure 13 presents a simplified example of columnizing without column switching circuitry. When bit n is independent of bit $n + 1$ during an

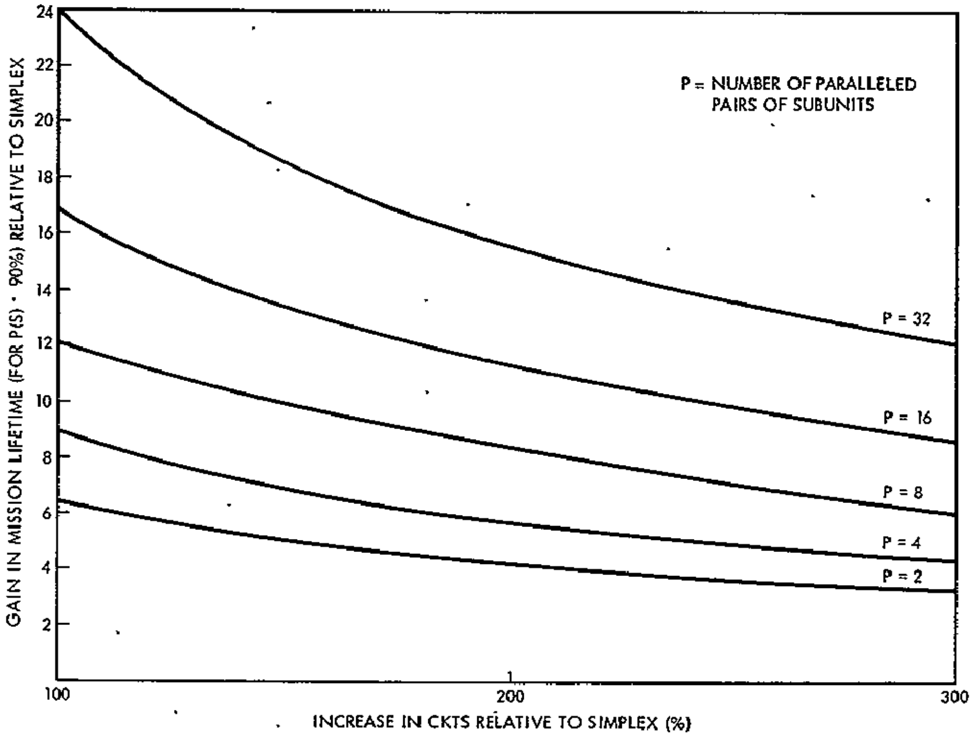


Figure 12–Subdividing and using cold standby redundancy with each subunit.

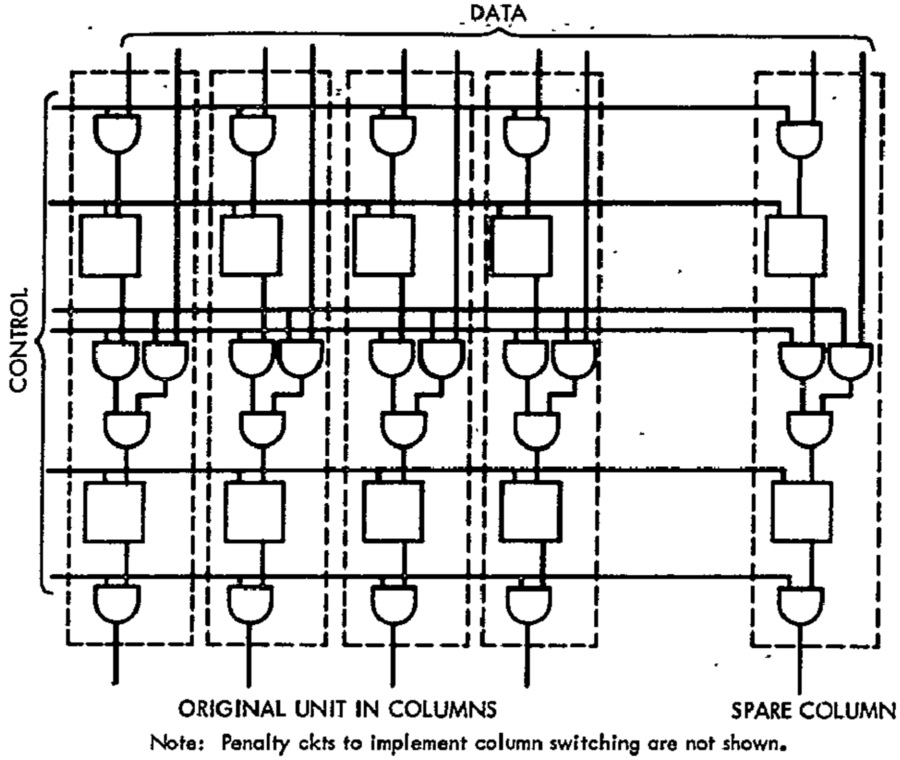

DATA
CONTROL
ORIGINAL UNIT IN COLUMNS
SPARE COLUMN
Note: Penalty ckts to implement column switching are not shown.

Figure 13–Simplified example of columnizing.

operation or data transfer to another register or through gating, then these registers can be readily columnized into one-bit columns.

A failure in the unit is repaired by switching out the column that contains the malfunction and switching in the spare column. Ideally, column switching only requires switching circuitry at the inputs and outputs of each column. In practice, specialized extra circuits would be required within the columns to effect column separation because, in areas, there is dependence of one bit to another, such as in a parallel adder.

Consider a simplex unit of n circuits that can be columnized into $1/k_1$ columns as shown in Figure 14. The column then contains k_1n circuits. The

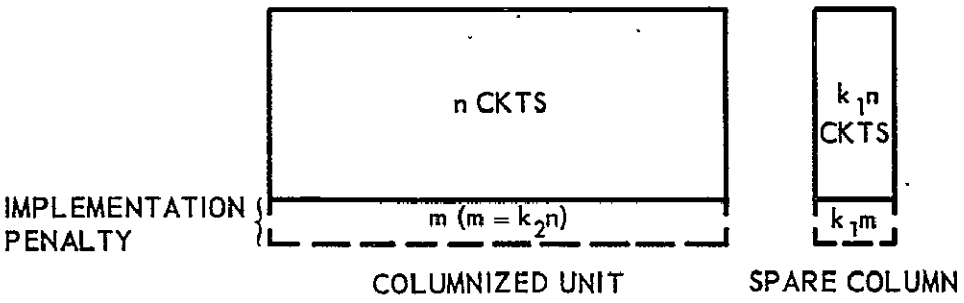


Figure 14–Representation of columnized simplex unit, spare column, and implementation penalty.

expected penalty in the way of additional circuits required to implement switching capability is represented by m for the original unit and k_1m for the spare column. Let $m = k_2n$, where the implemented columnized unit contains the following total circuits:

$$\begin{aligned}\text{Total unit circuits} &= n+m \\ &= n+k_2n \\ &= n(1+k_2).\end{aligned}$$

For the column

$$\begin{aligned}\text{Total column circuits} &= k_1(n+m) \\ &= k_1(n+k_2n) \\ &= k_1n(1+k_2).\end{aligned}$$

The reliability expression for active columnizing can be derived from the general expression for a system having two unequal portions in parallel redundancy so that a failure in the main unit can, by some means, be replaced by the second portion. It is given as

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

where λ_1 and λ_2 are the total failure rates for each portion. Let λ_1 equal total failure rate of the main unit (with its additional implementation circuits),

$$\lambda_1 = n(1 + k_2)\,\lambda,$$

and let λ_2 equal total failure rate of the added spare column,

$$\lambda_2 = k_1 n(1 + k_2)\,\lambda;$$

then the reliability for the columnized system becomes

$$R(t) = e^{-n\lambda(1 + k_2)\,t} + e^{-n\lambda k_1\,(1 + k_2)\,t} - e^{-[n\lambda(1 + k_2) + n\lambda k_1\,(1 + k_2)]\,t}$$

Then

$$R(t) = e^{-(1 + k_2)\tau} + e^{-k_1\,(1 + k_2)\tau} - e^{-(1 + k_1)\,(1 + k_2)\tau},$$

where

k_1 = column size relative to main unit,

k_2 = additional implementation circuits per column relative to the unmodified column,

and

$\tau = n\lambda t.$

The total additional circuitry relative to the original simplex unit is then

$$k_1 + k_2 + k_1 k_2.$$

Families of reliability curves were plotted for selected values of k_1 and k_2 and are included in Appendix B. From these, the 90-percent $P(S)$ intersections were taken, and the curves of Figure 15 were plotted. The same type of scaling is used as in previous curves. The solid lines represent the column size, and

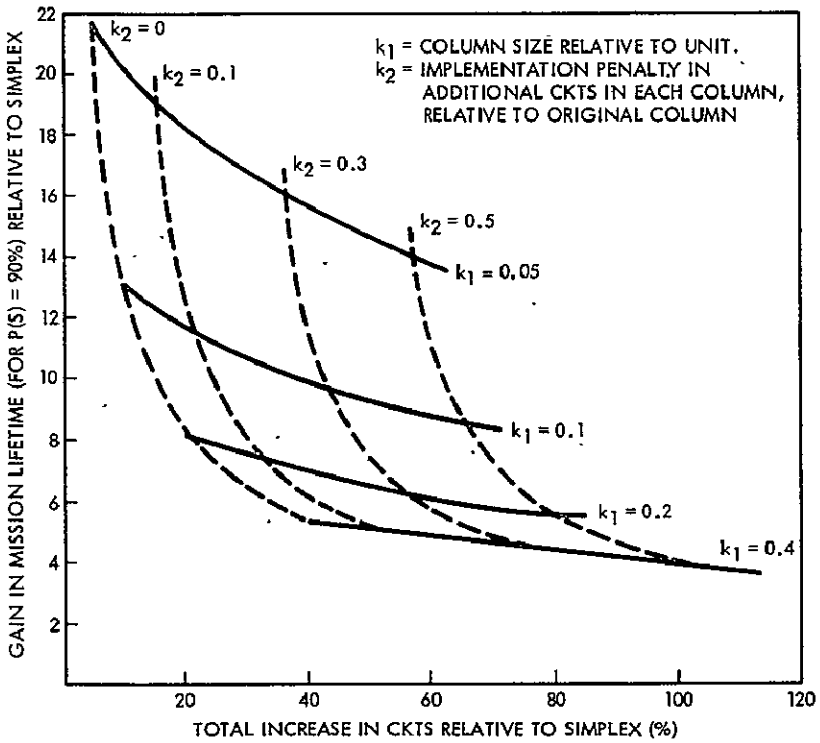


Figure 15—Active columnizing.

the dashed lines represent the implementation penalty of additional circuits. The ideal but unachievable curve for $k_2 = 0$ is included as an upper bound.

For a standby cold column, another set of curves can be generated. The expression is derived from the general expression of reliability for a parallel redundant system having a cold ($\lambda = 0$) standby portion. It is given by

$$R(t) = \frac{\lambda_2 e^{-\lambda_2 t} - \lambda_2 e^{-\lambda_1 t}}{\lambda_1 - \lambda_2}.$$

As previously explained for the columnized model,

$$\lambda_1 = n\lambda\,(1 + k_2)$$

$$\lambda_2 = n\lambda k_1 (1 + k_2).$$

Letting $\tau = n\lambda t$, the above expression reduces to

$$R(t) = \frac{(1 + k_2)\, e^{-k_1 (1 + k_2)\tau} - k_1 (1 + k_2)\, e^{-(1 + k_2)\tau}}{(1 - k_1)(1 + k_2)}$$

Curve families for this expression are given in Appendix B. The resultant curves for mission lifetime gain at the expense of total extra circuits for this case are given in Figure 16.

SUMMARY

For comparison with the foregoing techniques, a composite set of most of the curves is given in Figure 17. To avoid clutter, the subdividing technique does not include curves for 2, 4, or 8 subunits. Also excluded are some of the curves that were presented in the columnizing technique. The simplex unit is

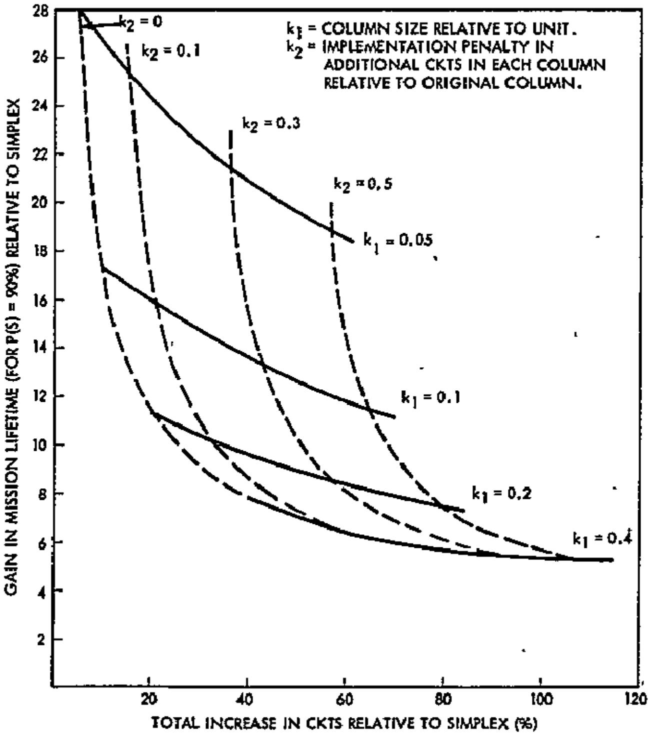


Figure 16–Cold columnizing.

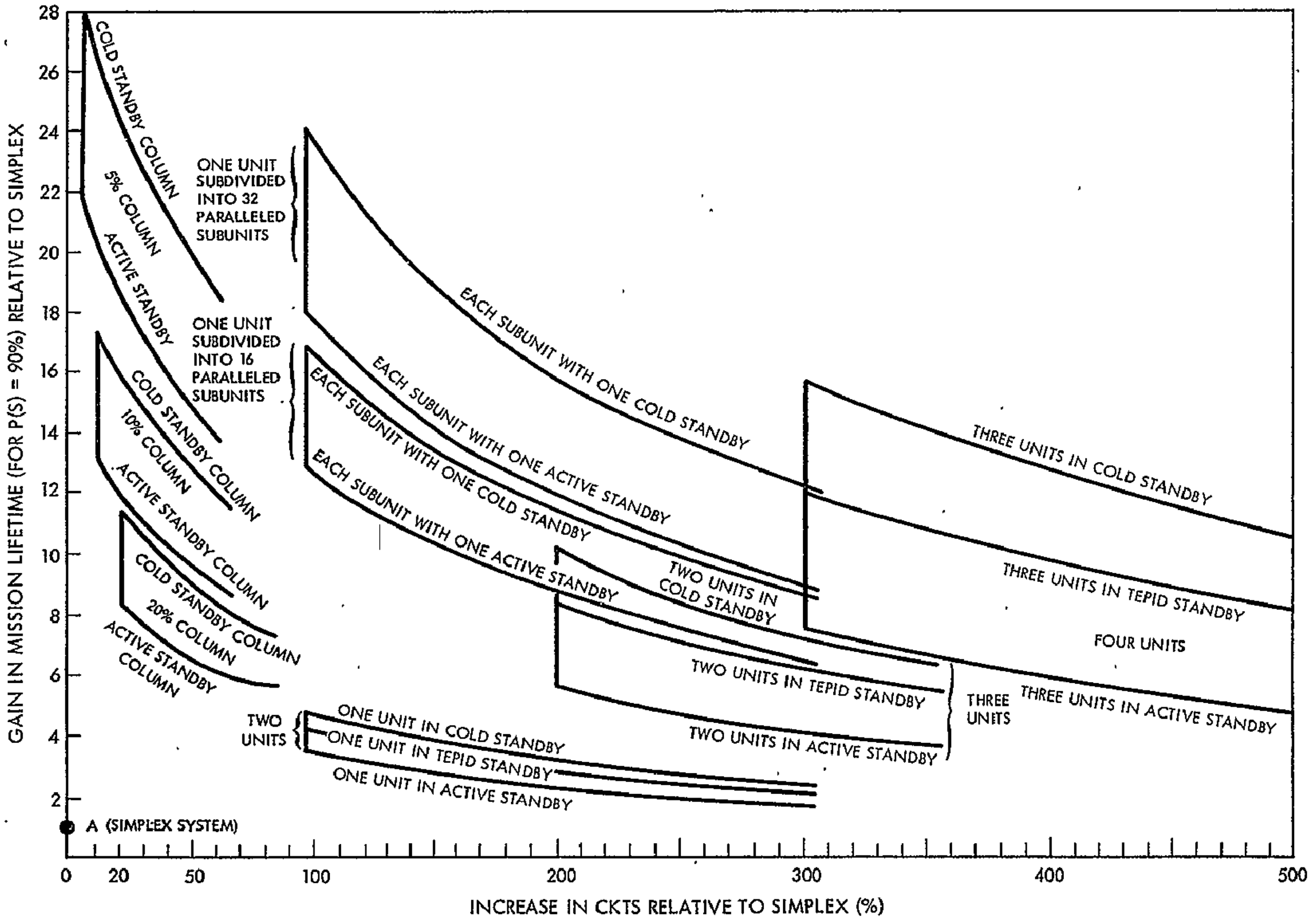


Figure 17—Composite of graphs for comparison of redundant techniques.

represented by point A, where its 90-percent probability of success is normalized to one. All other curves then represent the obtainable gain in mission lifetime, at the expense of additional circuits, relative to the simplex unit. It is, of course, desirable to be to the left and up on the graph. Clearly, this is best accomplished by columnizing—if it can be efficiently implemented and if other factors do not create offsetting problems.

It is worth realizing when a portion of a curve is applicable and when it is not. For example, in subdividing, if the subunits have few circuits, then the left portion of the curve could not be achieved. Also, if the subunits are large and have relatively few inputs and outputs, then the left portion of the curve might be achievable. For paralleled units, if the units are relatively large, then the right portion of these curves are not realizable. The curves for cold standby and active parallel serve as upper and lower bounds for each case, where the powered-off failure rate of a standby could lie anywhere within, depending on the ratio of off-to-on failure rate.

Presentation of the foregoing material is intended to provide some measure of comparison between three general techniques of redundancy. The merits of one technique over another for a particular system depend on such factors as—

(1) Whether it can be done. (Can, for example, the unit or part of the unit be columnized?)

(2) Whether it is expedient (or cost effective).

(3) Whether fault isolation and self-repair require human intervention.

(4) Whether it will impact scheduling. (For example, will longer and more intricate testing and evaluation be required to prove operational status?)

(5) Whether a single-point failure manifests itself in a degraded rather than a failed system. If so, what are the rules now for comparing?

In any final, real system employing redundancy, the ideal conditions that were assumed for the sake of comparing techniques will not present themselves. Judgment on design approaches to achieve acceptable reliability will have to include the expected functional and hardware inconsistencies that will deviate from these conditions. However, a basic understanding of the foregoing should provide considerable insight into designing for reliability.

PART 2
APPLYING REDUNDANCY TO EXISTING SUBSYSTEMS

INTRODUCTION

Part 2 is devoted to applying reliability models to a real system in different configurations to determine the optimum configuration for a long-mission lifetime. The use of existing simplex units and devices that have predicted failure rates enables calculations to be made that yield absolute reliability predictions for the various configurations.

The subsystem discussed is the On-Board Processor (OBP) that has been developed by GSFC. The OBP is a general purpose, stored program spacecraft computer. It consists of three functionally and physically separate units: a central processing unit (CPU), a memory unit, and an input-output unit (I/O). It is an 18-bit parallel machine with 2μs memory cycle time. The memory unit is fabricated in 4K modules and is scheduled to fly on the Orbiting Astronomical Observatory, Flight C, in 1971. The OBP for this flight will be a simplex system and will fly as an experiment. It will provide selected backup and work-around functions to other on-board subsystems such as the stabilization and control subsystem and the data handling subsystem. In future flights, the OBP will take on more responsible tasks.

The present design of the OBP provides for improving reliability by adding up to two spare CPU's, two spare I/O's, and 16 memory units. Thus, the first approach discussed in Part 1, that is, spare units, could be used to obtain higher confidence in the success of future missions where the OBP would take on line functional responsibilities. The following analyses predict the mission lifetimes that can be obtained through the use of those configurations that are within the present design, plus a few other design approaches.

CPU AND I/O RELIABILITY

Considered first is improvement of the CPU and I/O as a working pair of units, the purpose being to bring these up to long lifetimes and later to look into improving memory lifetime. Both the CPU and the I/O units have very nearly the same failure rate because they both contain approximately equal amounts of the same type of chip.* The CPU failure rate is based on the Fairchild 9040 series screened chips, which yield a failure rate per chip of 0.003 percent failures per 1000 hours.† Each unit contains close to 800 chips, which gives an MTBF of 4.75 years per unit.

When a failed unit is defined as any single point failure in the unit, the simplex pair reliability will be the product of the reliability functions of both the

*Other conditions, such as wiring contacts, affect reliability, but for the purpose of making coarse improvements in reliability, these conditions were not included. It has been estimated, for example, that the average number of wiring contacts used per chip would not alter the chip failure rate by more than 10 percent.

†As used by Westinghouse Defense and Space Center.

CPU and the I/O. The resultant MTBF for the working pair is then 2.38 years. The 90-percent probability of success predicts a mission lifetime of less than one year.

When redundancy is applied, the following configurations are evaluated:

(a) One spare working pair.

(b) Two spare working pairs.

(c) Three spare working pairs.

(d) One spare CPU and one spare I/O, each independent of the other.*

(e) Two spare CPU's and two spare I/O's, each independent of the others.*

(f) Three spare CPU's and three spare I/O's, each independent of the others.

These configurations are represented in Figure 18. In a, b, and c, each I/O is slaved to a particular CPU. In d, e, and f, each CPU and each I/O can be cross strapped to any other. To increase reliability and, more important, to conserve power, only the operating pair would be powered on. The failure rate of the powered-off units was estimated at $\lambda_{off} = 1/5\ \lambda_{on}$. Reliability was calculated with the tepid parallel redundancy expressions previously given in Part 1 and modified by a joint product for cases d, e, and f. In cases a, b, and c, the failure rate used for each pair was 4.8×10^{-5} failures per hour (f/hr), or 0.42 failure per year (f/yr). In d, e, and f, 2.4×10^{-5} f/hr or 0.21 f/yr was used separately for each unit.

*This configuration may now be implemented by the present design.

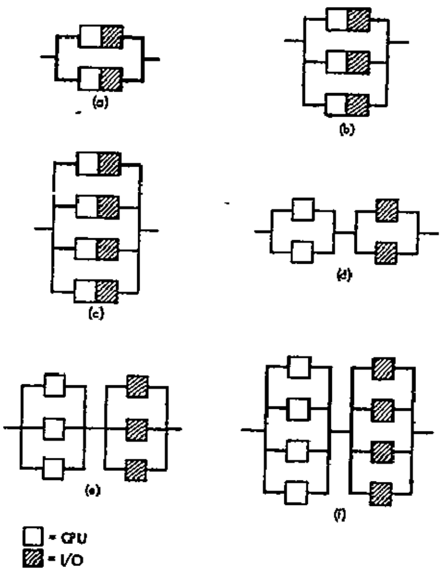


Figure 18 – Redundant configurations for improving mission lifetime of CPU and I/O.

Figure 19 gives resultant curves for all cases, including the simplex. (See Table 1 for expressions for the curves.) At this early stage, a tentative goal was established to achieve a mission lifetime of at least 3 years for $P(S) = 90\%$. Because of the close proximity of the two curves, C and E, which just met this condition, the investigation of these two cases was continued. It was necessary to determine the effect of active redundancy as well as cold redundancy because these serve as upper and lower bounds for all possible values of off-to-on failure-rate ratios. Figures 20 and 21 show the resulting curves. The bar charts high-light the need to know the true failure rates with reasonable accuracy if the mission lifetime must be predicted to better than a 1-year accuracy for these particular design configurations.

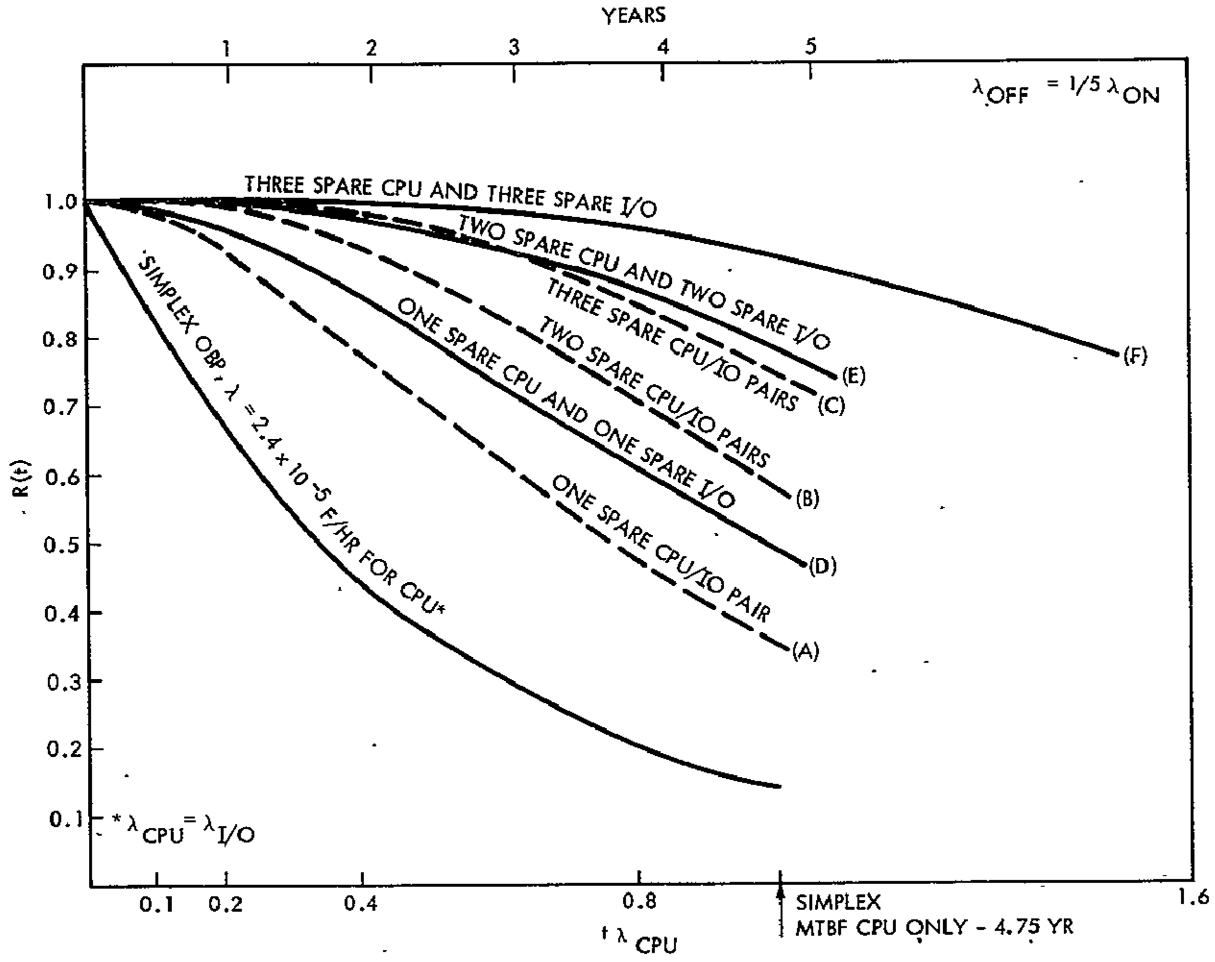


Figure 19—Reliability curves for OBP, CPU, and I/O configurations of Figure 17.

MEMORY RELIABILITY

The OBP memory system is now fabricated in 4K modules. It is presently anticipated that a future flight will require that 32K of core be operational over the entire mission. Consideration has been given to the idea of flying 64K of memory, from which the 32K would be selected by ground command. Again, it should be remembered that the worst case failure conditions are being assumed wherein a single-point failure renders a failed unit. Mission-lifetime predictions begin with the following expression:

$$P(S) = \sum_{x=k}^{m} \frac{m!}{x!\,(m-x)!}\, p^{x}\,(1-p)^{m-x},$$

where

x = number of units that must be operational,

m = total number of units that are available,

and

p = probability of success for one unit.

Table 1 — Expressions for reliability curves for Figure 20.

CONFIGURATION	λ (f/yr)	APPLICABLE RELIABILITY EXPRESSION
Simplex CPU and I/O	0.42	$R(t) = e^{-\lambda t}$
(a) One spare CPU & I/O pair	0.42	$R(t) = e^{-\lambda t} + 5\,(e^{-\lambda t} - e^{-1.2\lambda t})$
(b) Two spare CPU & I/O pairs	0.42	$R(t) = e^{-\lambda t}\left[1 + 5(1 - e^{-0.2\lambda t}) + 15(1 - e^{-0.2\lambda t})^{2}\right]$
(c) Three spare CPU & I/O pairs	0.42	$R(t) = e^{-\lambda t}\left[1 + 5(1 - e^{-0.2\lambda t}) + 15(1 - e^{-0.2\lambda t})^{2} + 35(1 - e^{-0.2\lambda t})^{3}\right]$
(d) One spare CPU and one spare I/O	0.21	$R(t) = \left[e^{-\lambda t} + 5(e^{-\lambda t} - e^{-1.2\lambda t})\right]^{2}$
(e) Two spare CPU's and two spare I/O's	0.21	$R(t) = \left\{e^{-\lambda t}\left[1 + 5(1 - e^{-0.2\lambda t}) + 15(1 - e^{-0.2\lambda t})^{2}\right]\right\}^{2}$
(f) Three spare CPU's and three spare I/O's	0.21	$R(t) = \left\{e^{-\lambda t}\left[1 + 5(1 - e^{-0.2\lambda t}) + 15(1 - e^{-0.2\lambda t})^{2} + 35\,(1 - e^{-0.2\lambda t})^{3}\right]\right\}^{2}$

$$\lambda_{CPU} = \lambda_{I/O} = 800 \text{ chips} \times \frac{0.003\%}{1000 \text{ hr-chip}} \times \frac{8760 \text{ hr}}{\text{yr}} = 0.21 \text{ f/yr}$$

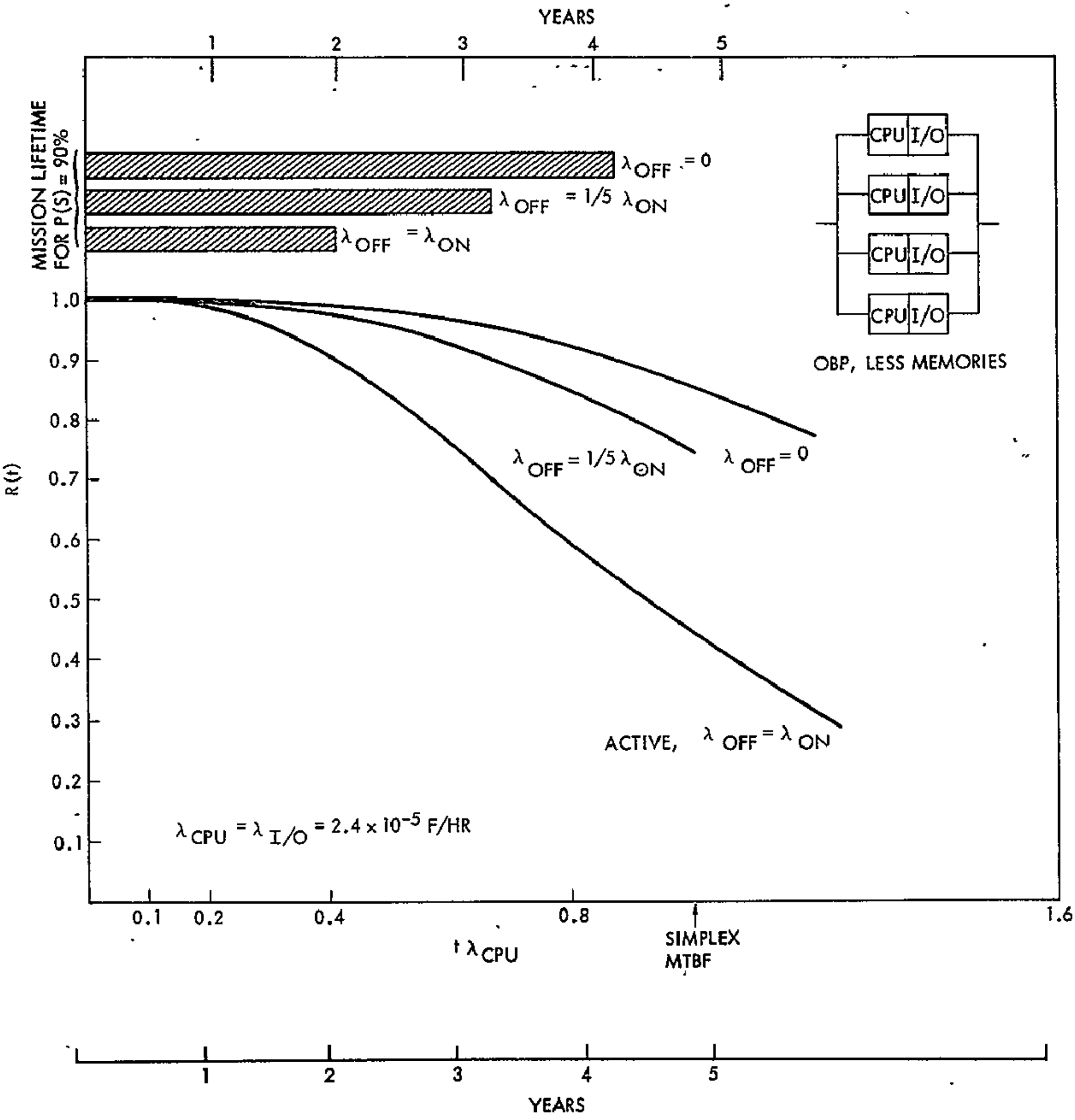


Figure 20 – Upper and lower bounds for CPU and I/O reliability for joined CPU's and I/O's.

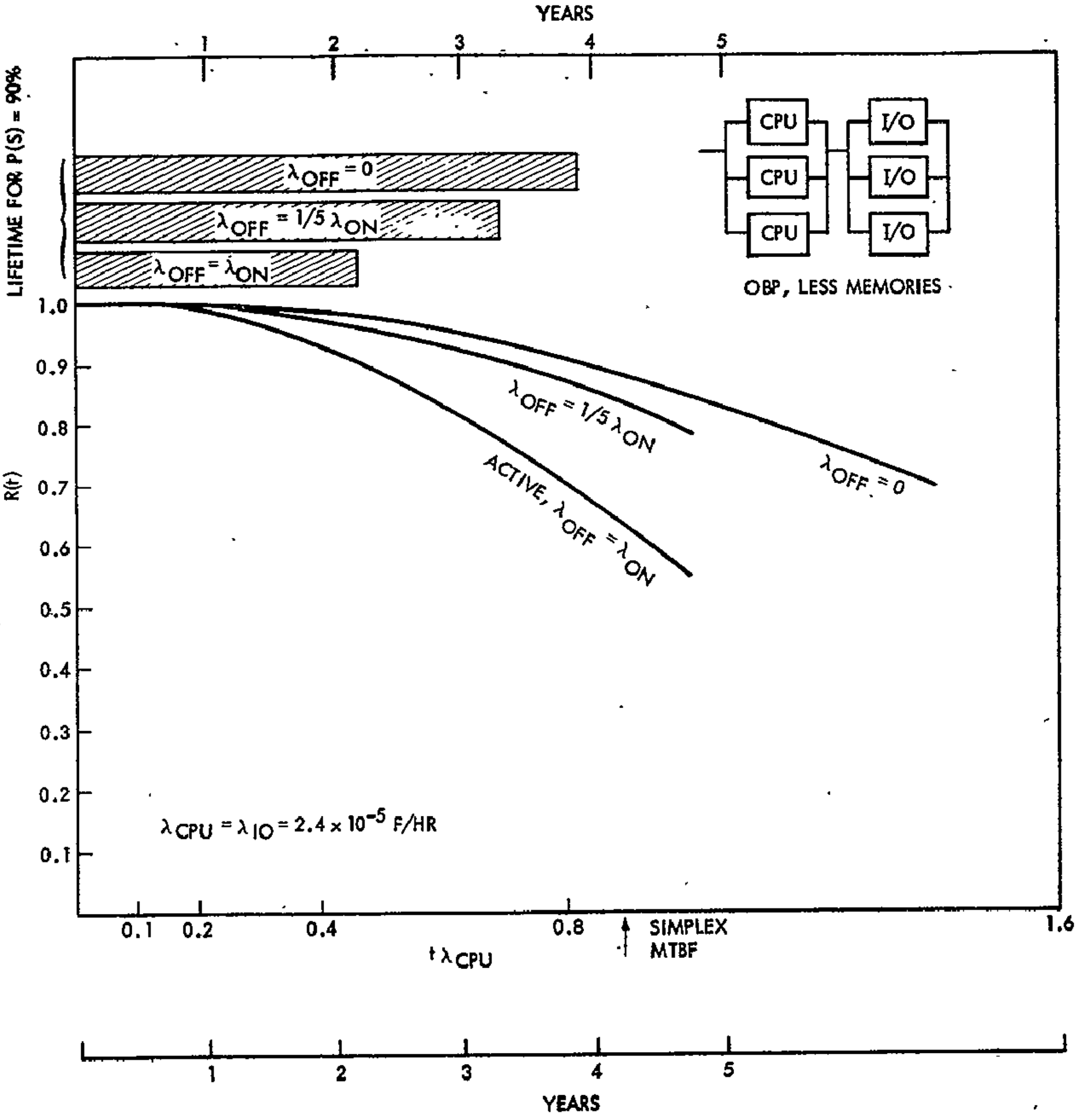


Figure 21–Upper and lower bounds for CPU and I/O reliability for separate CPU's and I/O's.

Note that $P(S)$ here is not a function of time and does not represent system reliability.

In Figure 22, the effect of this expression is shown for three configurations:

(a) Employing sixteen 4K modules to provide the required 64K of memory.

(b) Employing eight 8K modules to provide the 64K of memory.

(c) Employing four 16K modules.

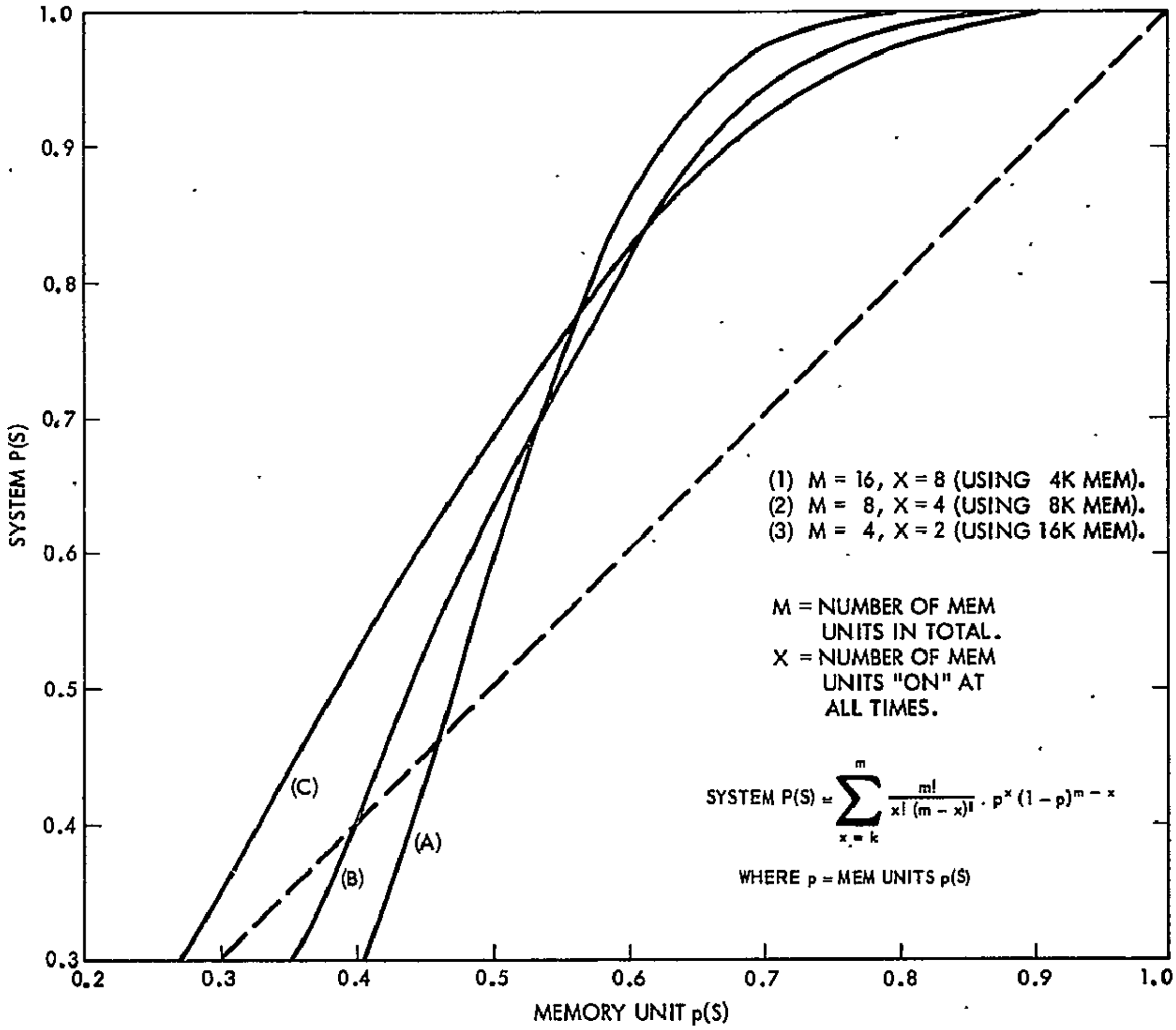


Figure 22–System P(S) as a function of unit p(S) when more units are available for use than the several that must be in use at any one time.

The abscissa is the module $P(S)$ and the ordinate is the resulting system $P(S)$ when 32K must operate.. If a particular model $P(S)$ intersects with the curve above the dashed line, a system $P(S)$ gain is realized. These gains are appreciable when the module $P(S)$ exceeds 0.6 or 0.7.

Since each module will be a simplex unit, the expression for the total memory-system reliability as a function of time can be represented as

$$R(t) = \sum_{x=k}^{m} \frac{m!}{x!\,(m-x)!} \left(e^{-\lambda t}\right)^{x} \left(1 - e^{-\lambda t}\right)^{m-x},$$

where

λ = failure rate of one memory module.

The memory-module failure rate will not be linear with module size if some redesign of the module is performed. A cursory look into the present 4K module employed by the OBP shows that the sum of all failure rates multiplied by their number of parts is 242×10^{-7} f/hr (which gives a MTBF of 41,000 hr). Two types of components account for about 70 percent of the failure rate of the module. They are switching transistors and steering diodes. Of these, the steering diodes account for 120×10^{-7} f/hr. Thus, if some redesign can enlarge core capacity with minimal impact on the use of additional diodes and transistors, an appreciable failure savings can be effected.

If a 4K module can be enlarged to 8K by enlarging each bit plane without requiring different circuit components or techniques, then the following extra components would be expected in the fabrication of 64 × 128 planes:

Part	Quantity	Failure rate (10^{-7} f/hr)	Sub-total (10^{-7} f/hr)
Switching transistors	16	.45	7.2
Transformers	8	.3	2.4
Steering diodes	128	.34	43.5
Cores	4K x 18	.00004	3
Solder connections	4000	.00005	2
			58.1

The new failure rate then would be

$$\lambda \doteq \frac{242 + 58}{242} \doteq 1.3 \times \text{ present 4K module failure rate.}$$

For a 16K module under the same conditions of being able to use the same components and techniques, the following increases would be expected:

(1) For 128 x 128 planes,

Part	Quantity	Failure rate (10^{-7} f/hr)	Sub-total (10^{-7} f/hr)
Switching transistors	32	.45	14.4
Transformers	16	.3	4.8
Steering diodes	256	.34	87
Cores	12K x 18	.00004	9
Solder connections	12,000	.00005	6
			121.2

The new failure rate would then be

$$\lambda \doteq \frac{242 + 121}{242} \doteq 1.5 \times \text{ present 4K module failure rate.}$$

(2) For 64 x 256 planes,

Part	Quantity	Failure rate (10^{-7} f/hr)	Sub-total (10^{-7} f/hr)
Switching transistors	32	.45	14.4
Transformers	16	.3	4.8
Steering diodes	128	.34	43.5
Cores	12K x 18	.00004	9
Solder connections	12,000	.00005	6
			77.7

The new failure rate would then be

$$\lambda \doteq \frac{242 + 78}{242} \doteq 1.4 \times \text{ present 4K module failure rate.}$$

Curves for active redundancy for several configurations are shown in Figure 23. It is recognized that the powered-off units would not exhibit a failure rate equal to a powered-on unit, but these curves serve as lower bounds on mission lifetime under the above conditions of cursory redesign to larger memory modules. A curve is included that represents the use of eight 4K modules without any spares. It emphasizes the gains given by redundancy as well as the need for redundancy.

Predicted reliability for the powered-off memory modules in cold standby, which will now be an upper bound, was achieved by using the following expression:

$$R(t) = e^{-N\lambda t} \sum_{i=0}^{m} \frac{(N\lambda t)^i}{i!},$$

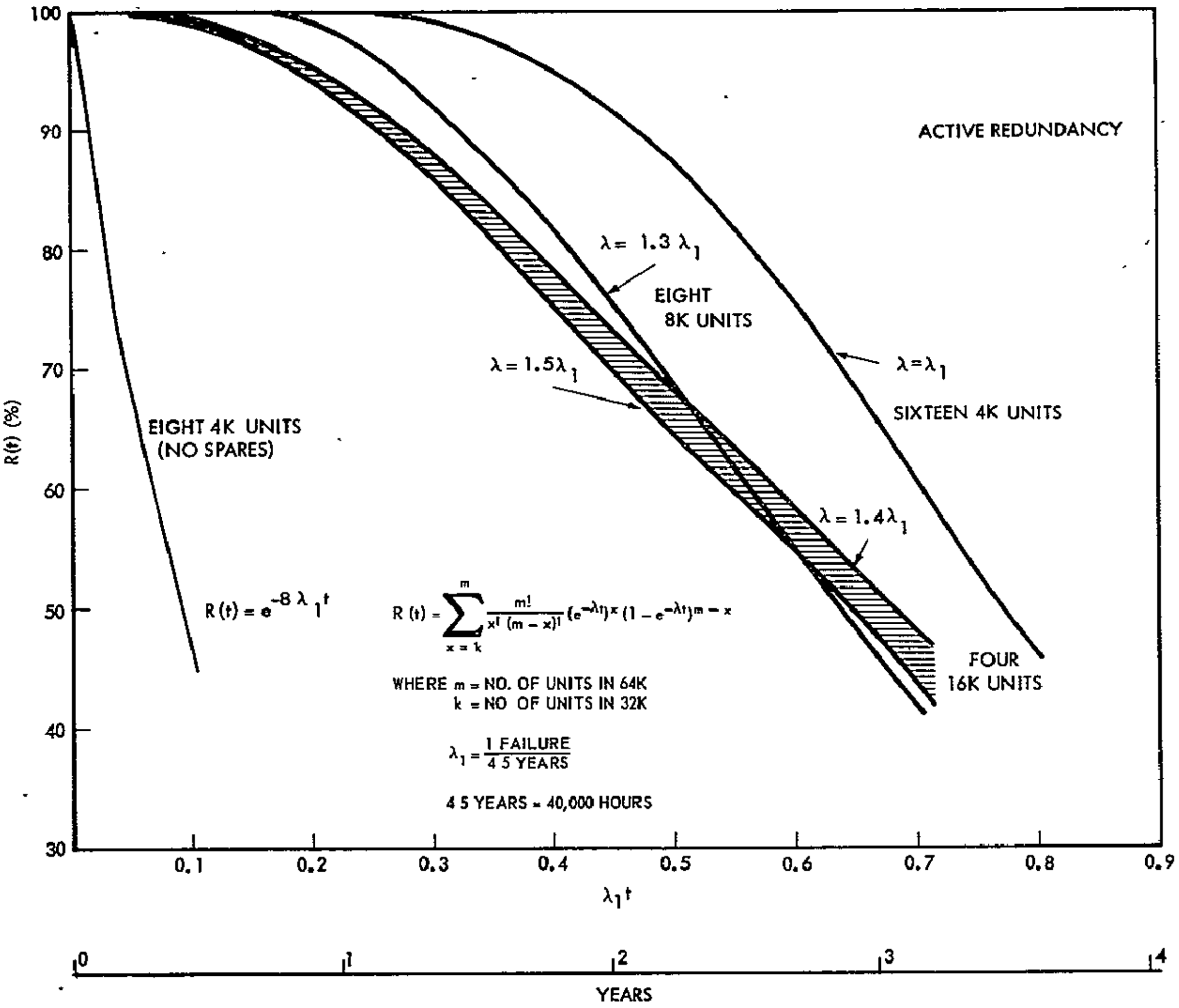


Figure 23—OBP memory reliability when 32K of memory must operate from an available 64K of memory (active standby).

where

m = number of units that are in standby,

N = number of units that must operate,

and

λ = failure rate per unit.

The resultant curves for this case are given in Figure 24. A curve is included that represents the flying of only 32K of memory without any spares. As might be expected, the configuration employing sixteen 4K modules exceeds the other

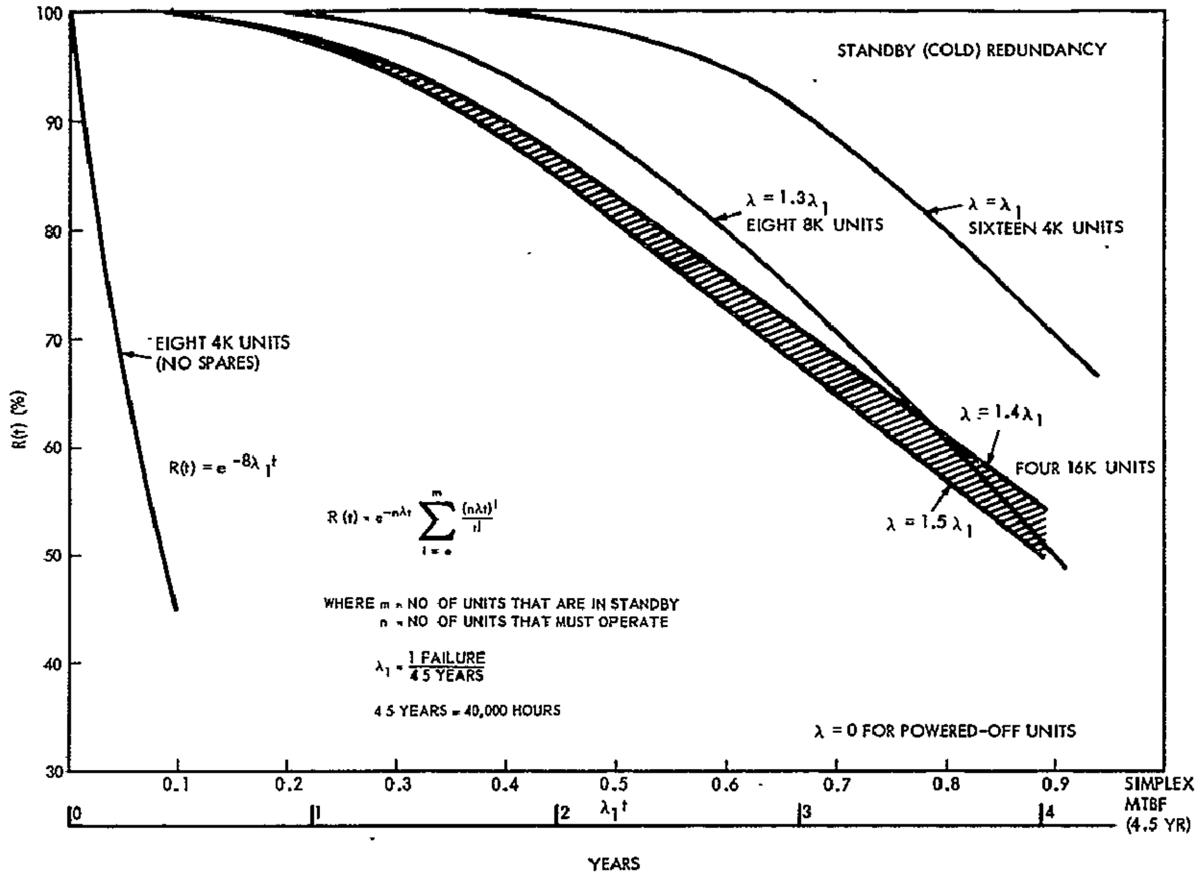


Figure 24–OBP memory reliability when 32K of memory must operate from an available 64K of memory (cold standby).

configurations despite the improvement of failure rate in proportion to memory expansion for the modified module. This is similar to the technique of subdividing, as presented in Part 1 of this paper; that is, the smaller the subdivisions the greater the return in reliability without a large penalty in additional circuits. On the other hand, unacceptable problems, such as interface cabling and greater control requirements, would eventually appear as the unit is subdivided further.

CONCLUSION

In Part 2 of this document, the discussions of configurations and their resultant reliabilities depart from the generalized discussions of Part 1 and serve to show absolute predictions based on existing designs or design techniques. Inspection of the reliability curves for the given limiting conditions of $\lambda_{off} = 0$ and $\lambda_{off} = \lambda_{on}$ indicates the amount of variance that can result in mission lifetimes, depending upon the ratio of powered-off failure rate to powered-on failure rate that is used.

The necessity for caution in making absolute predictions based on well-understood groundlines cannot be overemphasized. However, regardless of whether or not all exacting conditions are known, the need for redundancy becomes a requirement if, with reasonable confidence, acceptable mission lifetimes are to be achieved.

REFERENCES

1. Bazovsky, I., "Reliability Theory and Practice," New Jersey: Prentice-Hall, Inc., 1961.

2. Polovko, A. M., "Fundamentals of Reliability Theory," New York: Academic Press, Inc., 1968.

3. Dummer, G. W., and Griffin, N. B., "Electronics Reliability," New York: Pergamon Press Ltd., 1966.

APPENDIX A

Choice of $P(S)$

It is of practical interest to discuss the effect of different choices of $P(S)$, and the resulting gains in mission lifetime, when a simplex system is made redundant. System improvement will appear to be better if a higher $P(S)$ for mission lifetime is specified. That is, the higher the specification of $P(S)$, the greater will be the lifetime gain when a second system (or subsystem) is placed in parallel redundancy with the simplex system.

It was shown earlier in this document in the discussion on parallel redundancy that if the lifetime is based on $P(S) = 90$ percent, then a gain of 3.45 is attained under the conditions that provided curve B, Figure 2. If, instead, $P(S)$ was specified as 99 percent, then a gain of 10.5 is realized. On the other hand, if a low $P(S)$ of 80 percent were used, then a system gain of only 2.53 would result. This effect is shown in Figure 1A. The reason for this equivalent greater gain for higher $P(S)$ is that the exponential reliability curve for the simplex system begins at t_0 with a slope of -1/[system MTBF], whereas the parallel redundant reliability curve begins at t_0 with a slope of zero. In fact, all redundant techniques discussed in this document have reliability curves that begin with a zero slope.

It is understood that $P(S)$ is not a design variable. It is normally first specified, and then the system is designed to meet that specification. The improvement in mission lifetime will be a natural fallout from the reliability curves commensurate with the redundant configuration used. But it is of practical interest to point out that the effectiveness of various redundant configurations in providing increased mission lifetimes is contingent on the $P(S)$ chosen. $P(S) = 90$ percent is used throughout this document because it is a reasonable choice upon which to compare techniques.

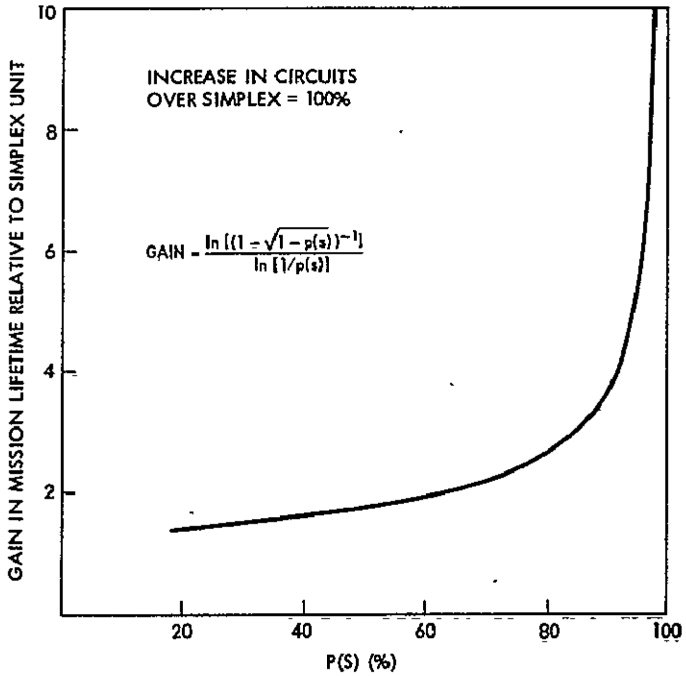


Figure 1A–Gain in mission lifetime for an active parallel pair of units, relative to the simplex unit, as a function of specified P(S).

APPENDIX B

Support Curves

This appendix contains supporting curves for the mission-lifetime gain curves of Part 1. By including these curves, mission-lifetime gains for levels of confidence other than 90 percent can be obtained.

Appendix curves 1 through 6 are curves that support parallel redundancy but are not included within Part 1:

(a) Curves 1 and 2 support active standby.

(b) Curves 3 and 4 support cold standby.

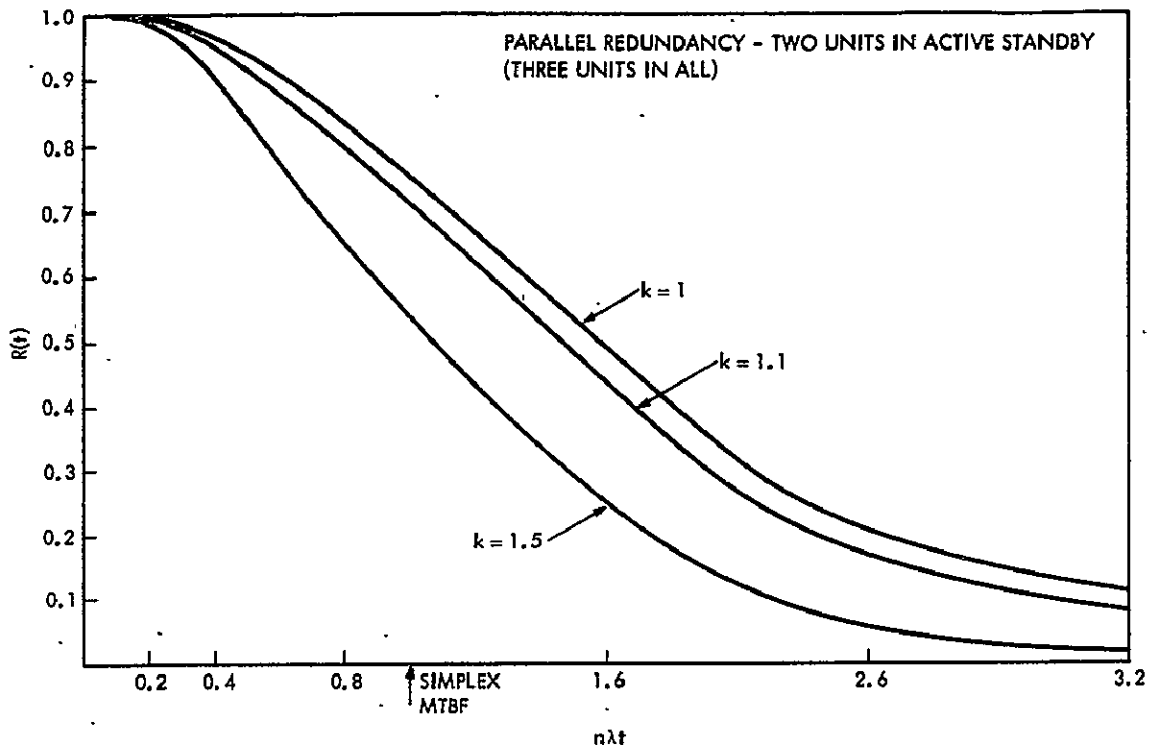
(c) Curves 5 and 6 support tepid standby.

Curves 7 through 10 support active-standby subdividing.

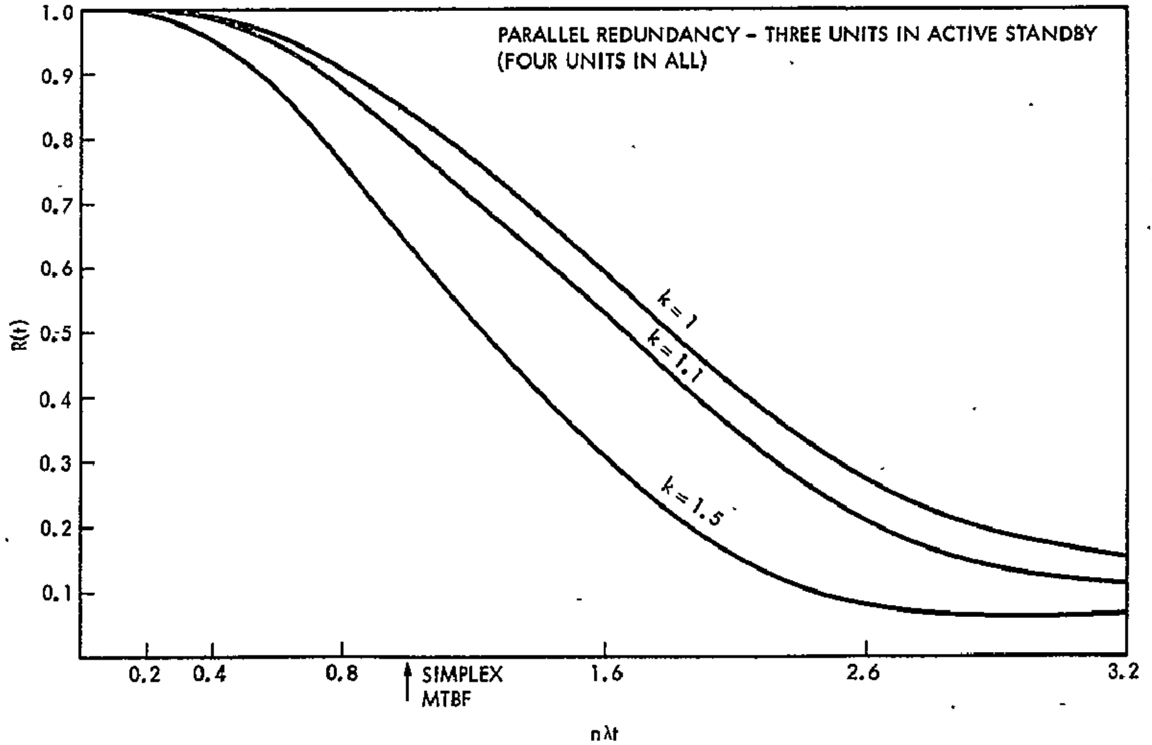
Curves 11 through 14 support cold-standby subdividing.

Curves 15 through 18 support active-standby columnizing.

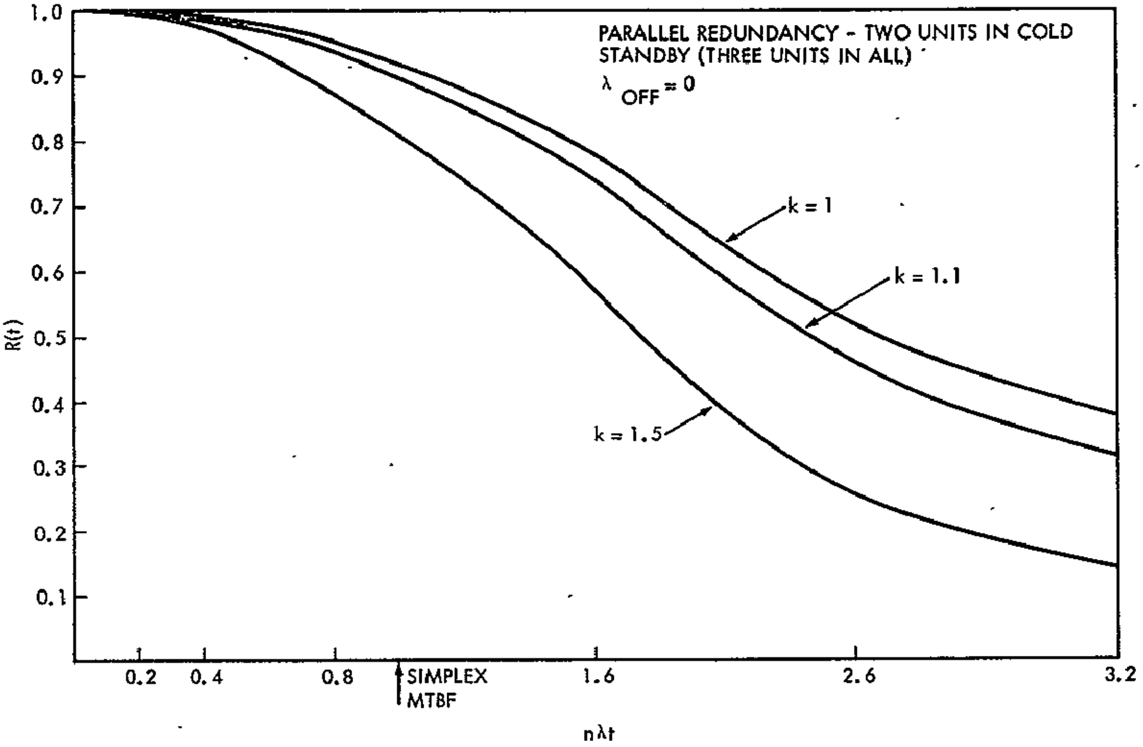
Curves 19 through 22 support cold-standby columnizing.



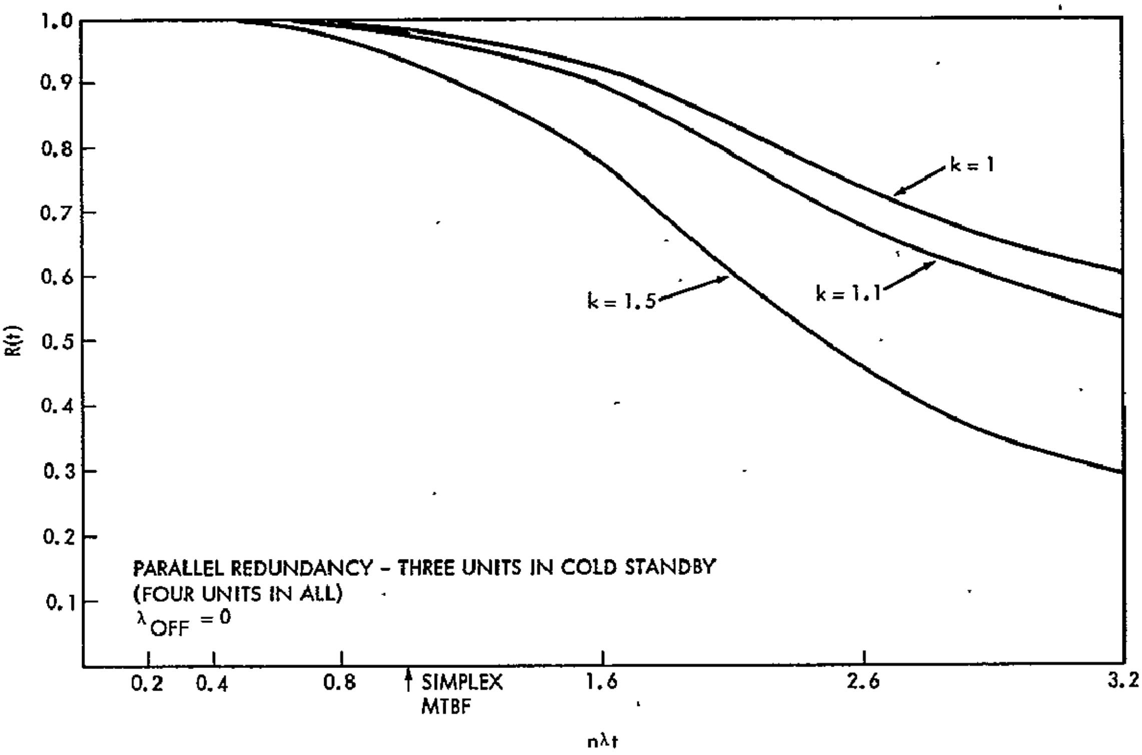
Curve 1



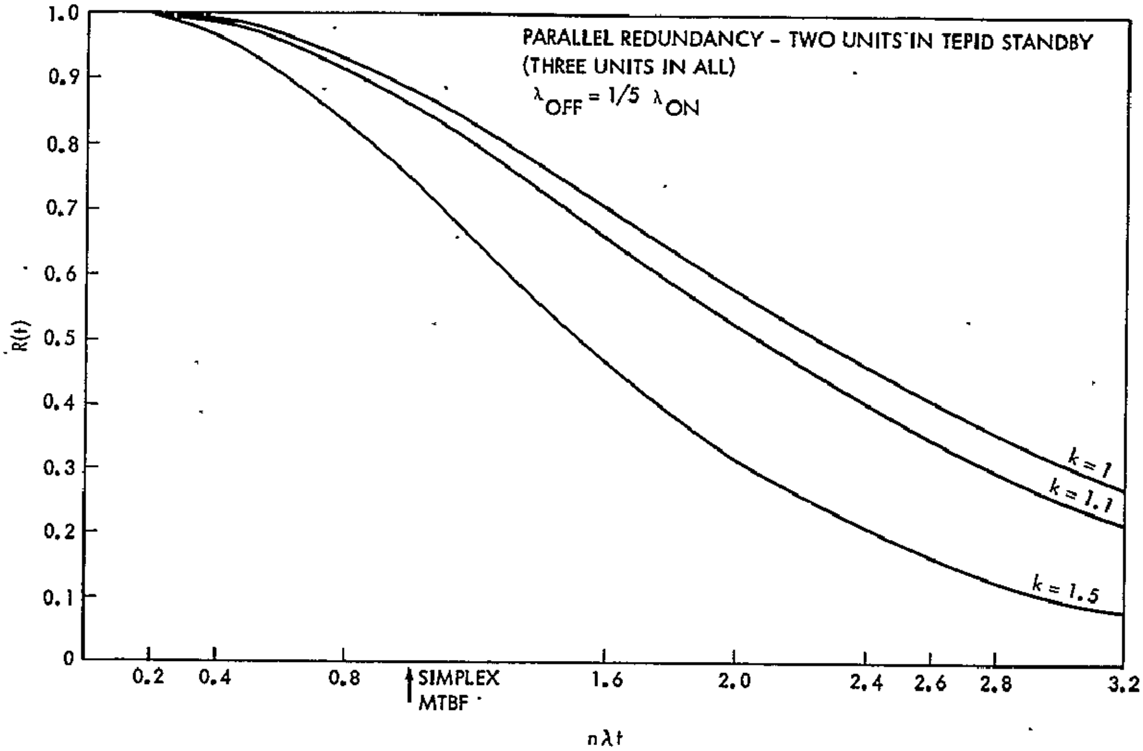
Curve 2



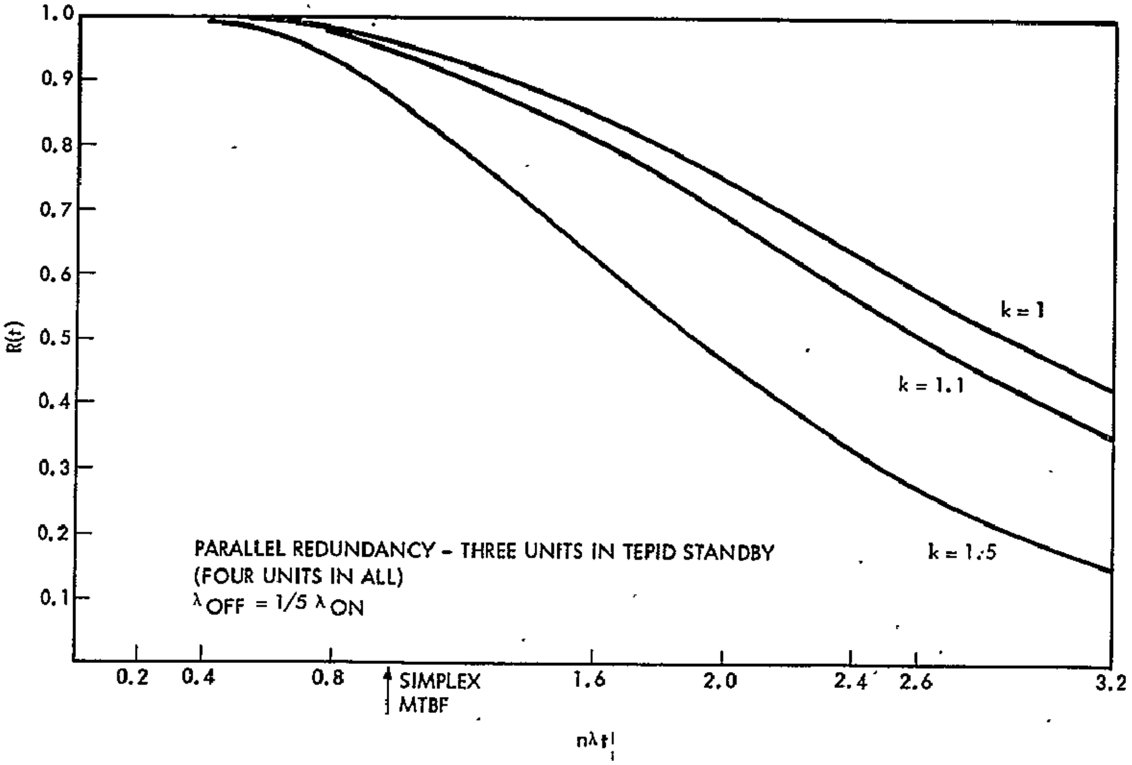
Curve 3



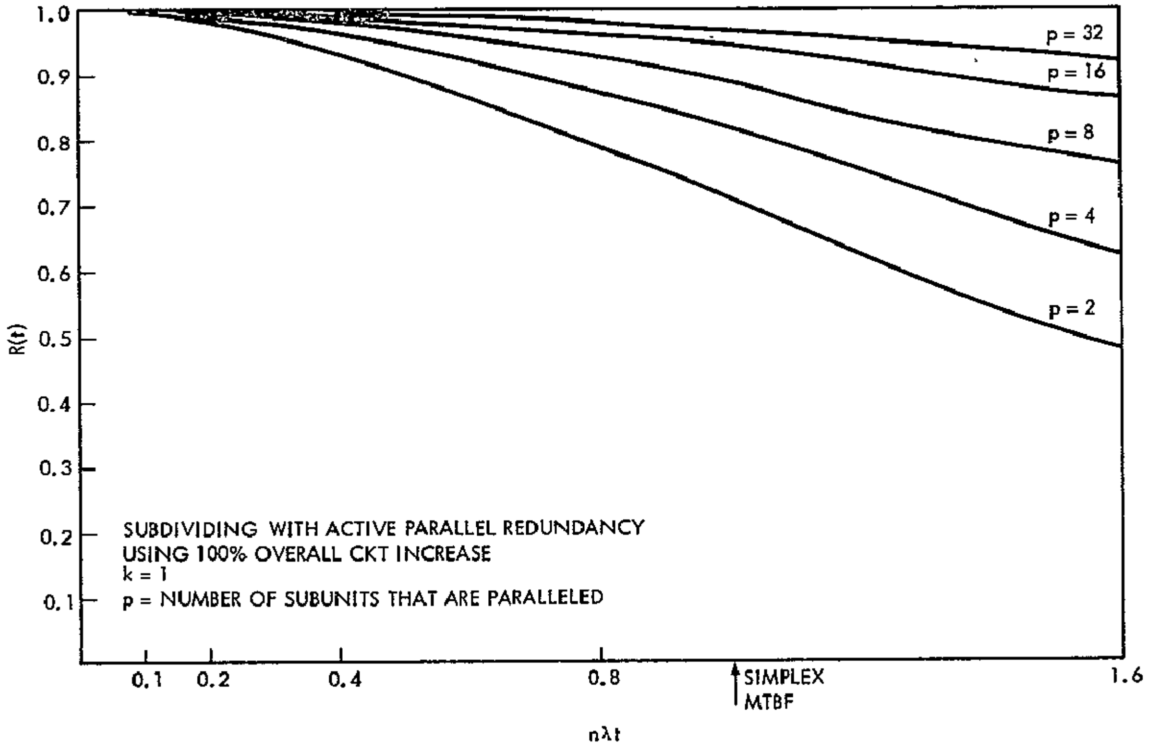
Curve 4



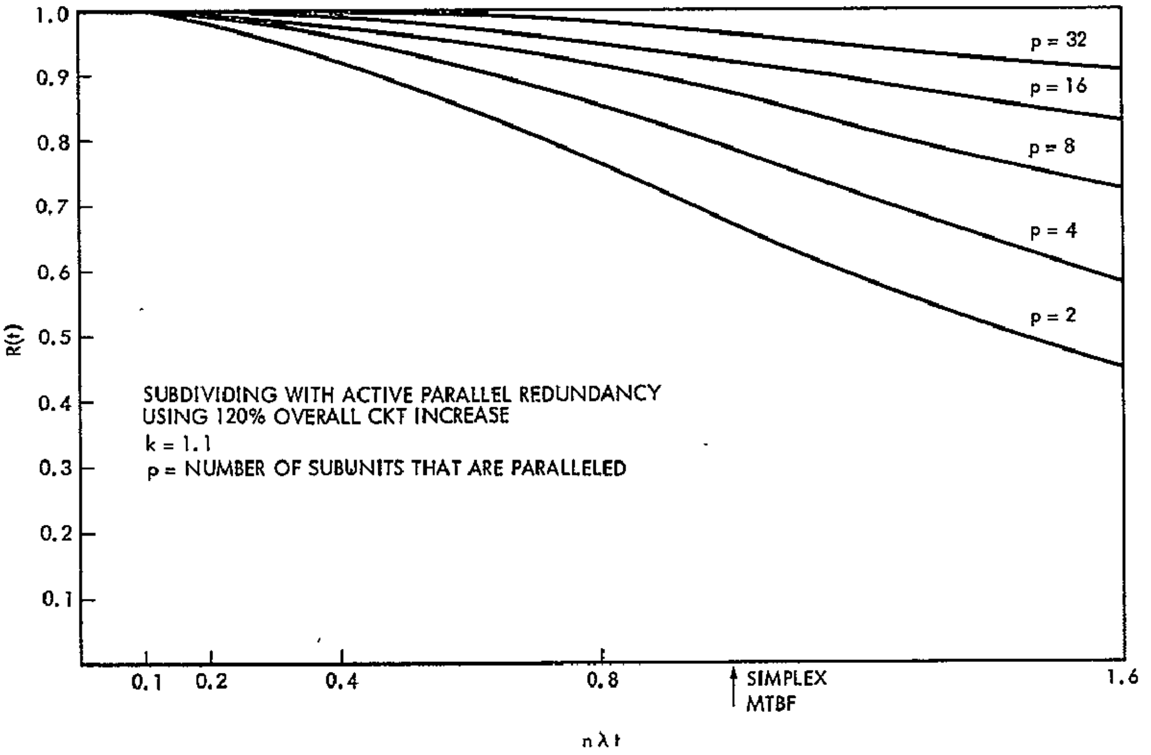
Curve 5



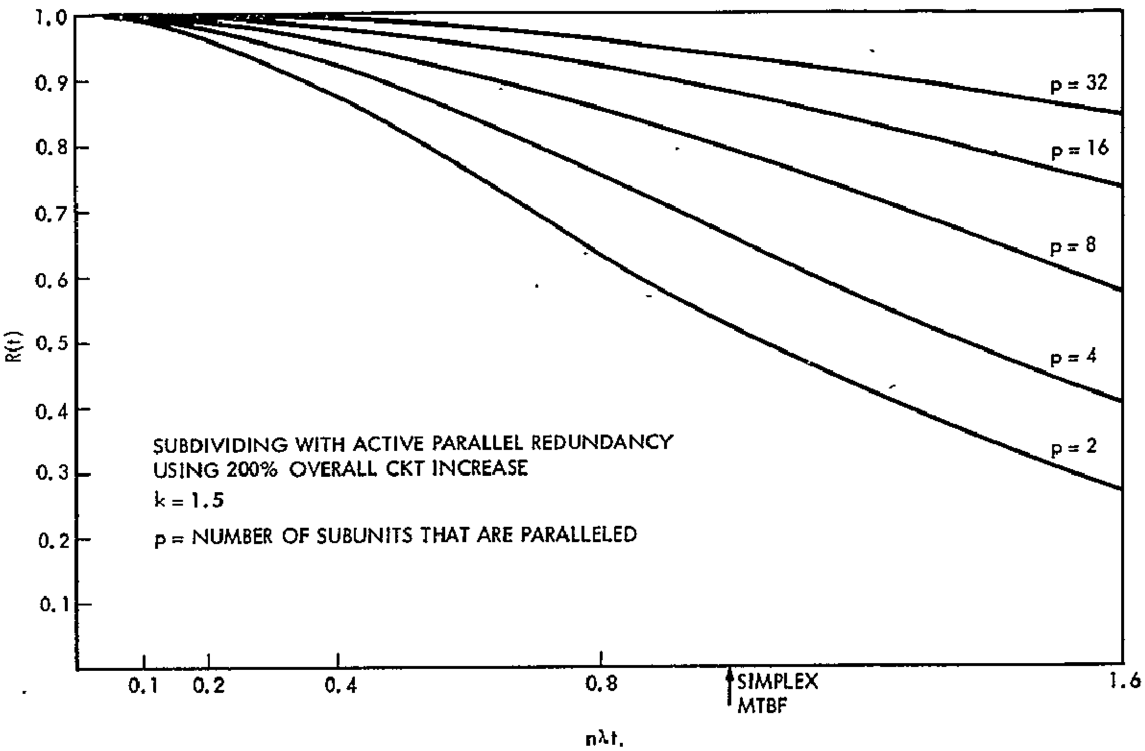
Curve 6



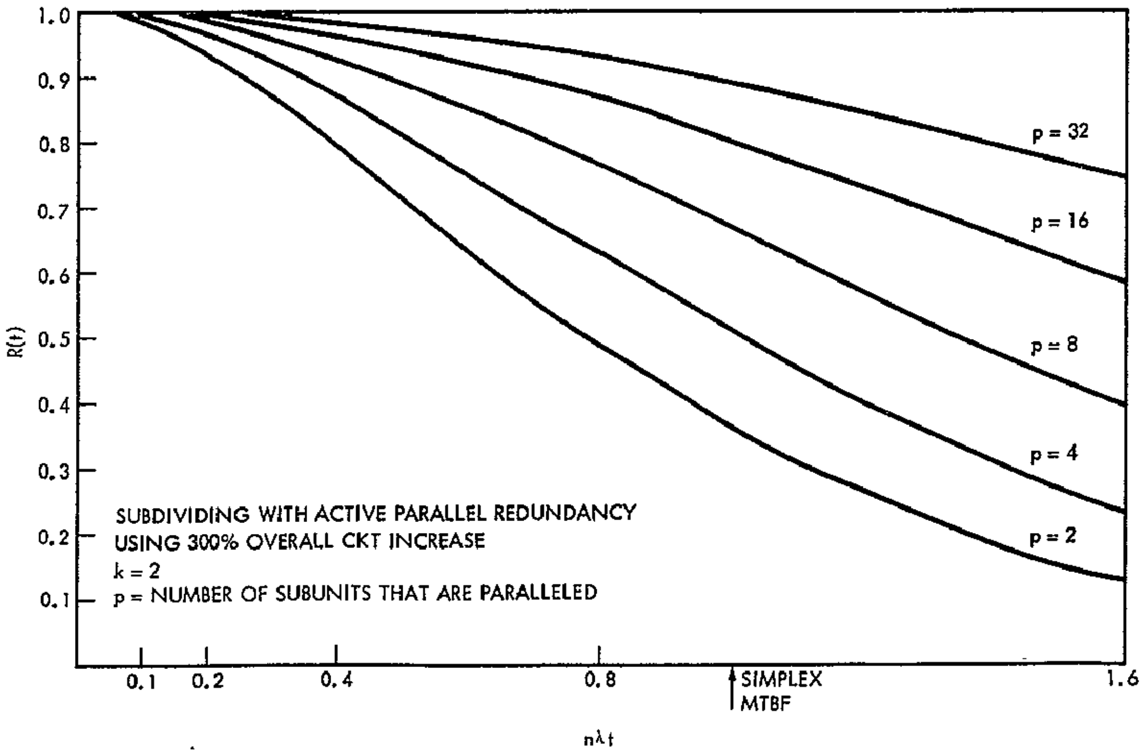
Curve 7



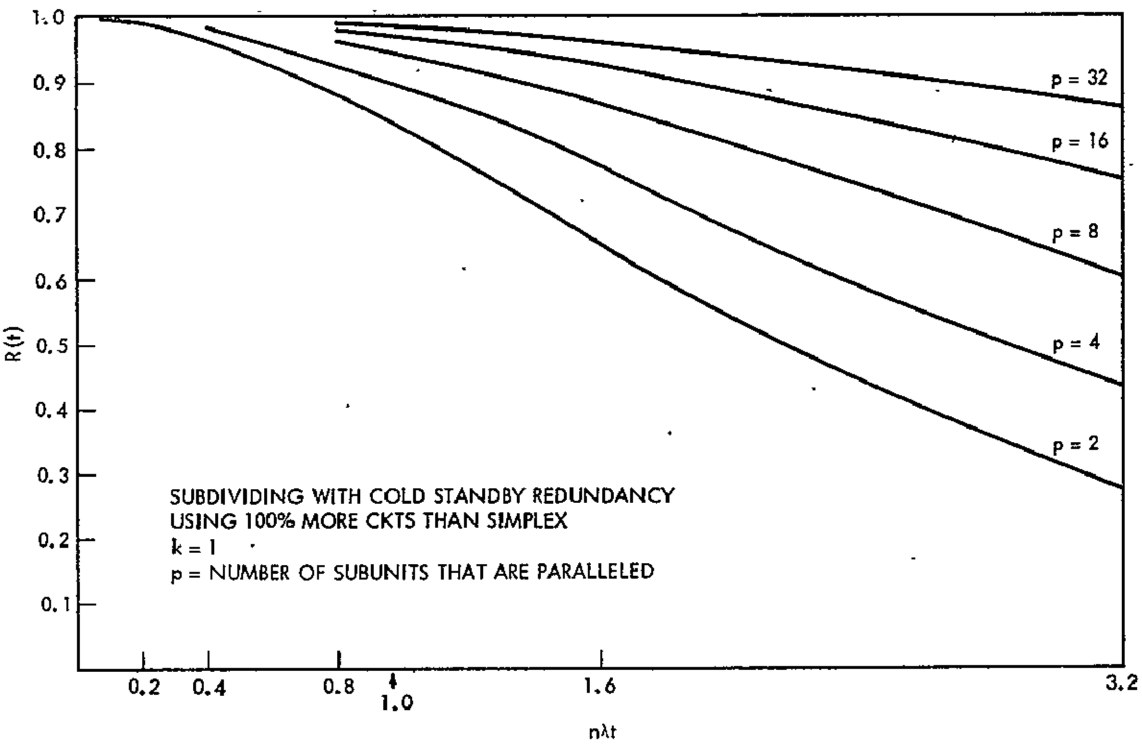
Curve 8



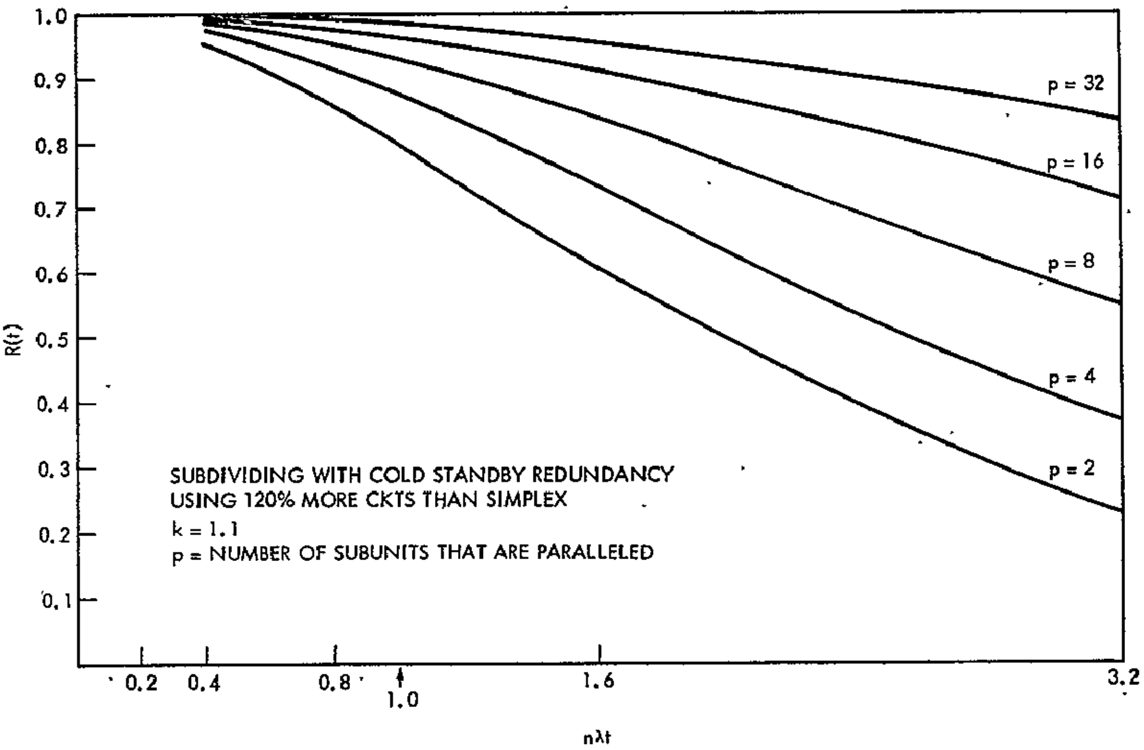
Curve 9



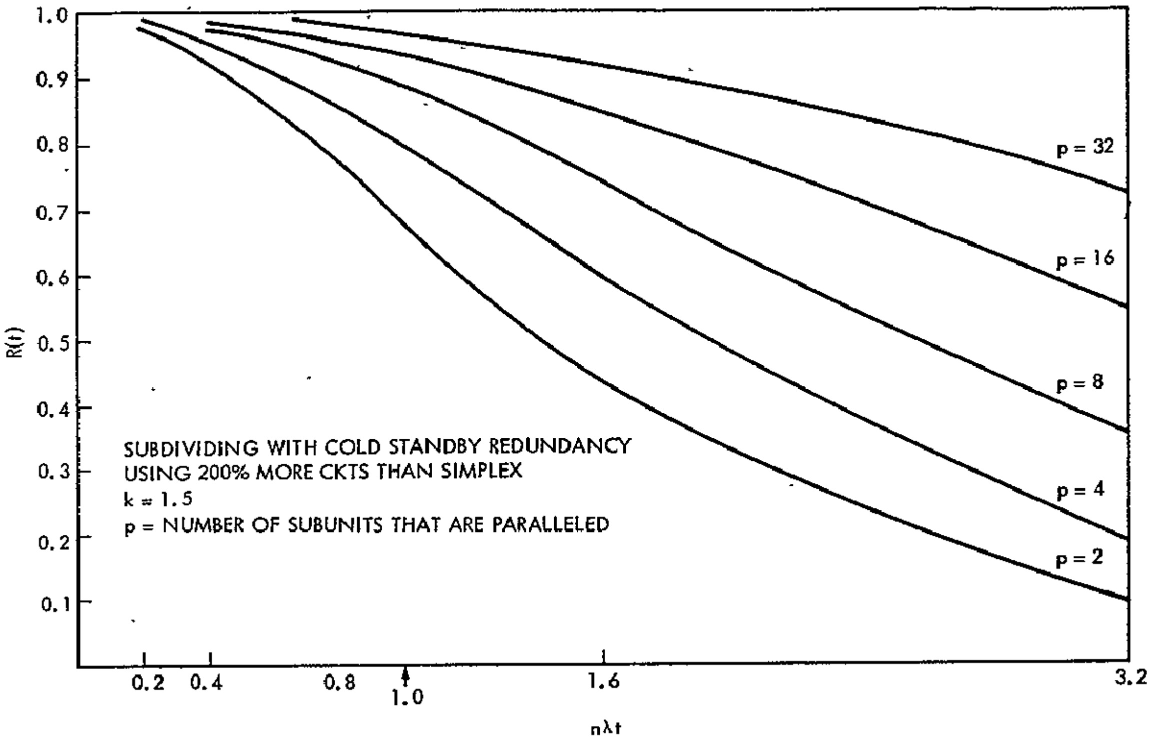
Curve 10



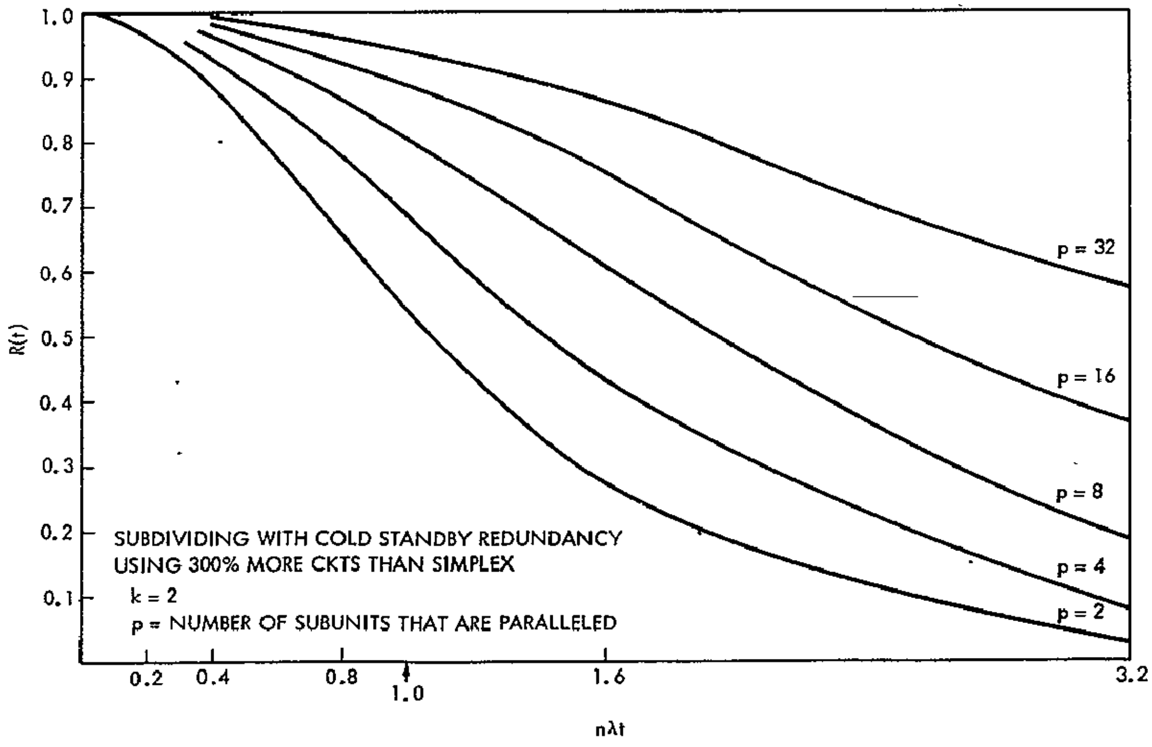
Curve 11



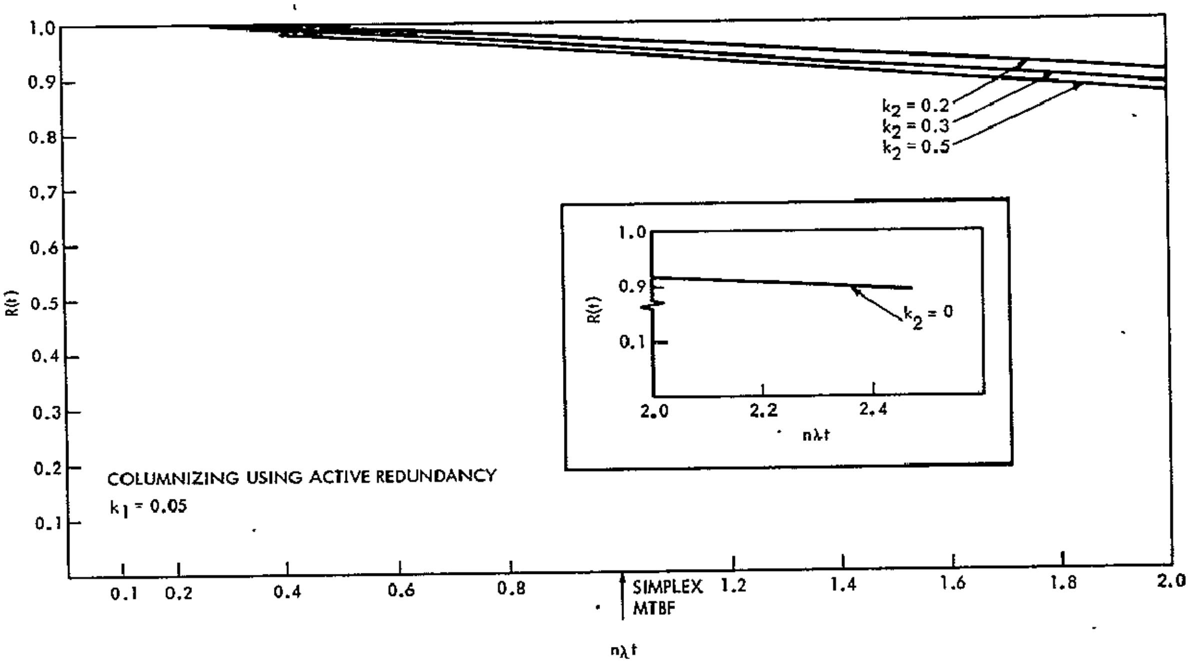
Curve 12



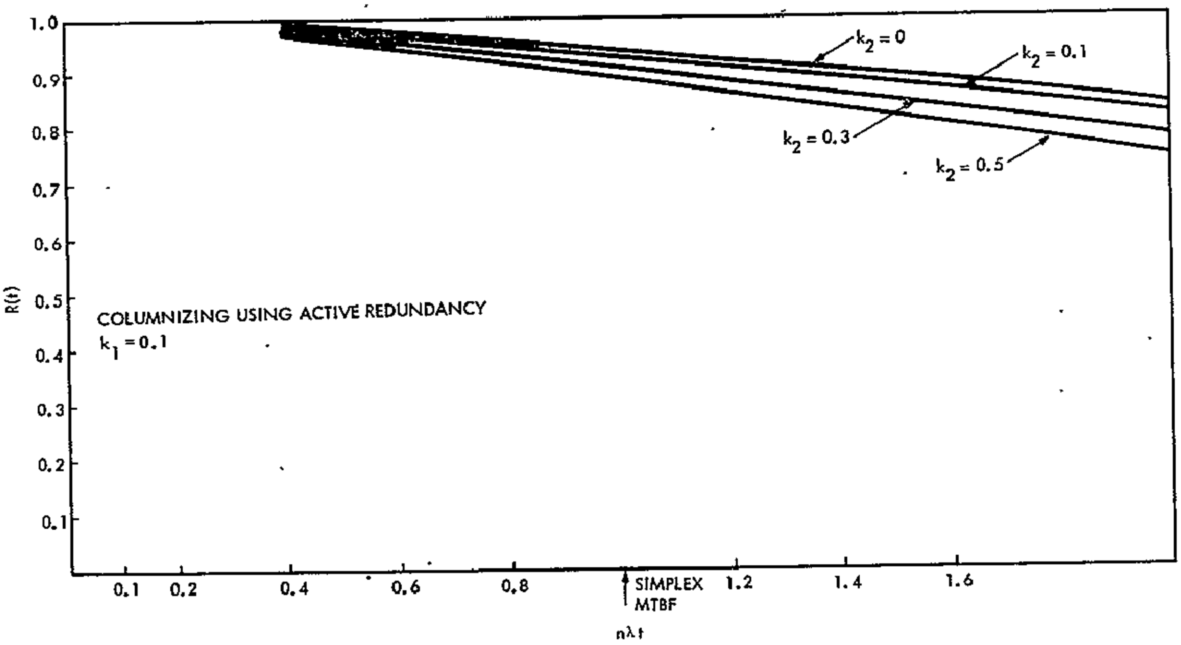
Curve 13



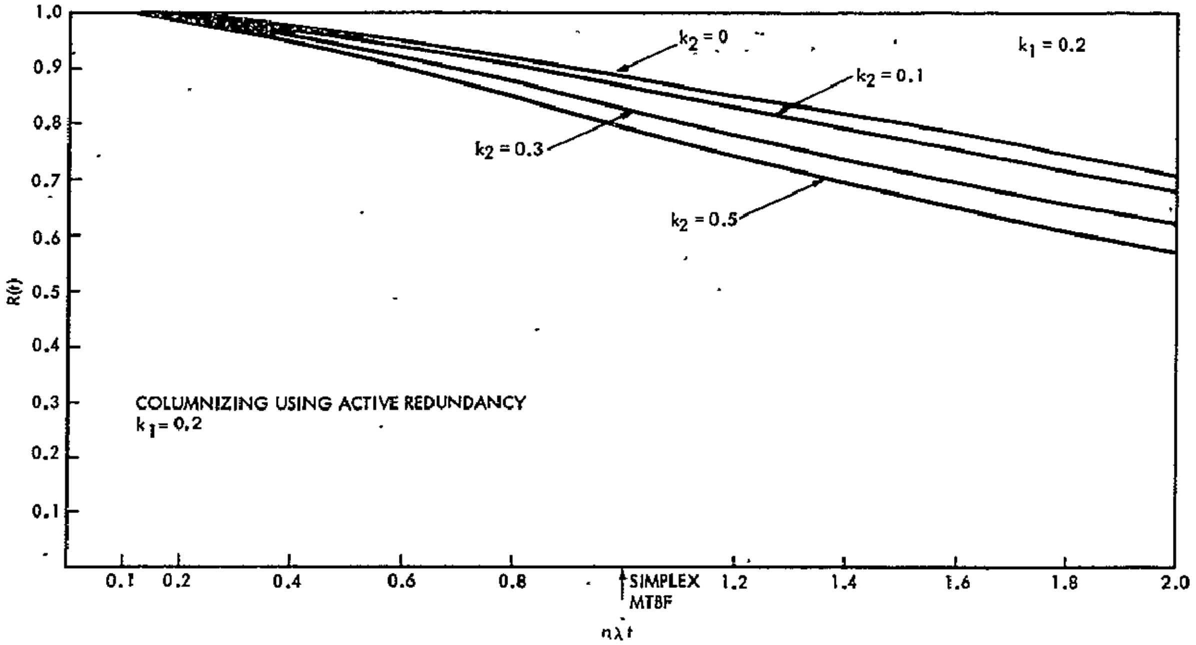
Curve 14



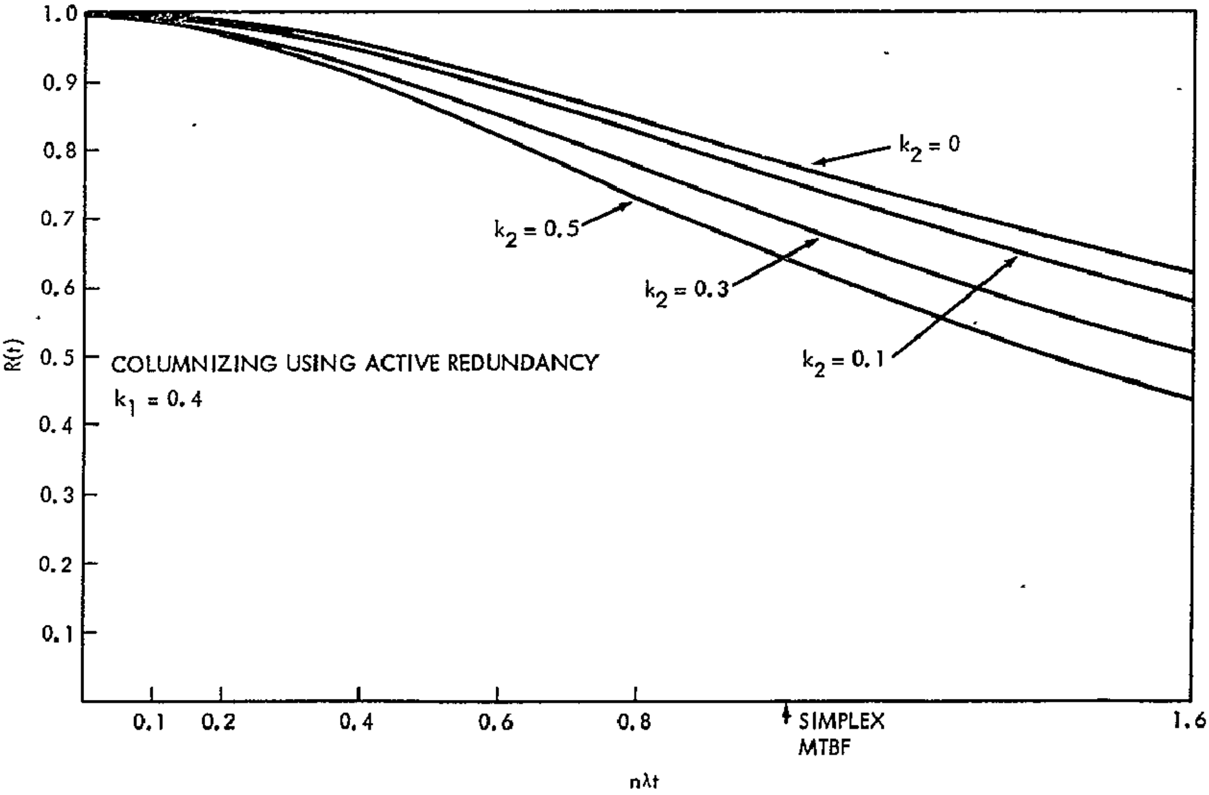
Curve 15



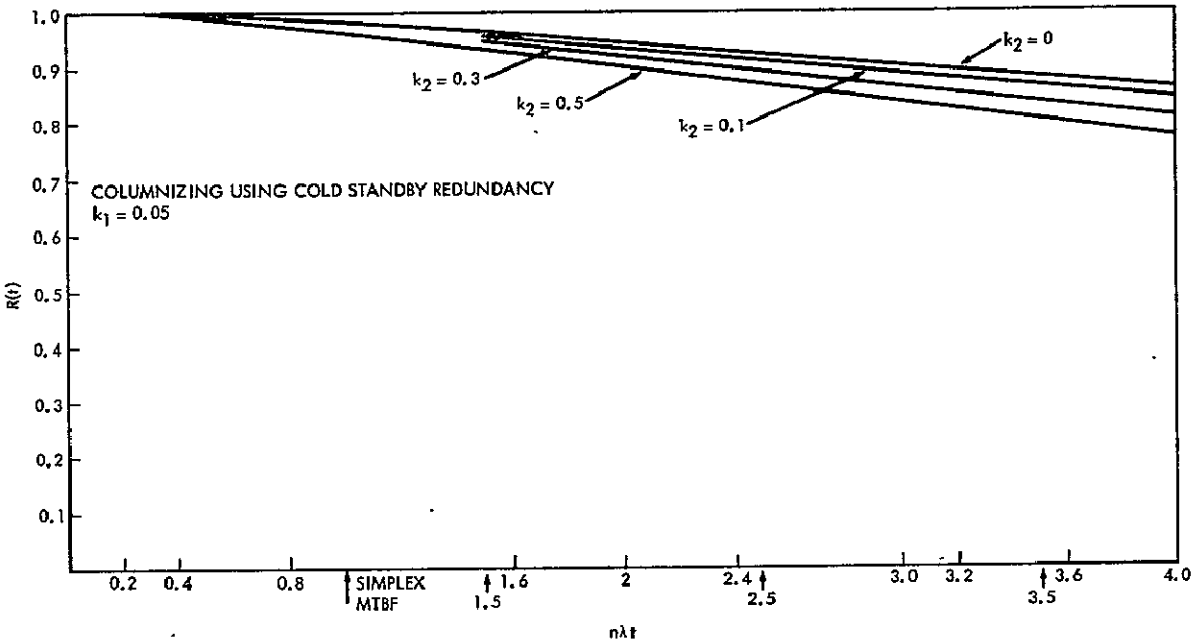
Curve 16



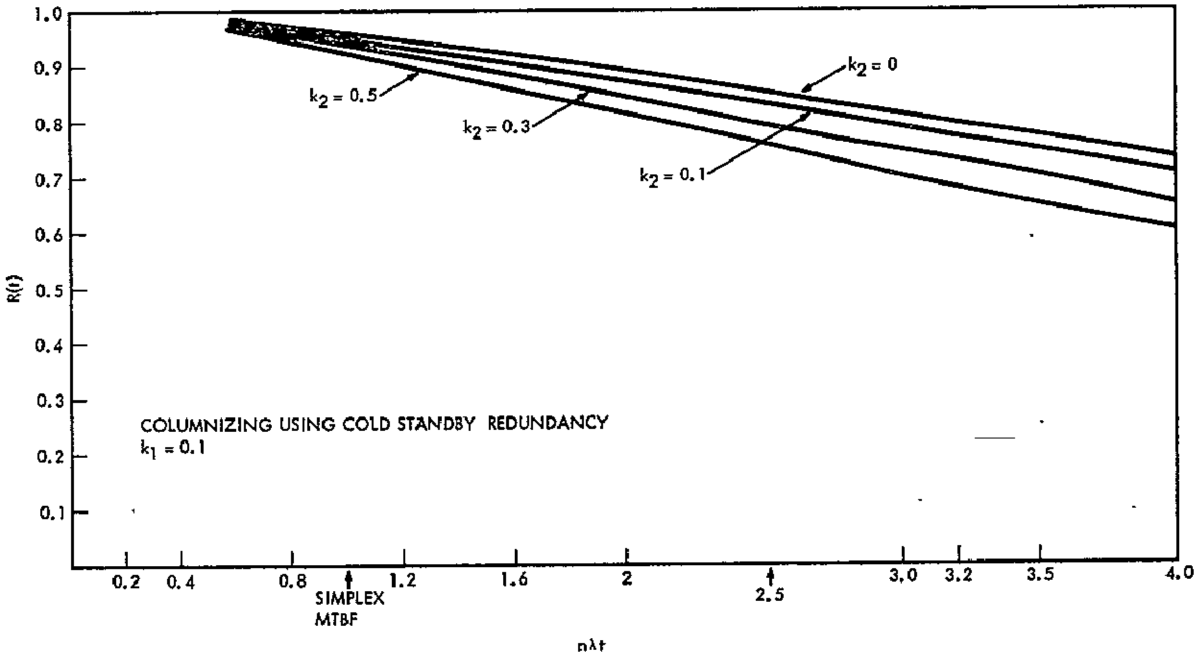
Curve 17



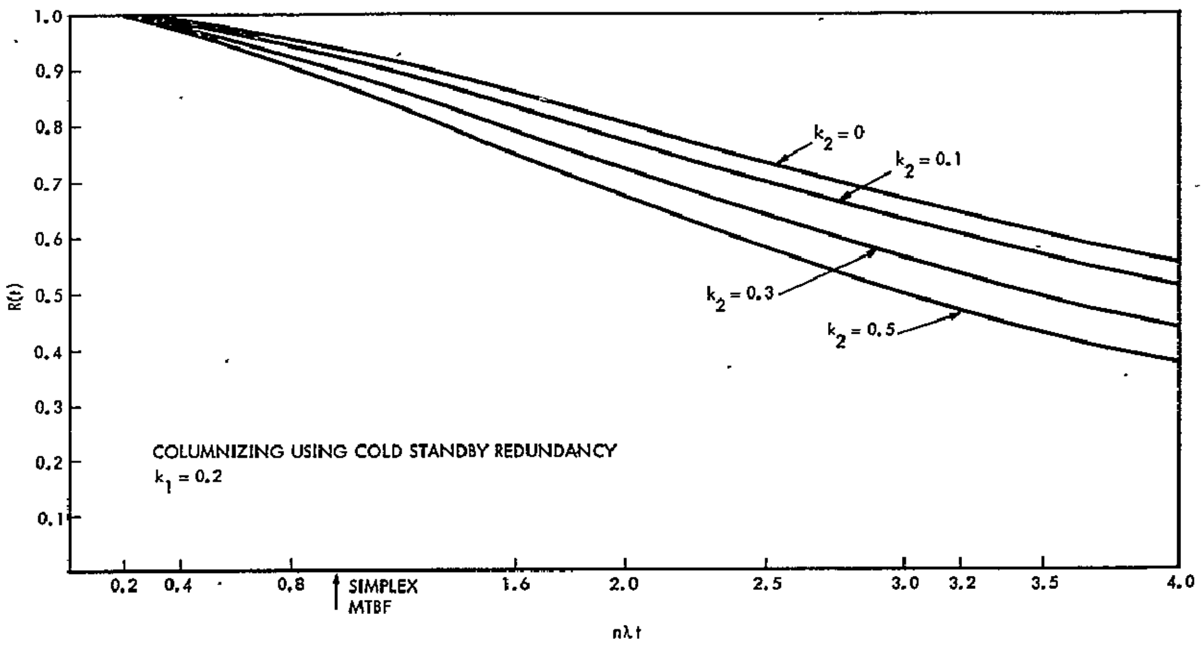
Curve 18



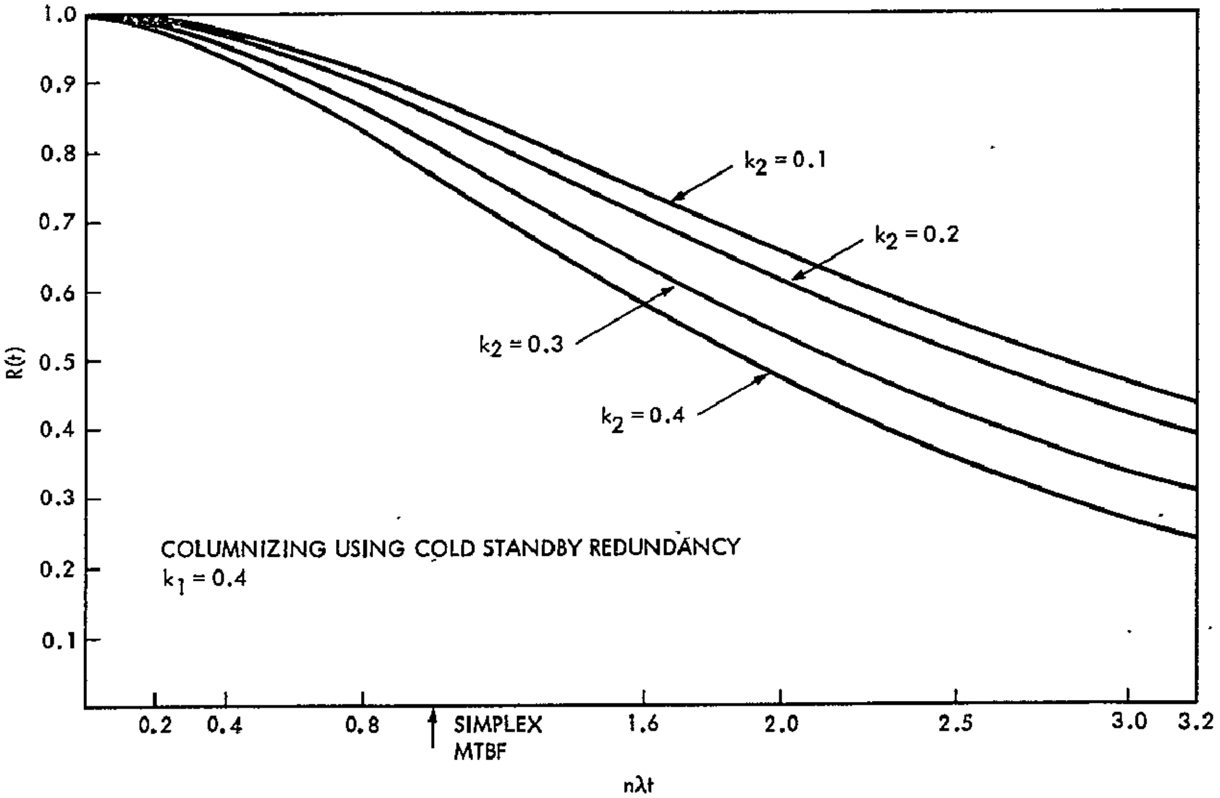
Curve 19



Curve 20



Curve 21



Curve 22