Continuous Computer Operational Reliability

ROBERT D. BRISKMAN†

Introduction

IN THE near future the homes, families, and lives of every individual in the United States will be protected against an aggressor attack by gigantic integrated radar defense networks. The heart of these networks will be large computer systems. With the probable use of ICBM (intercontinental ballistic missiles) and long-range strategic bombers as aggressive weapons, a criterion for defense against surprise attacks is an early-warning capability which must operate 24 hours a day, seven days a week. The consideration of methods to give maximum reliability in the operation of a computer system that must function continuously is of national importance.

Illustrative Computer System

For illustrative purposes, practical discussion will be limited to the typical large computer system described in this paragraph. Extension of consideration to computer systems of different structures or variants would be relatively simple. The computer will be divided into the basic components of synchronizer (clock), memory, logical systems (including program and arithmetic units), and input-output circuits. All operations and data flow will be serial in nature with internal, fixed programming. For ease of maintenance the computer circuits will be modularly constructed in the form of pluggable units. This type of construction will include a ferrite core memory.

Input information for the computer will come from multiple communication sources or data transmission links. Punched cards, punched tape, magnetic drum, or magnetic tape can be used if necessary for intermediate storage. The output data will be both permanently recorded and presented instantaneously on some alerting device for recognition and monitoring purposes. The computer will also have the capability of determining the proper courses of action concerning input and output data flow.

Reliability

No matter what operational characteristics and system organizations are attributed to the illustrative computer, the only important assumption is that the computer system will be so large or complex that a significant number of basic components fail daily. Actually the important fact is not the number of failures but that there is a significant probability of component malfunction.

For the case of a computer system which will continuously operate, the term reliability must be carefully examined. This term was not included in the "IRE Standards."[1] Reliability might be defined in terms of "component failure" which is related to function cessation rather than in terms of "accuracy" which is more related to degree of error. Reliability as concerned in this paper can be defined in relation to the probability of component failure. The degree of success in keeping the computer system continuously operating will be a function of the ability to predict this probability of component failure.

By the addition of a "prediction" function the variable of time is introduced. Prediction can be defined in time for this particular case by four periods.

1) The duration (dr) of the prediction interval.
2) The difference (dt) between the time of performing the prediction and the time that the prediction interval occurs.
3) The duration (dl) necessary for performing the prediction test.
4) The period (dz) elapsed between each probability test. For example, the probability of component failure during a one-hour (dr) period occurring five hours (dt) from performing a prediction test can be determined in a two-second (dl) interval which will be repeated every 20 minutes (dz).

An improvement in the prediction of reliability may be established by use of a longer dt period. However dt is determined practically from probability failure curves of various electronic components. These curves are obtained from life testing of the more sensitive electronic devices used in computers such as vacuum tubes, transistors, diodes, ferrite-core drivers, relays, etc.[2] Therefore dt will be limited in maximum length to the mean probability of operating life of the components being considered. Likewise, dr is limited by similar practical considerations. In general an improvement in the prediction of reliability may also be established by use of a longer dr period.

Prediction of operational reliability can be significantly improved by using a higher number of times that probability is sampled per unit time ($1/dz$) or a shorter dz period. The restrictions on increasing this probability sampling rate are imposed by the computer system and not by the characteristics of the individual circuit components. Basically, one restriction stems from the fact that any time used for probability sampling in a continuously operating system must be considered computer down time. High down time in a computer system creates a poor duty cycle and a low operational efficiency. Also, a normal requirement is that the computer

† Army Security Agency, Arlington 12, Va.

[1] "IRE standards on electronic computers: definitions of terms, 1956," PROC. IRE, vol. 44, pp. 1166–1173; September, 1956.

[2] For further discussion of this topic see IRE TRANS., vol. EC-5, no. 4; December, 1956.

output devices will need a certain information flow per unit time to properly function. Therefore the probability sampling rate is secondly restricted to low enough values that the information output flow necessary for continuity will be sufficient. The time required for performing each probability test (*dl*) should be as short as possible to allow either a higher number of probability samples or a decreased amount of down time with a corresponding increase in the output information rate. Actually *dl* is equal to the down time per operational period and usually is inversely proportional to the probability sampling rate.

From the above, one justified approach to maximum reliability in a continuously operating computer system is to attempt recurrent prediction of values for the precise probability of component failure during a specified period of time in the future.

Prediction Testing

Prediction testing on computers is a commonplace practice today. However, almost no computer systems must face the stringent requirements of continuous operation and prohibition of long-term outages.

The most common prediction test for computers is some type of diagnostic programming or programmed checks. A diagnostic program is designed to test as many circuit components as possible throughout the computer system in a rigorous manner to obtain early indications of malfunctioning parts. These tests are often performed with increased or reduced operating voltages. The variations in operating voltages are designed to place sensitive circuit components nearer a marginal region of performance. This causes the malfunction of components with the higher probabilities of failure. By replacing these components the over-all computer's *dt* and *dr* periods are increased for the subsequent operating period. For a certain large business computer which operates eight hours daily, one diagnostic program a day insures a 90 per cent reliability during the operating period. The whole diagnostic program takes 40 minutes including test runs with variations of plus and minus 12 per cent in all dc operating voltages.

Several disadvantages are apparent when diagnostic programming of this type is applied to a continuously operating computer system. The major disadvantage is that the operating section of the computer must usually be halted to perform the diagnostic program. As a thorough diagnostic test will probably take considerable time, it is necessary to switch to an auxiliary operating section of the computer. Switching of computer sections is always necessary if variations in operating voltages are used as part of the diagnostic testing.

The actual switching from one operational section of a computer to an auxiliary section will normally involve significant down time when the memory blocks are considered. If the data in the operational memory is unique, this information must be transferred to the auxiliary memory section with accompanying loss of time. If the data is accumulative from experience or computation, either the transfer can be effected or new data can be regenerated. Both alternatives may result in significant computer down time and may possibly cause a short term output data flow rate below requirements.

To illustrate the above, a transfer of information from the operational memory to an auxiliary memory by use of the computer's logical system would involve a minimum instructional program of SELECT, LOAD, SHIFT, SELECT, STORE, TRANSFER plus necessary check cycles. The actual time needed for a transfer can easily be computed from knowledge of storage capacity of the memory, time required for operational cycles, number of operational cycles necessary per transfer, and amount of information that can be transferred per operation cycle (usually limited by the accumulator length). With coincidence-driven ferrite-core memories in the order of 10^9 bits of storage, the time lost using the computer logic system for a memory transfer operation will be appreciable. On the other hand, if the auxiliary memory must be regenerated, even greater time can be lost when pertinent data is obtained through extensive recomputation (*e.g.*, a memory containing one thousand targets all stored in vectorially computed positions).

Computer System Organizations

It has been noted that a continuously operating computer system may consist of one or more integral computers. Obviously when failure during operation occurs or when normal maintenance is necessary, at least one stand-by computer unit would be required to insure continuity of operation. More elaboration on some possible configurations of computer systems is pertinent.

An obvious configuration is a system composed of three separate computers. One is in continuous operation, the second in stand-by, and the third in maintenance or semistand-by. When the computer in use makes a certain number of mistakes uncorrectable by the programmed error correction routines or exhibits operational errors through other failure detection devices, operations are switched to the stand-by computer. The stand-by computer has been previously prediction tested so extremely reliable operation will be maintained while the operational computer is in repair. After maintenance, the operational computer can be prediction tested and then become the stand-by computer. If the stand-by computer does fail during the time the operational computer is under maintenance, a third computer is still available.

Advantages of using the three-computer configuration are that individual computer down time is relatively unimportant and that no limitations are placed on the long term continuity of data output. However, computer system down time and short-term discontinuities in output data flow will be determined by the time required to transfer or regenerate memory information. Although this configuration for a continuous operating computer system obtains an exceptionally high reliabil-

ity by a brute force method, there are the previously mentioned advantages in such a solution. These were accrued by effectively reducing the problem to one computer operating on an eight-hour shift, substantially lowering the over-all efficiency of such a system. No further consideration will be given to a three-computer system due to the prohibitive construction cost.

A second configuration is a system composed of two computers. Although the cost of such a computer system is extremely high, it is the minimum construction with which any type of continuity of operation can be maintained.

One variation of the two-computer system configuration involves the use of an operational and a stand-by unit. The method of employment would be exactly similar to the three-computer system arrangement previously described, with the computers automatically switching upon failure of a significant component. The obvious objection to this system is the possibility of failure in the second computer while the first is being maintained, resulting in complete cessation of data output. However a computer simple enough for rapid maintenance and with an extremely low probability figure of component failure could efficiently operate in such a configuration. All the advantages and disadvantages of a two-computer system will be similar to the three-computer system with the above noted exception. To obtain maximum reliability with this two-computer system, the stand-by computer can be subjected to various prediction tests. The prediction tests should establish an insignificant probability of component malfunction over the time interval determined necessary to service the operational computer (normal or failure type of maintenance).

A second variation of the two-computer system configuration involves prediction of a predetermined high reliability figure for each of the computers over a specified time interval of practical length. At the end of this period the computers are automatically switched. For example, assume computer one is given stringent diagnostic programs until a prediction of 98 per cent reliable operation can be obtained for a certain minimum period (*e.g.*, three hours). Operations are started with computer one. Meanwhile computer two is subjected to the same diagnostic tests until it can be predicted that this computer can operate with 98 per cent reliability for the established minimum period. If computer one does not fail during the predicted three-hour reliability period, the computers will be switched at the end of that time. Failure of computer one during the predicted reliability period will cause immediate switching of operations to computer two. Computer one will then be resubjected to the prediction tests and become stand-by until computer two either fails or completes its predicted reliability period. The two computers are then alternated based on the above criteria to obtain continuity of operation.

Three of the major advantages of this computer configuration are listed below.

1) The over-all operational reliability of the above computer system can theoretically be made extremely high.
2) The computer system down time and short-term discontinuity in output data flow is determined solely by the switching time necessary to transfer stored information.
3) The majority of the switching operations normally occur when the operating computer is in perfect working order. In all previous cases this information transfer must be attempted with a malfunctioning component in the computer which may nullify the applicability of the transferred data.

One of the major disadvantages of this system is that a large number of switching operations will be necessary. This high switching rate will be required to maintain a prediction of low probability of component failure (*i.e.*, a high reliability). A high probability of component failure is inherent due to the large number of sensitive components used in present day computer circuitry. The ability to predict high reliability figures for practical periods depends directly on the mean life of the more sensitive circuit components. These mean life spans are relatively short for an application in this computer configuration. Another disadvantage is that this configuration is subject to complete stoppage if both computers fail consecutively or during a short interval.

If this system is to be practical, the time between each switching must be long. Also, the time required for performing the prediction test must be much shorter than the nominal predicted reliability period. Using the above computer configuration, transfer of information in memory cannot be done through the logical circuitry as too much time will be lost. A direct method of data transfer between memories must be used despite additional costs.

Continuous Internal Prediction

Of all the configurations previously described for a continuously operating computer system, the second variation of the two-computer system seems to utilize best the benefits of prediction and to indicate a direction towards solution.

One of the disadvantages of all the previously-mentioned computer systems is that prediction testing of the operational computer can only be accomplished before or after operation. Therefore no prediction testing can be done until either computer failure has occurred or a specified time interval of relatively long duration has elapsed.

A configuration is proposed as a possible solution whereby prediction testing is accomplished as an independent part of each operation cycle or multiple thereof. The use of prediction testing of the type previously described must be discarded as the time for the prediction test must be extremely small compared to the computer's operating cycle. This is necessary to preserve a

workable duty ratio. If a recurrent prediction test substantially increases the computer duty ratio, the probability of component failure will significantly increase with a corresponding decrease in reliability of operation. With present day computers, a 10-microsecond period for a prediction test (including circuit recovery time) repeated every 50 operational cycles may be a high figure. Variation of operating voltages as an aid to prediction testing for these short periods would also be impossible. Therefore a totally new method of prediction testing must be established.

The first consideration in developing a prediction test would be to establish new standards for component failure probability. This prediction test will be based on the application of an internally generated waveform to the computer circuitry. Each modular unit will be broken down into the various component circuits such as triggers, inverters, gates, amplifiers, delays, couplers, etc. These circuits are designed for normal operation with certain minimum-pulse type inputs. Therefore, life testing of these component circuits with various degenerative varieties of input test pulses will be performed in order to establish a favorable prediction test. A favorable prediction test would be defined by that test waveform input which causes the greatest number of malfunctions in those circuit components with the high probabilities of failure.

The parameters of a pulsed test input waveform that can be easily varied are the amplitude, shape, width, and recurrence frequency. The single test input which will provide the most favorable prediction for all the computer circuits will be a composite of pulse parameters. For example, an amplifier might respond primarily to variations in pulse amplitude, diode gates to pulse shapes, filters to pulse width, and multivibrators to pulse recurrence periods (especially transistorized triggers). A possible test input which might give favorable prediction would be a double pulsed waveform. This waveform would consist of two test pulses, each being one-quarter to three-quarters the width of the narrowest pulse used in normal operation. The two test pulses would be separated by a definite time period less than the shortest operating pulse spacing and have an amplitude of one-half to nine-tenths of the minimum voltage levels used in design. Various rise and fall times of either or both test pulses would also be employed to obtain the best prediction test. The entire duration of the test input waveform normally should occupy a period less than 2.0 per cent of an operation cycle. This would include circuit recovery time.

A computer configuration using a prediction testing system similar to that proposed above would not be very costly. The diagnostic circuitry would consist of the test waveform generator, an elementary timer (to synchronize the prediction test with the operation cycle), line drivers, and failure detection circuits. Each pluggable unit or modular circuit will also require a test waveform input and an error detection output. The computer system may employ separate busses for conveying the test input waveforms to the various sections of the computer.

The failure detection circuits can be built into each computer block , each operating section, each pluggable unit, or each modular circuit. Some advantages of placing failure detection devices into as small an operating entity as possible are listed below.

1) Failure location is tremendously simplified.
2) The actual detection devices are extremely simple.
3) The probability of error in the failure detection circuits themselves is reduced.

The above advantages may be nullified if it is necessary to use such a large number of simple detection devices that computer size and costs are substantially increased.

It is obvious that a computer system employing continuous prediction testing as an integral part of the operational cycle must be designed around the prediction-testing technique. This proposed type of testing cannot be easily added to existing computer systems. The computer system should also be designed with circuitry to allow complete transfer of information contained in memory to an auxiliary memory without the use of the logical circuitry. The construction needed for such a parallel-type transfer may be quite expensive although simple in design and extremely rapid in operation. In practice it may be advantageous costwise to sectionalize the memory and provide spare memory sections in case of failure in operating sections. Although this avoids fabrication of two complete memory blocks in parallel, sectionalization will involve considerable additional circuitry for addressing, reading, writing, parallel switching to auxiliary sections, and failure detection in each separate memory division.

Conclusion

Reliability for a continuous operating computer system can be considered by many approaches. In general, these computer systems are composed of multiple duplicated units which are interchanged to maintain continuity of operation. Of the approaches considered, a computer system which incorporates continuous prediction testing as part of the operational cycle seems a promising solution. Using this approach for design of the computer configuration and component circuits, continuous operation of a computer system may be obtained with high reliability by establishment of a favorable prediction-testing method. Computer design will also include the necessary circuitry for direct memory transfer upon failure detection.

The computer system using the proposed prediction testing technique would have the advantages of insignificant long and short term discontinuities in the infor-

mation output, a low data error level, negligible system down time, a high efficiency, and relatively low costs. The proposed prediction testing method is also advantageous as each memory transfer would be accomplished under normal operating environment, while the component failure had occurred during the more stringent test conditions.

BIBLIOGRAPHY

[1] Richards, R. K. *Arithmetic Operations in Digital Computers*' New York: D. Van Nostrand Co., Inc., 1955.
[2] Shea, R. F. *Principles of Transistor Circuits*, New York: John Wiley and Sons, 1953.
[3] Goldman, S. *Information Theory*, New York: Prentice-Hall, Inc., 1953.
[4] Engineering Research Associates. *High Speed Computing Devices*, New York: McGraw-Hill Book Co. Inc., 1950.

Discussion

Chairman Parsons: The speaker was very careful to develop a theoretical computing machine for his description of the continuous computer operational reliability; I wonder if we can comment on it concerning the applicability of this particular marginal technique to such existing systems as the SAGE?

Mr. Briskman: I stated, I believe, in the close of my speech that this cannot be added to the existing systems. My familiarity with the SAGE system is very slight; however, from the size there it might have been a very interesting experiment to try the prediction system of techniques, such as was proposed, rather than the standard formula technique which is employed. In other words, reducing various dc operating voltages, and running diagnostic programs. Actually the SAGE system is probably a little small to benefit on a cost basis, on changing to this alternative method of prediction testing.

J. G. Tryon (Bell Telephone Labs.): I question whether continuous internal prediction testing via special test signals can be realized with moderate equipment cost. Restoration of wave shapes is so extensive in a good computer that very many test signals and associated verification circuits would be required. I estimate that the size of the computer would be doubled.

Field Performance of a New Automatic Fault-Locating Means

J. F. SCULLY† AND L. P. COLANGELO‡

A MODERN Air Force electronic system does the work of scores of people. Viewed as a labor-saving device, it is comparable to an automatic telephone exchange. There is, however, a great organizational difference between these two automatic systems. A digital calculator, for example, is essentially a single unit of great complexity, whereas the telephone exchange is composed of a multiplicity of units, each capable of working independently. The telephone exchange can be operated successfully by disconnecting its malfunctioning circuits, but the entire digital calculator is rendered useless if one component fails. It is as though all the automatic clerks have staged a walk-out until the single troublesome source is located.

The net result of the ever-increasing complexity of electronic equipment has been that the shortage of adequately trained personnel in the Air Force has been accentuated. Not only has research and development work been hampered, but the reliability of operational field equipment and the establishment of sound maintenance programs for such equipment, have been adversely affected. It has therefore become incumbent upon designers, engineers, and manufacturers to strive for greater simplicity of electronic equipment and to produce equipment easier to maintain.

At the outset, we must clarify what we mean when referring to "reliability" in connection with a large ground electronic equipment. Since such equipment is repaired, and so made operational again after each failure, it is a different problem from, say, a missile or system in which one failure renders the device useless for all time. So, while the mean time between failures is of great importance, and the probability of successful operation for a given time interval is also important, an additional factor, the "down time" of the system, is of equal importance. We shall define the reliability of our system in terms of its operational efficiency as follows. The efficiency of a system is the ratio of the time during which the machine is capable of correct operation to the time during which correct operation is desired. Thus, if correct operation is experienced whenever we want it, the system has an efficiency of 1; if it never works when we want it to, an efficiency of 0. This definition makes

† Monroe Calculating Machine Co., Morris Plains, N. J.
‡ Rome Air Dev. Center, Rome, N. Y.