THE BELL SYSTEM TECHNICAL JOURNAL
Vol. 57, No. 9, September 1978
Printed in U.S.A.

Reliability of a Microprocessor-Based Protection Switching System

By G. S. FANG

(Manuscript received July 7, 1977)

High-capacity transmission systems usually include one or more hot spares for protection. When a regular transmission channel fails, its signal is rapidly transferred to the spare channel under the control of protection switching circuits so that there is little signal degradation or interruption. This paper studies the reliability of a microprocessor-based terminal protection switching system. Some new and interesting behavior patterns for transmission systems with automatic protection switching are revealed. Also, some new memory self-checking algorithms are presented which increase the capability of microprocessor system fault recognition.

I. INTRODUCTION

In high-capacity transmission systems, any failure may affect a large number of message circuits. Such systems usually include one or more hot spares to increase system reliability. When a regular transmission channel fails, its signal is rapidly transferred to the spare channel under the control of protection switching circuits so that there is little signal degradation or interruption. This paper studies the reliability of a microprocessor-based terminal protection switching system (TPSS). The specific transmission facility under consideration is the L5E coaxial cable analog system, which is an expanded version of the L5 system.[1] The L5E multiplex equipment, or multimastergroup translators (MMGT), carry up to eight mastergroups, or 4800 telephone circuits. The TPSS will automatically switch into service a protection MMGT in the event of a failure of any one of up to 20 MMGTs.

Reliability theory has been studied by numerous authors,[2,3] and almost every Bell System transmission facility with automatic protection switching has been the subject of at least one reliability study.[4,5] The present analysis was undertaken for several reasons. First, many simplifying assumptions were made in the previous studies. Not all the effects of the reliability of the switch, the protection switching control circuit, and the monitor circuit failures were taken into account. Second, in most cases, exponentially distributed restoration time has been assumed. This means that the probability of restoration at any instant after a failure is assumed to be independent of how much time has already been spent on restoring the failure. This assumption is rarely true in high-capacity transmission systems. Third, only steady-state analyses were made. A system with hidden failures will not reach its steady state in its lifetime. Fourth, a microprocessor-based protection switching control circuit has not been studied in such detail before. Finally, past experiences have shown that maintenance-induced service outages contribute to a very big share of the total outage time. This study also tries to take these outages into consideration.

With the MMGT system as an example, the present study attempts to analyze the same reliability problem in more detail and with less restrictive assumptions. Section II describes the protection switching arrangement. Section III explains the specific approaches used in this paper. Section IV presents the results graphically to emphasize the various reliability trends. Section V summarizes the conclusions obtained. Appendix A investigates some new microprocessor self-checking algorithms and Appendix B presents the derivations.

II. MMGT PROTECTION SWITCHING SYSTEM DESCRIPTION

Figure 1 is a simplified MMGT-system block diagram which illustrates the 1 × n protection switching arrangement. There is one protection channel in each direction of transmission. Under the command of the microprocessor, each protection channel protects up to n regular channels, where n is equal to 20 in the TPSS. The same processor is used to control the switching actions of both directions of transmission. The switches are all solid-state devices, and their normal states are indicated in the figure. The crucial output switches are dual-powered. Parts of the output switch are designated the through switch and the substitute switch for later reference.

When there is no alarm from the various regular pilot detectors, the processor exercises the input switches for each channel sequentially to detect possible protection failures. In the event of a failure of one of the regular channels, the corresponding pilot detector sends an alarm to the processor. If the protection channel is available, the processor will first switch the input signal through the input switches to feed the protection channel. Whether the protection detector indicates a good signal or not, the processor will complete the 1 × 2 output switch. The regular detector is now monitoring the signal supplied by the protection channel via the output substitute switch. If the regular detector still alarms after the protection switch, the switching action will be reversed. The 1 × 2 output

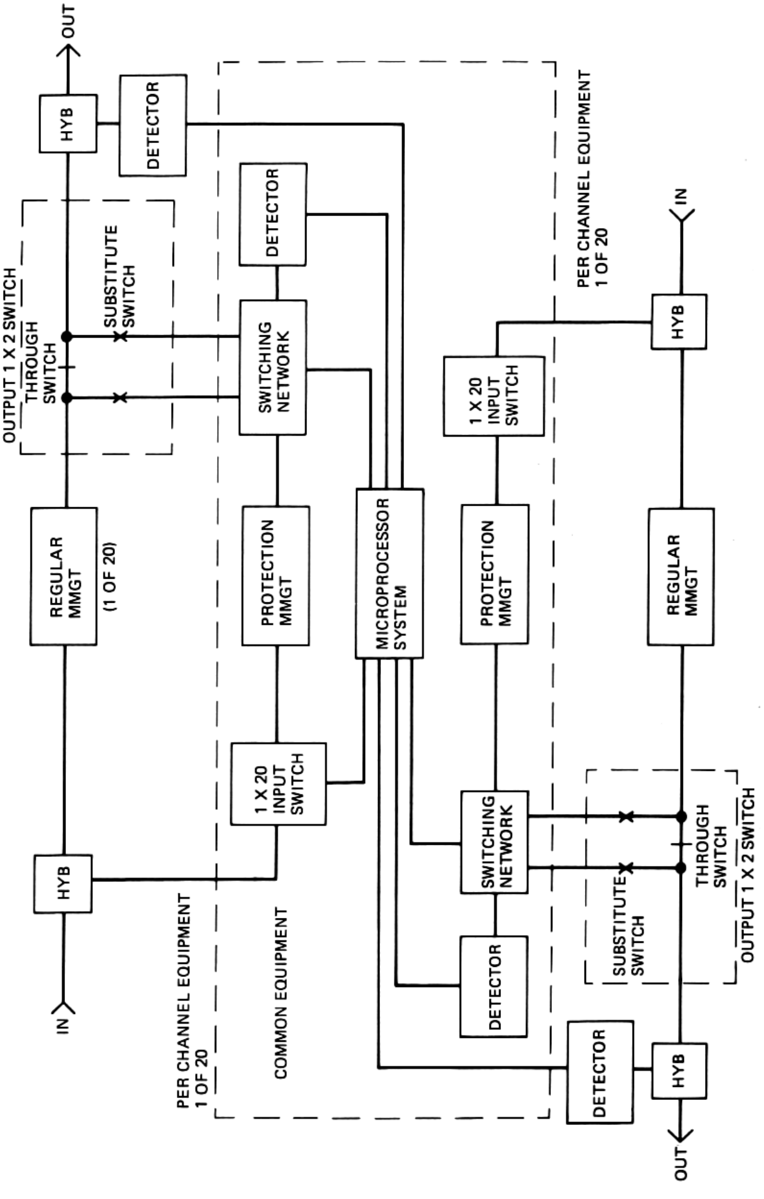

Fig. 1—TPSS block diagram.

switch will be deactivated and the input switch released. If the regular detector stops alarming after the output switching, a successful protection switch has been made, and the protection detector is monitoring the failed regular channel. When the failed channel is repaired, the protection detector will see a good signal, and the switches will return to their normal states. The protection channel is then free to service another regular channel failure.

Service outages can occur in many ways. In addition to multiple transmission failures, they can also be generated by the failures of the detectors, the switches, or the microprocessor system. The various failure modes are taken into account in later derivations.

III. APPROACHES

Two reliability measures of interest in transmission systems are used in this study. The first measure is the probability of service outage due to equipment failures. This probability translates directly to the system outage time per year and is the most commonly used figure of merit in determining transmission system reliability. The second measure is the probability of having maintenance activities going on. This measure will be abbreviated as the probability of activity. It is believed to be closely related to the probability of having maintenance-induced outages. This probability of activity is greater than the probability of having alarms because there are failures that cannot be detected locally. For instance, if the pilot detector for a failed regular channel is stuck to the state of no alarm, the failure can only be detected by downstream offices. Thus there may be maintenance activities in an office but no alarm. The probability of activity is less than the probability of having failures because there are undetectable failures such as the breakdown of an output substitute switch. A reliable system should have a small probability of outage and a small probability of activity.

Two additional criteria are used to measure the effectiveness of the overall protection plan. The improvement factor (IF) is defined as the ratio of the probability of outage without protection switching to that with protection switching. The activity factor (AF) is defined as the ratio of the probability of activity with protection switching to that without protection switching. These definitions agree with the common notion that an effective protection plan should provide more improvement and less activity. Thus, a better protection system has a bigger IF and a smaller AF. The activity factor is always greater than one.

The probabilities discussed above are derived under the assumptions that the various failures are statistically independent and the failure rates are constant. These are very simple assumptions considering the complexity of the problem. The assumption of statistical independence is made to avoid estimating conditional failures, although there is probably dependency between the through switch and the substitute switch. The constant failure rate implies exponentially distributed failures, i.e., any working item is as good as new. This is a reasonable assumption for solid-state devices after the initial "burn-in" period. Notice that no distributional assumption is made on the restoration time. Based only on the failure rates and the restoration times of the components of the system, the various probabilities are derived from the basic definitions of conditional probability. Not only does this approach require little mathematical background, but the result is more general and more accurate than the usual method of Markoff chain or birth-and-death stochastic processes,[2,3] which assume that both failure and restoration times are exponentially distributed.

IV. DETAILED RESULTS

Table I introduces the notations and gives the estimated failure rates in FITS (number of failures per component per 10^9 hours), restoration times in hours, and the availabilities of the various components. The restoration time is the sum of the detection time and the equipment replacement time. The mean value of the replacement time t is assumed to be 1 hour. Some failure rates are expressed in terms of other failure rates to show their relative dependence. This is necessary in later parameter sensitivity studies. The failure of a substitute switch can only be detected when its use is called for. Thus, its detection time is the mean time between transmission failures of its corresponding channel, i.e., $1/(\lambda_r + \lambda_t + \lambda_0)$. The same is true for the detection time of a regular detector, except that the assumed probability that a failed detector gives a no-alarm indication is 1/4. In both cases, the equipment replacement time is ignored since it is small compared with the detection time.

The detection times of the hidden CPU (central processing unit) and EROM (erasable read-only memory) failures should also be similarly calculated. However, the failure of the regular channels to be exercised sequentially should provide local craftspeople with the indication that something is wrong. Therefore, the detection times are assumed to be 24 hours. The availability[3] of an item is the probability that the item is working. It is a function of time with an initial value of one and with a steady-state value equal to the mean time to failure divided by the sum of the mean time to failure and the mean restoration time. If a component has a short failure detection time, the transient portion in its availability value vanishes quickly, and the steady-state theoretical availability approximates the actual availability very well. For example, the steady-state availability of the regular channel is $p_r = 1/1.000001$. The reliability function of the regular channel is $e^{-10^{-6}t}$. It takes only 1 hour for the reliability function to reach its steady-state availability value.

Table I — Estimated failure rates

	FITS	Mean Restoration Time (hr)	Availability
Regular channel	$\lambda_r = 1000$	$\mu_r = t$	$p_r = \frac{1}{1 + \lambda_r \mu_r}$
Through switch	$\lambda_t = 150$	$\mu_t = t$	$p_t = \frac{1}{1 + \lambda_t \mu_t}$
Output switch	$\lambda_0 = \frac{1}{3} \lambda_t$	$\mu_0 = t$	$p_0 = \frac{1}{1 + \lambda_0 \mu_0}$
Substitute switch	$\lambda_s = \frac{2}{3} \lambda_t$	$\mu_s = \frac{1}{\lambda_r + \lambda_t + \lambda_0}$	$p_s = \frac{1}{1 + \lambda_s \mu_s} + \frac{\lambda_s}{(\lambda_s + \mu_s^{-1})^2 T} [1 - e^{-(\lambda_s + \mu_s^{-1}) T}]$
Regular detector	$\lambda_d = 300$	$\mu_d = \frac{1}{4} \frac{1}{\lambda_r + \lambda_t + \lambda_0}$	$p_d = \frac{1}{1 + \lambda_d \mu_d} + \frac{\lambda_d}{(\lambda_d + \mu_d^{-1})^2 T} [1 - e^{-(\lambda_d + \mu_d^{-1}) T}]$
Protection detector	$\lambda_D = 300$	$\mu_D = t$	$p_D = \frac{1}{1 + \lambda_D \mu_D}$
Protection channel	$\lambda_p = \lambda_r + 4\lambda_s + 100$	$\mu_p = t$	$p_p = \frac{1}{1 + \lambda_p \mu_p}$
CPU	$\lambda_c = 500$	$\mu_c = 24 + t$	$p_c = \frac{1}{1 + \lambda_c \mu_c}$
EROM	$\lambda_e = 300$	$\mu_e = \mu_c$	$p_e = \left(\frac{1}{1 + \lambda_e \mu_e}\right)^4$
RAM	$\lambda_a = 400$	$\mu_a = t$	$p_a = \left(\frac{1}{1 + \lambda_a \mu_a}\right)^2$

These arguments do not hold for failures requiring long detection times. For instance, the mean time to failure and the mean restoration time of a substitute switch are in the order of hundreds of years, while the life span of the equipment is expected to be only 40 years. To obtain an appropriate availability in such cases, one would observe that the restoration time of the substitute switch is exponentially distributed. This is due to the fact that the replacement time is ignored and the detection time depends on the transmission failures which are exponentially distributed. Thus the availability function can be derived explicitly as

$$A_s(t) = \frac{1}{1 + \lambda_s \mu_s} + \frac{\lambda_s}{\lambda_s + \mu_s^{-1}} e^{-(\lambda_s + \mu_s^{-1})t}.$$

The availability p_s given in Table I is the $A_s(t)$ averaged over the life span T of the equipment. The availability of the detector p_d is obtained similarly. The availability expressions of the EROM and the RAM reflect the use of 4 EROMs and 2 RAMs in the TPSS.

To gain insight and to study the sensitivity of the derived probabilities to the estimated failure rates and restoration times, the various estimated parameters are varied one at a time to show the system reliability trends. The results are presented graphically in the figures. In each figure, the solid line corresponds to the ordinate at the left and the dotted line to that at the right.

Figures 2 through 7 present the variations of the outage and the activity probabilities as functions of the regular channel, the detector, the switch, the CPU, the EROM, and the RAM failure rates, respectively. Most of the curves are almost linear because, for the small failure rates of interests, they are still in their linear regions. As far as the probability of outage is concerned, undetectable failures are the most damaging. The hidden detector and the substitute switch failures contribute to the bigger slopes in Figs. 3 and 4. Increasing the microprocessor system failures adds very little to the outage probability, as can be seen from Figs. 5 to 7. The probability that has the fastest increase is the switch failure rates because there are so many switches in the system. Figure 8 indicates that service outage can increase substantially if the replacement time for failed equipment is long. Figure 9 shows the effect of varying the detection time of the hidden microprocessor failure. Neither the outage nor the activity probability is sensitive to the detection time. Figure 10 shows the effect of varying the number of regular channels equipped. The discrete points in the figure are connected to show the almost linear trends. When the system is fully loaded, i.e., $n = 20$, there are about 2 minutes of service outage each year due to equipment failures and there is about half an hour of maintenance activities. It should be emphasized that the curves present the right trends

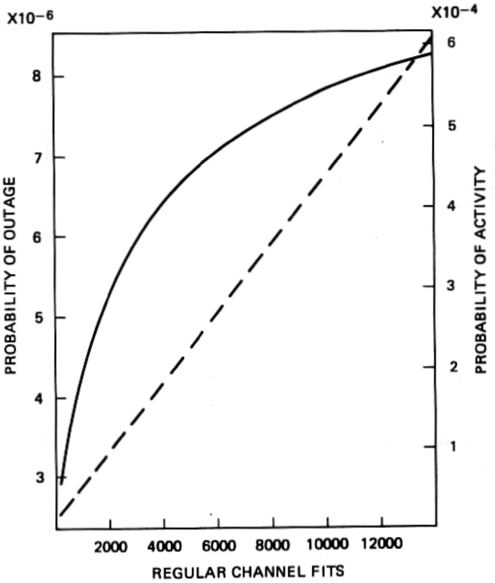

Fig. 2—Probabilities of outage and activity as functions of regular channel failure rate.

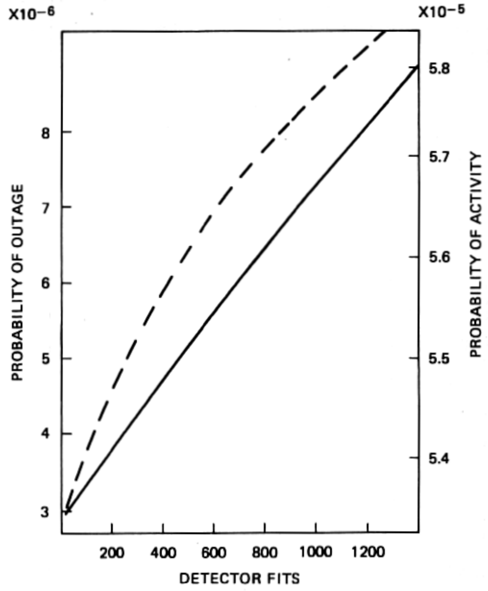

Fig. 3—Probabilities of outage and activity as functions of detector failure rate.

rather than numerical accuracy. From Fig. 2, if the failure rate of the regular channel is increased by ten times, there will be 4 minutes of outage and 4 hours of activity each year. Figure 10 shows the two

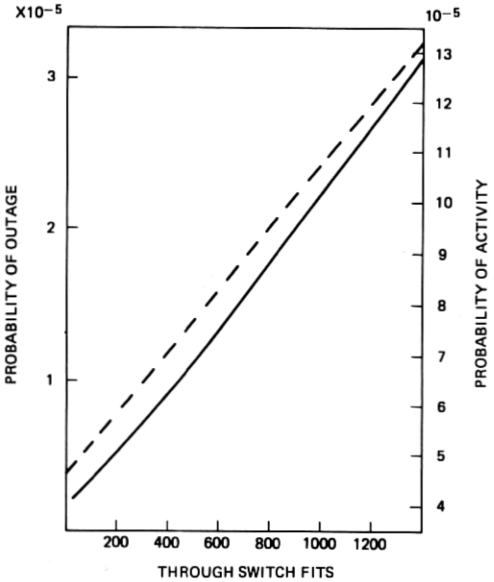

Fig. 4—Probabilities of outage and activity as functions of through switch failure rate.

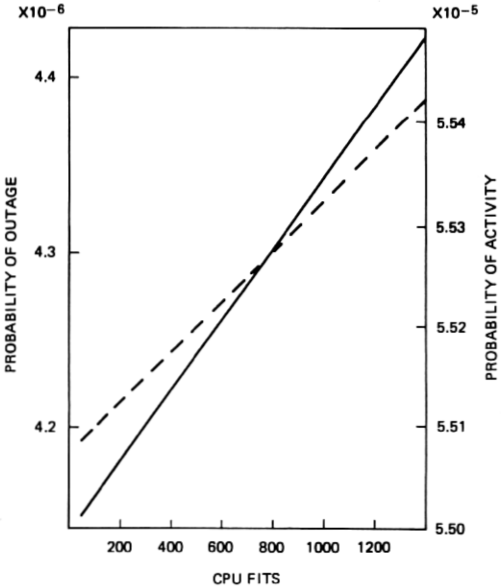

Fig. 5—Probabilities of outage and activity as functions of CPU failure rate.

probabilities as functions of the number of regular channels. The discrete points are connected to indicate trends. For terminal circuits which usually have small failure rates, there is scarcely any need for a second

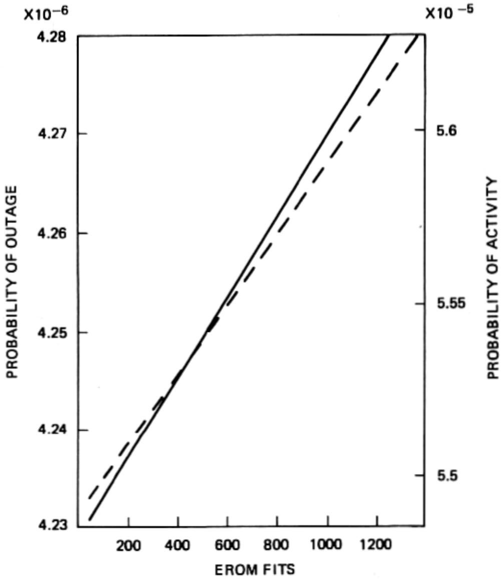

Fig. 6—Probabilities of outage and activity as functions of EROM failure rate.

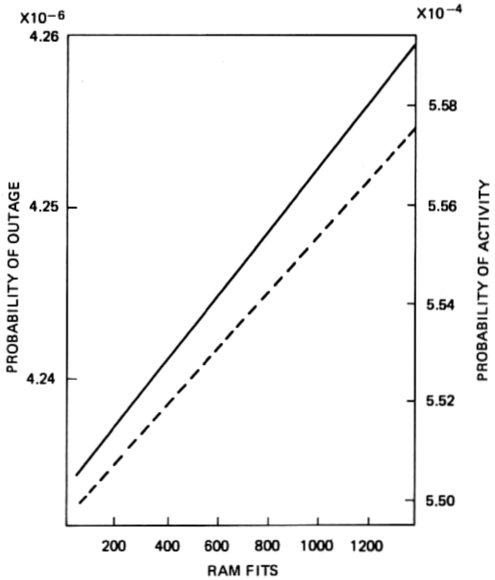

Fig. 7—Probabilities of outage and activity as functions of RAM failure rate.

protection channel even when the number of regular channels is large.

A system without protection switching has only the regular channels and their corresponding detectors to indicate alarms. The switches and

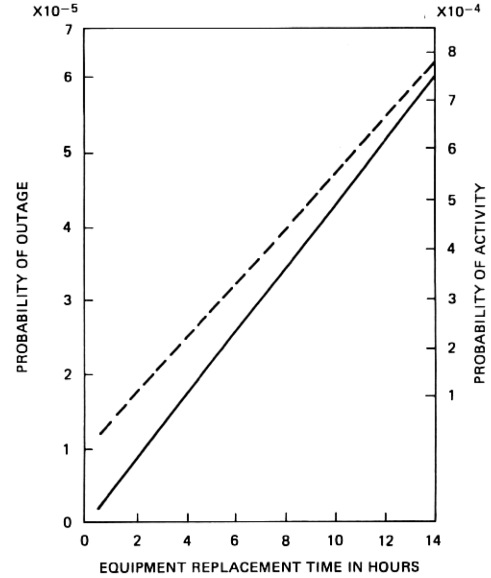

Fig. 8—Probabilities of outage and activity as functions of equipment replacement time.

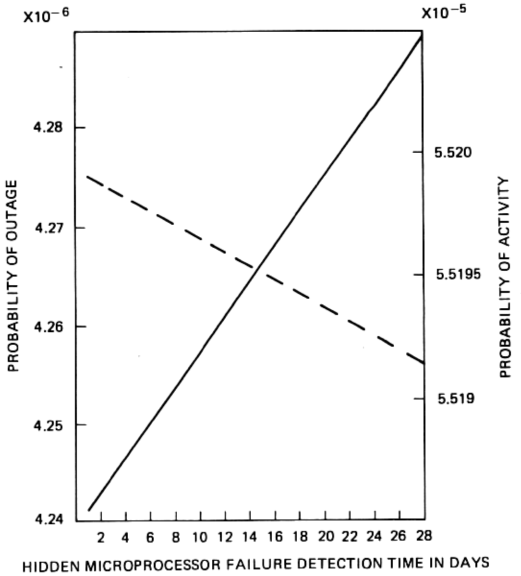

Fig. 9—Probabilities of outage and activity as functions of hidden microprocessor failure detection time.

the microprocessor devices are not required. Thus there is definitely less activity in the maintenance offices. Figure 11 shows the trend that, for small regular channel failure rates, the IF can be less than unity, i.e.,

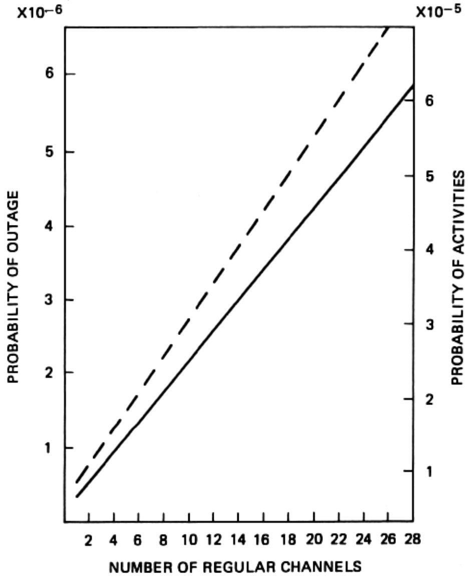

Fig. 10—Probabilities of outage and activity as functions of number of regular channels.

having protection switching actually causes more service outage. This is true when the failure rate of the regular channel is small compared with those of the protection switching circuits. Furthermore, protection switching generates many more activities at low regular channel failure rates. Figure 12 amplifies this fact by examining the 1 × 1 configuration. The IF is so small and the AF is so big that implementation of a 1 × 1 protection plan is questionable at low failure rates. Figure 13 gives the variations of the two factors with detector failure rates. Since detector failures have little effect on the outage probability of an unprotected system, the IF decreases with increasing detector failure. The interesting shape of the AF curve is due to the relatively rapid increase in the probability of activity for an unprotected system when the detector failure rates are small. This behavior is unique to the variation of the detector failure rate because an unprotected system is equipped only with the transmission channels and the detectors.

Figure 14 again indicates the important role played by the output switch. If its failure rate is high enough, the IF can reduce to less than unity. With a perfect switch, the outage of a protected system can be hundreds of times less than that of an unprotected system. The curves showing the two factors as functions of the CPU, the EROM, and the RAM failure rates are not given here. These curves can be simply deduced from Figs. 5 to 7 because the various probabilities of an unprotected system are independent of microprocessor failures. Similarly, the factors involving hidden microprocessor failure restoration time can be obtained from Fig. 9. Figure 15 shows that both the IF and the AF are not very sensitive to how long it takes to replace failed equipment. Figure 16 varies the number of regular channels. It indicates that more than 10 regular

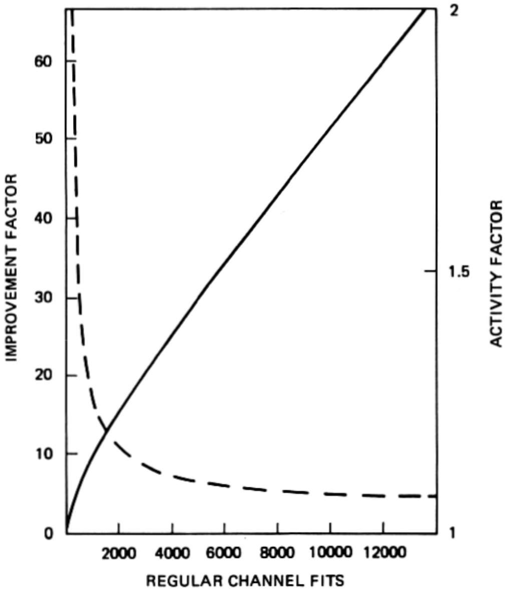

Fig. 11—Improvement and activity factors as functions of regular channel failure rates.

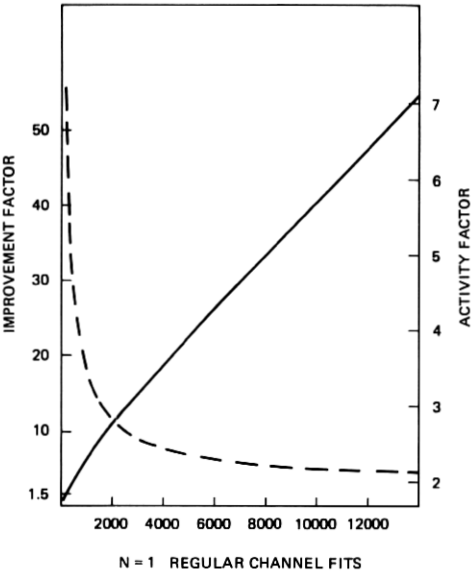

Fig. 12—Improvement and activity factors as functions of regular channel failure rates.

channels should be used to take advantage of the protection switching arrangement.

Figure 17 exhibits an interesting behavior of general protection

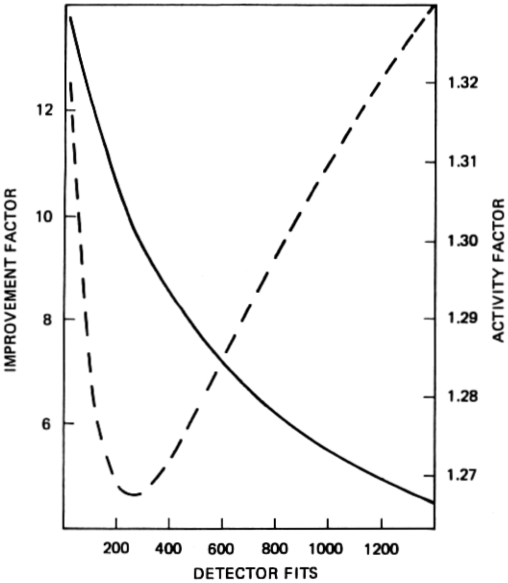

Fig. 13—Improvement and activity factors as functions of detector failure rates.

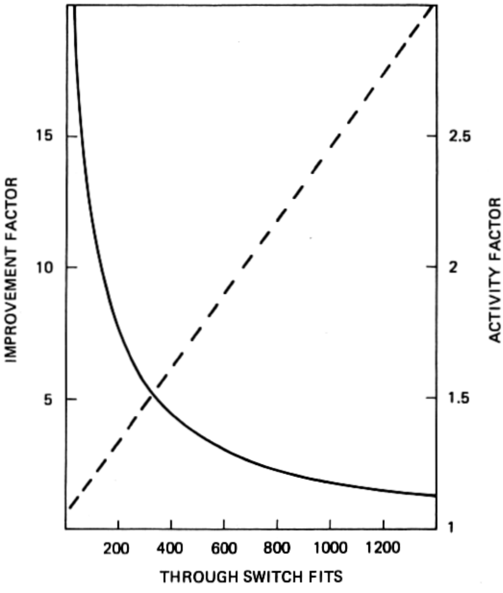

Fig. 14—Improvement and activity factors as functions of through switch failure rates.

switching systems. As the failure rate of the regular channel increases, the IF increases from less than one to a maximum and then starts to decrease. When the failure rate becomes very large, the outage probability is close to 1 with or without protection switching. Thus the IF approaches 1 eventually. The maximum IF shown in the figure occurs at around 150,000 FITS. Although it is unlikely for a terminal multiplexer to possess so high a failure rate, a line transmission system with many cascading repeaters may very well have a failure rate of this order. Therefore, whenever a line protection switching system is planned, the reliability should be studied to determine the length of the protection span so that the IF does not fall in its decreasing region. Of course, the outage probability should also be taken into account to meet any prescribed service objectives.

V. CONCLUSIONS

The reliability of the microprocessor-based TPSS has been studied in detail using conditional probability. Consideration of the four criteria; i.e., the probability of outage, the probability of activity, the improvement factor, and the activity factor, should provide an adequate description of the effectiveness of the overall protection plan. Several conclusions can be drawn from the analysis. First, terminal circuits usually have low failure rates so that one protection channel is adequate for the protection of many regular channels without having excessive

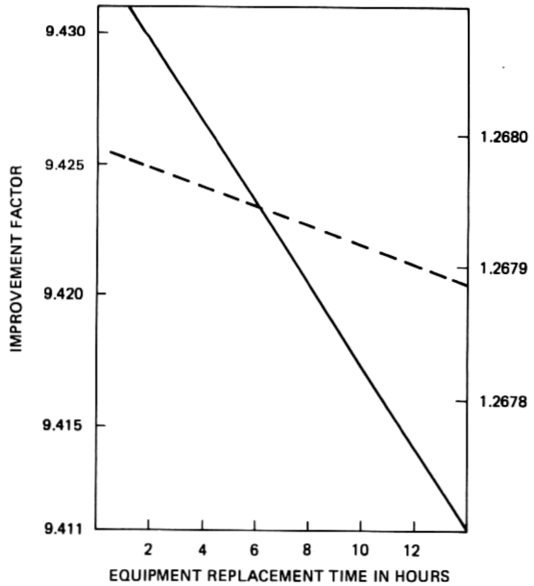

Fig. 15—Improvement and activity factors as functions of equipment replacement time.

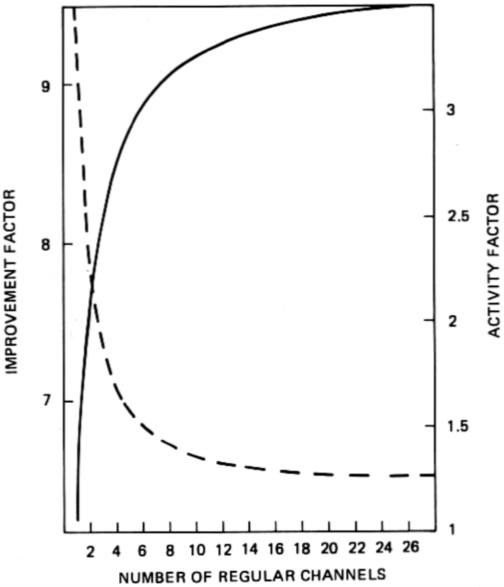

Fig. 16—Improvement and activity factors as functions of number of regular channels.

probability of service outage. Second, undetectable failures are usually the prime causes for increased outage probability and decreased improvement factor. If preventive maintenance is ever to be carried out, the hidden failures should be the principal targets. Third, the microcomputer is reliable as a protection switching controller. Although microprocessor system failures can cause false switching all by themselves, they contribute only a very small amount of the total outage if adequate self-checking is implemented. Reliability could be further improved by providing hardware interlock logic to guard against an insane microprocessor. For example, logic circuit can be provided in the TPSS to prevent the operation of an output switch whenever its input switch is inactive. Fourth, all the figures indicate that, around the various estimated failure rates of interest, the outage probabilities increase almost linearly with the failure rates. Thus there is no "preferred" range of failure rates that any equipment should be designed to. Only the sensitivities of the outage probabilities to the various estimates are different. Fifth, for any TPSS, the implementation of a 1 × 1 protection plan should be studied carefully. Even if there is improvement in the outage probability due to equipment failure, the increased activity will generate more maintenance-induced outages, not to mention increased costs.

The above comments do not apply in line protection switching systems, which have much higher regular channel failure rates because of the cascaded repeaters. Finally, Fig. 17 suggests one more consideration in determining the length of a line protection switching span. The failure

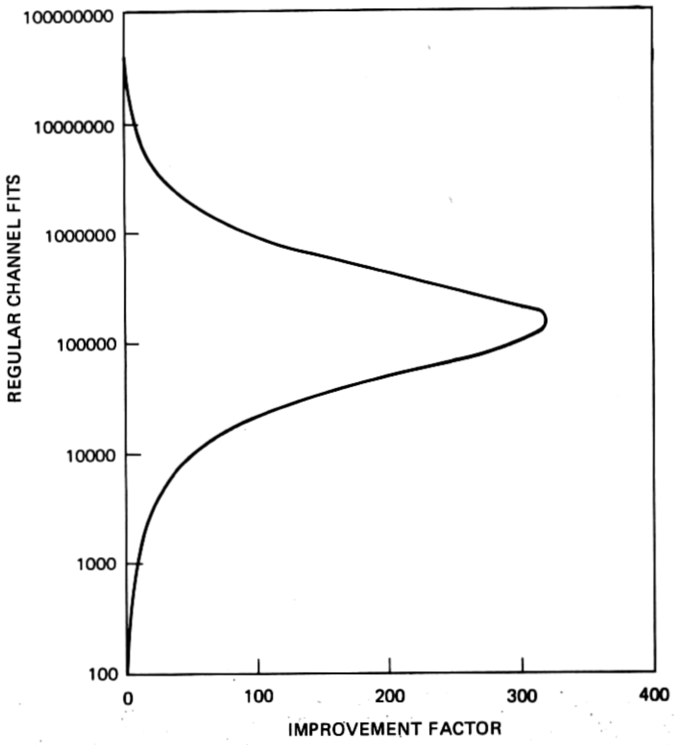

Fig. 17—Regular channel failure rates as functions of improvement factor.

rate of the line should preferably not fall into the decreasing region of its improvement factor. The last two points are obvious and interesting protection switching behavior patterns which seem not to have been explictly pointed out before.

APPENDIX A

This appendix discusses microprocessor self-test algorithms whose purpose is to generate alarms as early as possible to initiate maintenance actions. The test should be exhaustive but should not require too much additional program memory. An 8-bit microprocessor is used in the TPSS application.

When the power is turned on, the microprocessor immediately performs a thorough RAM check. Static RAMs are used, so there is no pattern sensitivity problem. The checking algorithm is to write the least-significant 8-address bits of each RAM byte into that specific RAM location. After all RAM locations are loaded, the contents of each byte are compared with its least-significant 8-bit address. After a byte is checked, its contents are complemented and checked again. The complemented contents will remain in those bytes already checked. This algorithm is able to detect any bit, any data pin, and any combination of address pins stuck to zero or one. It can also discover data and address lines shorted together. Thus most RAM failures can be detected.

The ROMs are checked immediately following the RAM check. Two consecutive bytes in each ROM are reserved for self-test. One byte is used for parity check and the other for short-circuits in address and data lines. The microprocessor reads out every byte in the ROM and performs a cumulative odd parity check through an exclusive-OR operation on each bit. It will be seen first that, as far as independent ROM bit failures are concerned, it is adequate to use only one byte to check the parity of all ROMs no matter how many ROMs are used in the system. Let ℓ be the number of ROM bytes (excluding the reserved checking byte) used in the system and ϵ be the probability of a ROM bit failure. The probability of having parity violations is $1 - (1 - p)^8$, where p is[6]

$$\left[\frac{1-(1-2\epsilon)^{\ell}}{2} \times (1-\epsilon) + \frac{1+(1-2\epsilon)^{\ell}}{2} \times \epsilon\right].$$

The probability of having bit errors is simply $1 - (1 - \epsilon)^{(\ell+1)\times 8}$. For $\ell\epsilon \ll 1$, both probabilities can be approximated by $8 \times (\ell + 1) \times \epsilon$. Thus the single byte parity check is adequate when $\ell\epsilon \ll 1$. It can be seen below that this condition is always valid in practice. Since the experimental failure rate of the 1K-byte EROM is 300 FITS, the failure rate of each bit cannot be more than $300/(8 \times 1024) \approx 0.037$ FIT. If a ROM failure can be discovered in 24 hours, then $\epsilon < 10^{-9}$. The number ℓ is limited by the microprocessor addressing capability which is 64K. Therefore, $\ell\epsilon \ll 1$. The reason that one parity byte is used in each ROM is to detect address and data lines stuck to one or zero. Since the ROM has a capacity equal to a power of 2, a stuck output looks like an even number of ones or zeros and violates the odd parity. A stuck address will cause half the bytes to be read twice and again violate the odd parity.

The contents of the bits of the other byte used for self-test are alternating ones and zeros. When this byte is read, short-circuits in data lines are detected. If this byte is located at an address whose 10 least-significant address bits are alternating ones and zeros, reading this byte will most likely detect short-circuits among these address lines. The probability is very small that within the same ROM another byte which also contains alternating ones and zeros is read because of shorted address lines. To detect some of the short-circuits in the remaining six most significant address lines, complemented numbers are stored in these checking bytes according to their address parities. Each ROM can select one of two hexidecimal numbers, AA or 55, to store at one of two addresses. For the first ROM with 0000 starting address, the two addresses are 0155 and 02AA.

The two consecutive checking bytes must be preceded by a jump or branch instruction to bypass them in normal program execution. It is obvious that, if a single parity checking byte is located at an address with alternating ones and zeros, it alone can detect all ROM failures mentioned above except shorted data lines. It is sometimes possible to make use of the opcode and the operand of the jump or branch instruction to check the shorted data lines. If any failure occurs in the first ROM where the checking program is stored, the failure cannot always be detected. Duplicating the first ROM may be a possible solution.

After the two memory tests, a few instructions are exercised to test the CPU. Then the microprocessor starts executing the main program. Under normal circumstances, the program never comes back to the above RAM, ROM, and CPU tests. Different checks are performed in the main program. To avoid delaying the program execution, only distributed checks on the memory system are made. For example, in going through a program loop, only one RAM byte is tested and only one ROM exclusive OR is taken. However, the ROM check uses the same algorithm discussed above. The RAM check uses alternating ones and zeros which detect only shorted data lines and stuck bits because the exhaustive RAM check discussed before will destroy the temporary data stored, in addition to requiring long execution time. After each cycle of the nonexhaustive RAM check, an additional test[7] is made. Zeros are stored in the first RAM byte. Ones are stored only in RAM bytes with addresses 2^i, $i = 1,2,\cdots$. Every time all ones are loaded into an address, the contents of the first all-zero byte are also checked. The check is also distributed so as not to delay normal program execution. Most remaining RAM failures can be discovered by this additional test.

The effectiveness of the two RAM checking algorithms discussed above is similar. The first one used when turning on the power requires fewer steps and is faster. The second one does not destroy any temporary data because every check involves at most two RAM bytes (the first byte and the 2^ith byte) whose contents can be temporarily stored into CPU registers.

No CPU check is performed in the main program. A restarting sanity timer is employed to detect CPU failures. Under normal operation, the program retriggers the timer at durations shorter than the length of the timer. If the timer times out, an alarm is generated and the microprocessor system will go through its power on restart cycle again. The restarting sanity timer detects complete CPU failures. It can sometimes catch other CPU failures (for example, program counter skipping). It also reduces the damages that are caused by power transients because it restarts the system. RAM failures sometimes cause the timer to time out. ROM failures have similar effects but are more difficult to be self-detected. Output failures can only be detected by reading back the output bits immediately after each output operation.

APPENDIX B

This appendix derives the probabilities of outage and activity with and without protection switching. Figure 1 shows the configuration for a 1 × n protection switching system in each direction of transmission. The microprocessor is responsible for the switching actions of $2n$ regular channels. The unprotected system has only the regular transmission channels plus pilot detectors for alarm.

The events of interests in deriving the outage probabilities are

S: service outage without protection switching.
S_P: service outage with protection switching.
G_1: all regular channels are good.
G_2: both protection channels are good.
G_3: all regular detectors are good.
G_4: all through switches are good.
G_5: all substitute switches are good.
G_6: the microprocessor system is good.
G_7: all output switches are good.

The events G_i's are assumed to be statistically independent. Their probabilities are given by

$$P\{G_1\} = p_r^{2n}$$

$$P\{G_2\} = p_p^2$$

$$P\{G_3\} = p_d^{2n}$$

$$P\{G_4\} = p_t^{2n}$$

$$P\{G_5\} = p_s^{2n}$$

$$P\{G_6\} = p_m = p_c p_e p_a$$

$$P\{G_7\} = p_0^{2n},$$

where the notations are defined in Table I. The symbol q with appropriate subscripts is defined to be $1 - p$ with the same subscript. Let $\overline{G}_i$ be the complement of G_i and g be the joint events of the G_i's with subscripts denoting the complemented events. For instance,

$$g_0 = G_1 G_2 G_3 G_4 G_5 G_6 G_7$$

and

$$g_{35} = G_1 G_2 \overline{G}_3 G_4 \overline{G}_5 G_6 G_7.$$

If these events represent all the possible failure modes of the system, then

$$P\{S_P\} = P\{S_P g_0\} + P\{S_P g_1\} + \cdots + P\{S_P g_6\} + P\{S_P g_7\} + P\{S_P g_{12}\} + \cdots + P\{S_P g_{234567}\} + P\{S_P g_{1234567}\}. \quad (1)$$

There are a total of 2^7 terms in (1). Half the terms involve the event $\overline{G}_7$, which generates service outage regardless of the other events. Therefore,

$$P\{S_P\} = 1 - p_0^{2n} + P\{S_Pg_0\} + \cdots + P\{S_Pg_6\} + P\{S_Pg_{12}\} \\ + \cdots + P\{S_Pg_{23456}\} + P\{S_Pg_{123456}\}. \quad (2)$$

The 2^6 unknown terms in (2) are to be evaluated. Since the derivations of each term are very similar, only the details in obtaining the more involved $P\{S_Pg_{1345}\}$ and $P\{S_Pg_{26}\}$ will be given. From the definition of conditional probability,

$$\begin{aligned} P\{S_P/g_{1345}\} = {} & P\{S_P/g_{1345}, \text{three or more channel failures}\} \\ & \cdot P\{\text{three or more channel failures}/g_{1345}\} \\ & + P\{S_P/g_{1345}, \text{two channel failures}\}P\{\text{two channel failures}/g_{1345}\} \\ & + P\{S_P/g_{1345}, \text{one channel failure}\}P\{\text{one channel failure}/g_{1345}\}. \quad (3) \end{aligned}$$

It is obvious that two protection channels cannot protect three failures; hence

$$P\{S_P/g_{1345}, \text{three or more channel failures}\} = 1.$$

The joint event of three or more regular channel failures and $\overline{G}_1G_2\overline{G}_3\overline{G}_4\overline{G}_5G_6G_7$ has the conditional probability

$$P\{\text{three or more channel failures}/g_{1345}\}$$

$$= \frac{\begin{matrix}[1 - p_r^{2n} - 2np_r^{2n-1}q_r - n(2n-1)p_r^{2(n-1)}q_r^2] \\ \times p_p^2(1 - p_d^{2n})(1 - p_t^{2n})(1 - p_s^{2n})p_mp_0^{2n}\end{matrix}}{P\{g_{1345}\}}. \quad (4)$$

The second term in (3) will be evaluated next. The various events will be abbreviated by their initials after their full names are introduced; e.g., tcf represents two channel failures.

$$\begin{aligned} P\{S_P/g_{1345}, \text{tcf}\} = {} & P\{S_P/g_{1345}, \text{tcf, both failures in the same} \\ & \text{direction of transmission}\} \cdot P\{\text{both failures in the same} \\ & \text{direction of transmission}/g_{1345}, \text{tcf}\} + P\{S_P/g_{1345}, \text{tcf, one failure} \\ & \text{in each direction}\} \cdot P\{\text{one failure in each direction}/g_{1345}, \text{tcf}\} \\ = {} & 1 \cdot \{n(n-1)p_r^{2(n-1)}q_r^2p_p^2(1 - p_d^{2n})(1 - p_t^{2n})(1 - p_s^{2n})p_mp_0^{2n}\}/ \\ & P\{g_{1345}, \text{tcf}\} + P\{S_P/g_{1345}, \text{tcf, one failure in each} \\ & \text{direction}\} \cdot P\{\text{ofied}/g_{1345}, \text{tcf}\}. \quad (5) \end{aligned}$$

Equation (5) follows because one protection channel cannot protect two failures in the same direction of transmission. The second term of (5) gives

$$\begin{aligned} P\{S_P/g_{1345}, \text{tcf,ofied}\} = {} & P\{S_P/g_{1345}, \text{tcf,ofied, two} \\ & \text{associated detectors are not both good}\} \cdot P\{\text{two associated} \end{aligned}$$

$$\begin{aligned}
&\text{detectors are not both good}/g_{1345},\text{tcf,ofied}\} \\
&+ P\{S_P/g_{1345},\text{tcf,ofied, two associated detectors good}\} \\
&\cdot P\{\text{two associated detectors good}/g_{1345},\text{tcf, ofied}\} \\
&= 1 \cdot [n^2 p_r^{2n-2} q_r^2 p_p^2 (1 - p_d^2)(1 - p_t^{2n})(1 - p_s^{2n}) p_m p_0^{2n}]/ \\
&P\{g_{1345},\text{tcf,ofied}\} + P\{S_P/g_{1345},\text{tcf,ofied,tadg}\} \cdot P\{\text{tadg}/g_{1345},\text{tcf,ofied}\}.
\end{aligned} \tag{6}$$

$$\begin{aligned}
&P\{S_P/g_{1345},\text{tcf,ofied,tadg}\} = P\{S_P/g_{1345},\text{tcf,ofied,tadg,} \\
&\text{both associated substitute switches good}\} \cdot P\{\text{both} \\
&\text{associated substitute switches good}/g_{1345},\text{tcf,ofied,tadg}\} \\
&+ 1 \cdot [n^2 p_r^{2n-2} q_r^2 p_p^2 p_d^2 (1 - p_d^{2n-2})(1 - p_t^{2n})(1 - p_s^2) p_m p_0^{2n}]/ \\
&P\{g_{1345},\text{tcf,ofied,tadg}\}.
\end{aligned} \tag{7}$$

$$\begin{aligned}
&P\{S_P/g_{1345},\text{tcf,ofied,tadg,bassg}\} = P\{S_P/g_{1345},\text{tcf,ofied,} \\
&\text{tadg,bassg, both associated through switches good}\} \\
&\cdot P\{\text{both associated through switches good}/g_{1345},\text{tcf,ofied,} \\
&\text{tadg,bassg}\} + P\{S_P/g_{1345},\text{tcf,ofied,tadg,bassg, not both} \\
&\text{through switches good}\} \cdot P\{\text{not both through switches} \\
&\text{good}/g_{1345},\text{ttcf,ofied,tadg,bassg}\} \\
&= 1 \cdot [n^2 p_r^{2n-2} q_r^2 p_p^2 p_d^2 (1 - p_d^{2n-2}) p_t^2 (1 - p_t^{2n-2}) p_s^2 (1 - p_s^{2n-2}) p_m p_0^{2n}]/ \\
&P\{g_{1345},\text{tcf,oefied,tadg,bassg}\} + P\{S_P/g_{1345},\text{tcf,ofied,tadg,} \\
&\text{bassg, nbtsg}\} \cdot P\{\text{nbtsg}/g_{1345},\text{tcf,ofied,tadg,bassg}\}.
\end{aligned} \tag{8}$$

For the first term in (8), it is known that not all through switches are good because of $\overline{G}_4$. The outage probability is one because if the two failed channels have good through switches, the rest of the through switches must have failure. Finally,

$$\begin{aligned}
&P\{S_P/g_{1345},\text{tcf,ofied,tadg,bassg,nbtsg}\} = P\{S_P/g_{1345},\text{tcf,} \\
&\text{ofied,tadg,bassg,nbtsg, no other through switch failure}\} \\
&\cdot P\{\text{no other switch failure}/g_{1345},\text{tcf,ofied,tadg,} \\
&\text{bassg,nbtsg}\} + P\{S_P/g_{1345},\text{tcf,ofied,tadg,bassg,nbtsg, other} \\
&\text{through switch failure}\} \cdot P\{\text{other through switch} \\
&\text{failure}/g_{1345},\text{tcf,ofied,tadg,bassg,nbtsg}\} \\
&= 0 + [n^2 p_r^{2n-2} q_r^2 p_p^2 p_d^2 (1 - p_d^{2n\text{-}2})(1 - p_t^2)(1 - p_t^{2n-2}) \\
&\cdot p_s^2 (1 - p_s^{2n-2}) p_m p_0^{2n}]/P\{g_{1345},\text{tcf,ofied,tadg,bassg,nbtsg}\}.
\end{aligned} \tag{9}$$

In (9), the first conditional outage probability is zero because all the failures are protected by the two protection channels. The above derivations illustrate one of the basic approaches. Each event and its complement are assumed until the conditional probability of outage is either one or zero.

The third term in (3) is similarly derived.

$$P\{S_P/g_{1345},\text{ocf}\} = P\{S_P/g_{1345},\text{ocf, associated detector bad}\}$$

$$\cdot P\{\text{associated detector bad}/g_{1345},\text{ocf}\} + P\{S_P/g_{1345},\text{ocf, associated detector good}\} \cdot P\{\text{associated detector good}/g_{1345},\text{ocf}\}$$
$$= 1 \cdot [2np_r^{2n-1}q_r p_p^2 q_d(1 - p_t^{2n})(1 - p_s^{2n})p_m p_0^{2n}]/P\{g_{1345},\text{ocf}\} + P\{S_P/g_{1345},\text{ocf,adg}\}P\{\text{adg}/g_{1345},\text{ocf}\}. \quad (10)$$

$$P\{S_P/g_{1345},\text{ocf,adg}\} = P\{S_P/g_{1345},\text{ocf,adg, associated substitute switch good}\} \cdot P\{\text{associated substitute switch good}/g_{1345},\text{ocf,adg}\} + 1 \cdot [2np_r^{2n-1}q_r p_p^2 p_d(1 - p_d^{2n-1}) \times (1 - p_t^{2n})q_s p_m p_0^{2n}]/P\{g_{1345},\text{ocf,adg}\}. \quad (11)$$

$$P\{S_P/g_{1345},\text{ocf,adg,assg}\} = P\{S_P/g_{1345},\text{ocf,adg,assg, one other through switch bad}\} \cdot P\{\text{one other through switch bad}/g_{1345},\text{ocf,adg,assg}\}$$
$$+ 1 \cdot \{2np_r^{2n-1}q_r p_p^2 p_d(1 - p_d^{2n-1})[1 - p_t^{2n-1} - (2n - 1)p_t^{2n-2}q_t] \cdot p_s(1 - p_s^{2n-1})p_m p_0^{2n}\}/P\{g_{1345},\text{ocf,adg,assg}\}. \quad (12)$$

Equation (12) indicates that the status of the through switch associated with the failed regular channel has no effect on the outage probability.

$$P\{S_P/g_{1345},\text{ocf,adg,assg,ootsb}\} = P\{S_P/g_{1345},\text{ocf,adg, assg,ootsb, bad through switch in other direction of transmission}\} \cdot P\{\text{bad through switch in other direction}/g_{1345},\text{ocf,adg,assg,ootsb}\}$$
$$+ 1 \cdot [2np_r^{2n-1}q_r p_p^2 p_d(1 - p_d^{2n-1})p_t^n(n - 1)p_t^{n-2}q_t p_s \times (1 - p_s^{2n-1})p_m p_0^{2n}]/P\{g_{1345},\text{ocf,adg,assg,ootsb}\}. \quad (13)$$

$$P\{S_P/g_{1345},\text{ocf,adg,assg,ootsb,btsiod}\} = P\{S_P/g_{1345},\text{ ocf,adg,assg,ootsb,btsiod, bad switch has good detector}\} \cdot P\{\text{bad switch has good detector}/g_{1345},\text{ocf,adg,assg,ootsb,btsiod}\}$$
$$+ 1 \cdot [2np_r^{2n-1}q_r p_p^2 p_d q_d n p_t^{2n-2}q_t p_s(1 - p_s^{2n-1})p_m p_0^{2n}]/ P\{g_{1345},\text{ocf,adg,assg,ootsb,btsiod}\}. \quad (14)$$

$$P\{S_P/g_{1345},\text{ocf,adg,assg,ootsb,btsiod,bshgd}\}$$
$$= P\{S_P/g_{1345},\text{ocf,adg,assg,ootsb,btsiod,bshgd, corresponding substitute switch bad}\} \cdot P\{\text{corresponding substitute switch bad}/g_{1345},\text{ocf,adg,assg,ootsb,btsiod,bshgd}\}$$
$$+ \mathit{0} \cdot P\{\text{corresponding substitute switch good}/g_{1345},\text{ocf, adg,assg,ootsb,btsiod,bshgd}\}$$
$$= 1 \cdot [2np_r^{2n-1}q_r p_p^2 p_d^2(1 - p_d^{2n-2})np_t^{2n-2}q_t p_s q_s p_m p_0^{2n}]/ P\{g_{1345},\text{ocf,adg,assg,ootsb,btsiod,bshgd}\}. \quad (15)$$

From (3) through (15),

$$P\{S_P g_{1345}\} = p_p^2 p_m p_0^{2n}\{(x + x_3)(1 - p_d^{2n})(1 - p_t^{2n})(1 - p_s^{2n})$$

$$
\begin{aligned}
&+ x_1[q_d(1 - p_t^{2n})(1 - p_s^{2n}) + p_d(1 - p_d^{2n-1})(1 - p_t^{2n})q_s \\
&+ p_d(1 - p_d^{2n-1}) \cdot [1 - p_t^{2n-1} - (2n - 1)p_t^{2n-2}q_t]p_s(1 - p_s^{2n-1}) \\
&+ p_d(1 - p_d^{2n-1}) \cdot (n - 1)p_t^{2n-2}q_tp_s(1 - p_s^{2n-1}) \\
&+ p_dq_dnp_t^{2n-2}q_tp_s(1 - p_s^{2n-1}) + p_d^2(1 - p_d^{2n-2})np_t^{2n-2}q_tp_sq_s] \\
&+ x_4[(1 - p_d^2)(1 - p_t^{2n})(1 - p_s^{2n}) + p_d^2(1 - p_d^{2n-2})(1 - p_t^{2n})(1 - p_s^2) \\
&+ p_d^2(1 - p_d^{2n-2})p_t^2(1 - p_t^{2n-2})p_s^2(1 - p_s^{2n-2}) + p_d^2(1 - p_d^{2n-2}) \\
&\cdot (1 - p_t^2)(1 - p_t^{2n-2})p_s^2(1 - p_s^{2n-2})]\}, \quad (16)
\end{aligned}
$$

where

$$
\begin{aligned}
x_1 &= 2np_r^{2n-1}q_r \\
x_2 &= 1 - p_r^{2n} - 2np_r^{2n-1}q_r \\
x_3 &= 1 - p_r^{2n} - 2np_r^{2n-1}q_r - n(2n - 1)p_r^{2n-2}q_r^2 \\
x_4 &= n^2p_r^{2n-2}q_r^2 \\
x &= n(n - 1)p_r^{2n-2}q_r^2.
\end{aligned}
$$

To evaluate $P\{S_Pg_{26}\}$, the events

H_1: CPU is good
H_2: ROMs are good
H_3: RAMs are good

will be considered separately. Let h represent joint events similar to those for g, for example, $h_2 = H_1\overline{H}_2H_3$. As before,

$$
\begin{aligned}
P\{S_P/g_{26}\} &= P\{S_P/g_{26}, \text{both protection channels bad}\}P\{\text{both} \\
&\quad \text{protection channels bad}/g_{26}\} + P\{S_P/g_{26}, \text{one protection} \\
&\quad \text{channel bad}\}P\{\text{one protection channel bad}/g_{26}\}P\{S_P/g_{26}, \text{bpcb}\} \\
&= P\{S_P/g_{26}, \text{bpcb}, h_1\}P\{h_1/g_{26}, \text{bpcb}\} + P\{S_P/g_{26}, \text{bpcb}, h_2\} \\
&\quad \times P\{h_2/g_{26}, \text{bpcb}\} + P\{S_P/g_{26}, \text{bpcb}, h_3\}P\{h_3/g_{26}, \text{bpcb}\} \\
&\quad + P\{S_P/g_{26}, \text{bpcb}, h_{12}\}P\{h_{12}/g_{26}, \text{bpcb}\} + P\{S_P/g_{26}, \text{bpcb}, h_{13}\} \\
&\quad \times P\{h_{13}/g_{26}, \text{bpcb}\} + P\{S_P/g_{26}, \text{bpcb}, h_{23}\}P\{h_{23}/g_{26}, \text{bpcb}\} \\
&\quad + P\{S_P/g_{26}, \text{bpcb}, h_{123}\}P\{h_{123}/g_{26}, \text{bpcb}\}. \quad (17)
\end{aligned}
$$

The microprocessor operation is so complicated that simplifying assumptions have to be made before (17) can be further evaluated. There are two kinds of CPU failures. The first kind is a partial failure which may not be detected by the self-checking method discussed in Appendix A. For instances, program counter skipping and one CPU transistor failure within the CPU may not always be detectable. This partial failure may generate false switching and result in service outage. The second kind is a complete failure, and the CPU operation stops altogether. No false switching will be made in this case, and the sanity timer will detect the failure immediately. It is assumed that partial failures accounts for 20 percent of the total CPU failures.

When the CPU is partially failed, it executes the contents of the ROMs insanely. Every "instruction" has a finite probability of generating a false switching. The TPSS software contains approximately 4000 bytes of which 100 can be I/O instructions. Out of the $2n + 5$ hardware addresses, $2n$ have outputs controlling the switches. If a correct parity bit and an appropriate output switch control bit are stored in the accumulator, an I/O instruction will operate the output switch. If the protection channels are bad, the operation of the output switch will generate service outage regardless of the status of the input switch. Thus the probability p_1 that any instruction will cause an outage is approximately

$$p_1 = \frac{100}{4000} \cdot \frac{1}{4} \cdot \frac{2n}{2n + 5}.$$

When the protection channels are working, the same probability is now

$$p_2 = \frac{100}{4000} \cdot \frac{1}{8} \cdot \frac{2n}{2n + 5}$$

because the input switch should be inactive for the false output switching to generate service outage. It is to be noted that false switching can also occur randomly if the 8-bit "instruction," the 16-bit "address," the parity bit, and the switch control bit happen to match the real instruction and address. This probability is of the order $2n/2^{26}$ and is negligible compared with p_1 and p_2. On the average, each instruction takes about 4 microseconds. Thus before restoration, about

$$n_1 = \frac{\mu_c \times 60 \times 60 \times 10^6}{4}$$

"instructions" are executed. The probability p_3 that an outage will occur is

$$\begin{aligned} p_3 &= p_1 + q_1 p_1 + \cdots + q_1^{n_1 - 1} p_1 \\ &= p_1 \frac{1 - q_1^{n_1}}{1 - q_1} \\ &= 1 - q_1^{n_1}. \end{aligned}$$

When the protection channels are good, the corresponding probability is

$$p_4 = 1 - q_2^{n_1}.$$

After a false switching, it is possible that insane CPU may deactivate the switch and restore service. It may also operate other output switches to generate additional service outages. These two conditional probabilities are small. If they are ignored, the outage probability assuming partial CPU failure and bad protection channels is then p_3t/μ_c. If only one of the two protection channels is bad, let

$$p_5 = \frac{100}{4000}\cdot\frac{1}{8}\cdot\frac{n}{2n+5} + \frac{100}{4000}\cdot\frac{1}{4}\cdot\frac{n}{2n+5}.$$

The outage probability is p_6t/μ_c where

$$p_6 = 1 - q_5^{n1}.$$

When a memory failure occurs, the program counter jumps to an arbitrary location. The initial effect is somewhat like that of a partially failed CPU. Experiments indicate that outage is unlikely to occur if it has not occurred during the initial period. Since 25 out of the 4000 bytes are used to activate the output switches in normal program operation, a jump to these bytes will cause a false switching. Therefore, the false switching probability is

$$p_7 = \frac{25}{4000} + p_1$$

or

$$p_8 = \frac{25}{4000} + p_2,$$

depending on whether the protection channels are bad or good. If only one of the two protection channels is bad, the probability is

$$p_9 = \frac{25}{4000} + p_5.$$

It will be assumed that all RAM failures can be detected. Most of the RAM bytes are used for stack. The effects of the ROM and the RAM failures are assumed to be identical, but their restoration times are different because not all ROM failures are self-detectable. When the CPU fails, memory failures are assumed to have no effect on the system. This makes the evaluation of the fourth, the fifth, and the last terms in (17) unnecessary once the first term is evaluated. It is further assumed that when there are both ROM and RAM failures, the trouble can be detected immediately. Given the previous assumption, then

$$\begin{aligned} P\{S_P/g_{26},\text{bpcb},h_1\} &= P\{S_P/g_{26},\text{bpcb},h_1,\text{ complete failure}\}P\{\text{complete failure}/g_{26},\text{bpcb},h_1\} \\ &\quad + P\{S_P/g_{26},\text{bpcb},h_1,\text{ partial failure}\}P\{\text{partial failure}/g_{26},\text{bpcb},h_1\} \\ &= 0 + \frac{p_3t}{\mu_c}\frac{p_{10}q_p^2 0.2q_cp_ep_a}{P\{g_{26},\text{bpcb},h_1\}}, \end{aligned}$$

where

$$p_{10} = (p_rp_dp_tp_sp_0)^{2n}. \tag{18}$$

$$P\{S_P/g_{26},\text{bpcb},h_2\} = \frac{p_7t}{\mu_e}\frac{p_{10}q_p^2p_cq_ep_a}{P\{g_{26},\text{bpcb},h_2\}}$$

$$P\{S_P/g_{26},\text{bpcb},h_3\} = p_7\frac{p_{10}q_p^2p_cp_eq_a}{P\{g_{26},\text{bpcb},h_3\}}$$

$$P\{S_P/g_{26},\text{bpcb},h_{23}\} = p_7\frac{p_{10}q_p^2p_cq_eq_a}{P\{g_{26},\text{bpcb},h_{23}\}}.$$

Hence

$$P\{S_P,g_{26},\text{bpcb}\} = p_{10}\left\{\frac{p_3t}{\mu_c}\,0.2\,q_c + \frac{p_7t}{\mu_e}\,p_cq_ep_a + p_7p_cq_a\right\}. \tag{19}$$

The expression $P\{S_P,g_{26},\text{opcb}\}$ can be similarly evaluated. Finally,

$$P\{S_Pg_{26}\} = p_{10}\left\{2p_pq_p\left[\frac{p_6t}{\mu_c}\,0.2q_c + \frac{p_9t}{\mu_e}\,p_cq_ep_a + p_9p_cq_a\right]\right.$$
$$\left. + q_p^2\left[\frac{p_3t}{\mu_c}\,0.2q_c + \frac{p_7t}{\mu_e}\,p_cq_ep_a + p_7p_cq_a\right]\right\}. \tag{20}$$

After deriving (16) and (20), the remaining terms in (2) are easy to obtain. They will not be given here. Thus the outage probability with protection switching $P\{S_p\}$ is obtained from (2). It should be emphasized that, because there are hidden failures, multiple equipment failures cannot be neglected in evaluating the various terms in (2). In fact, the term that contributes the most to the outage probability is $P\{S_pg_{135}\}$, which involves both of the undetectable failures (detector and substitute switch).

Since the detectors used to generate alarms do not affect signal transmission, the outage probability without protection switching is simply

$$P\{S\} = 1 - p_r^{2n}. \tag{21}$$

The improvement factor is

$$\text{IF} = \frac{P\{S\}}{P\{S_P\}}. \tag{22}$$

Next, the probabilities of activity with and without protection switching will be considered. The additional events of interest are

A: activity without protection switching
A_P: activity with protection switching
G_5: protection detectors are good.

G_5 is redefined because protection detector failures generates maintenance activities, but the hidden substitute switch failures are assumed to cause no activity. To calculate the probability of activity with protection switching, notice that whenever $\overline{G}_1$, $\overline{G}_4$, and $\overline{G}_7$ occur, there will definitely be maintenance activity. Furthermore, the events $\overline{G}_2$ and $\overline{G}_5$ are detectable when G_6 is true. Therefore

$$P\{A_P\} = 1 - (p_r p_t p_0)^{2n} + (p_r p_t p_0)^{2n} p_m (1 - p_p^2 p_D^2) + P\{A_p g_0\}$$
$$+ P\{A_P g_3\} + P\{A_P g_6\} + P\{A_P g_{26}\} + P\{A_P g_{36}\} + P\{A_P g_{56}\}$$
$$+ P\{A_P g_{236}\} + P\{A_P g_{256}\} + P\{A_P g_{356}\} + P\{A_P g_{2356}\}. \quad (23)$$

In (23), $P\{A_P g_0\}$ is always zero. The last seven terms are negligible compared with $P\{A_P g_3\}$ and $P\{A_P g_6\}$. It is assumed that 10 percent of the CPU and the ROM failures will not generate alarm. The derivation of $P\{A_P g_6\}$ is similar to that of (17). For example,

$$P\{A_P/g_6 h_1\} = P\{A_P/g_6, h_1, \text{ undetectable failure}\}P\{\text{undetectable failure}/g_6 h_1\}$$
$$+ P\{A_P/g_6, h_1, \text{ detectable failure}\}P\{\text{detectable failure}/g_6, h_1\}$$

$$= 0 + \frac{t}{\mu_c} \cdot (p_r p_d p_t p_0)^{2n} (p_p p_D)^2 \cdot 0.9 \cdot q_c p_e p_a / P\{g_6 h_1\}.$$

Thus,

$$P\{A_P g_6\} = (p_r p_d p_t p_0)^{2n} (p_p p_D)^2 \left[0.9 \frac{t}{\mu_c} q_c + 0.9 \frac{t}{\mu_e} p_c q_e p_a + p_c q_a \right]. \quad (24)$$

If it is assumed that, when a detector fails, the probability that it is stuck to an ON state is 0.25, then

$$P\{A_P/g_3\} = P\{A_P/g_3, \text{ one detector bad}\}P\{\text{one detector bad}/g_3\} + \cdots + P\{A_P/g_3, 2n \text{ detectors bad}\}P\{2n \text{ detectors bad}\}. \quad (25)$$

The ith term in (25) is

$$P\{A_P/g_3, \text{idb}\} = P\{A_P/g_3, \text{idb, all bad detectors on}\}P\{\text{all bad detectors on}/g_3, \text{idb}\}$$
$$+ P\{A_P/g_3, \text{idb, some bad detectors off}\}$$
$$\cdot P\{\text{some bad detectors off}/g_3, \text{idb}\}$$

$$= 0 + \frac{t}{\mu_d} \cdot \frac{(p_r p_t p_0)^{2n} (p_p p_D)^2 p_m \binom{2n}{i} p_d^{2n-i} q_d^i (1 - 0.25^i)}{P\{g_3, \text{idb}\}}.$$

Therefore,

$$P\{A_P g_3\} = \frac{t}{\mu_d} p_m (p_p p_D)^2 (p_r p_t p_0)^{2n} \sum_{i=1}^{2n} p_d^{2n-i} q_d^i (1 - 0.25^i). \quad (26)$$

Equations (23) through (26) yield the probability of activity with protection switching $P\{A_P\}$. The probability of activity without protection switching $P\{A\}$ is simply

$$P\{A\} = 1 - p_r^{2n} + \frac{t}{\mu_b} p_r^{2n} \sum_{i=1}^{2n} \binom{2n}{i} p_b^{2n-i} q_b^i (1 - 0.25^i),$$

where

$$p_b = \frac{1}{1 + \lambda_d \mu_b}$$

and

$$\mu_b = \frac{1}{4\lambda_r}$$

is the detector restoration time without protection switching. The activity factor is given by

$$\mathrm{AF} = \frac{P\{A_P\}}{P\{A\}}. \quad (27)$$

REFERENCES

1. "L5 Coaxial-Carrier Transmission System," B.S.T.J., *53,* No. 10 (December 1974), pp. 1897–2268.
2. J. A. Buzacott, "Markov Approach to Finding Failure Times of Repairable Systems," IEEE Trans. on Reliability, *R-19* (November 1970), pp. 128–134.
3. B. V. Gnedenko, Y. K. Belyayev, and A. D. Solovyev, *Mathematical Methods of Reliability Theory* (Russian orig. and English transl. edited by R. E. Barlow), New York: Academic Press, 1969.
4. I. Welber, H. W. Evans, and G. A. Pullis, "Protection of Service in the TD-2 Radio Relay System by Automatic Channel Switching," B.S.T.J., *34*, No. 3 (May 1955), pp. 473–510.
5. W. Y.-S. Chen, "Estimated Outage in Long-Haul Radio Delay Systems With Protection Switching," B.S.T.J., *50,* No. 4 (April 1971), pp. 1455–1485.
6. G. S. Fang, "Alarm Statistics of the Violation Monitor and Remover," B.S.T.J., *55,* No. 8 (October 1976), pp 1197–1217.
7. B. A. Zimmer, "Test Techniques for Circuit Boards Containing Large Memories and Microprocessor," IEEE Computer Society Conf. Proceedings, Semiconductor Test Symposium, Oct. 19 to 21, 1976, Cherry Hill, N. J.