LA-UR-77-1394

TITLE: AVAILABILITY ANALYSIS FOR HIGH RELIABILITY COMPUTER SYSTEMS IN NUCLEAR FACILITIES

AUTHOR(S): EDWARD P. SCHELONKA Q-4

SUBMITTED TO: FOR PRESENTATION TO THE 18th ANNUAL INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT (INMM) MEETING, JUNE29-JULY 1, 1977, IN WASHINGTON, DC

los alamos
scientific laboratory
of the University of California
LOS ALAMOS, NEW MEXICO 87545

An Affirmative Action/Equal Opportunity Employer

MASTER

UNITED STATES
ENERGY RESEARCH AND
DEVELOPMENT ADMINISTRATION
CONTRACT W-7405-ENG-36

AVAILABILITY ANALYSIS FOR HIGH RELIABILITY COMPUTER SYSTEMS IN NUCLEAR FACILITIES

Edward P. Schelonka
LASL Safeguards Staff (Q-4)
Los Alamos Scientific Laboratory
Los Alamos, NM 87545

ABSTRACT

Availability, defined as the ratio of time a computer system is functioning normally to the total time it is in demand, is a measure of the overall accessibility to the system and its operational effectiveness. This ratio allows estimates of down time to be calculated for contingency planning. Single and multiple machine configurations are evaluated in terms of typical component values for mean time between failure (MTBF) and mean time to repair (MTTR), and the Availability of each configuration is computed. Through the use of interconnected, redundant processors with multiprogramming operating systems and all input data provided to each processor, down time for even failure prone units can be reduced from 781 to 32.3 hours per year. Several interconnection methods are shown with projected reliability data.

INTRODUCTION

The primary function of information systems in nuclear facilities is to provide data for decisions. The quality, timeliness, and accessibility of data are particularly important in emergency response situations. In this analysis primary emphasis is placed on the Availability of computational resources.

RELIABILITY

Data on failure rates of individual devices such as resistors, capacitors, inductors, diodes, transistors, and integrated circuits are used to predict the reliability of an assembly of such devices (1). When they are assembled into components, manual calculations and computer programs tabulate device strings for required functions and the associated probability of failure calculated for each required mode of operation. From these probabilities an overall theoretical mean time between failure (MTBF) is determined for each component as a measure of its reliability. If failures are assumed to occur randomly in time the probability P that a component will function normally at any time t is given by

$$P = \exp(-t/MTBF). \qquad (1)$$

For example, if the time since the last failure is equal to the MTBF there is a 36.8% probability that the component has not failed.

After a number of components have been assembled, life test data are accumulated in order to determine an experimental value for the MTBF, and comparisons to theoretical values are made. Often thermal and overvoltage stresses are applied in accelerated life tests to obtain preliminary MTBF estimates as early as possible.

In ordinary operating environments additional sources of failure may contribute to down time. These are listed in Table 1. Careful system design can reduce these effects: for example by incorporating standby batteries to prevent loss of power and the use of optical isolation to eliminate externally induced line transients. Cost-benefit trade-offs usually determine the degree of protection implemented. The remaining sources of failure are then combined into an effective system MTBF.

The time required to return a component to service is its mean time to repair (MTTR). Some of the factors contributing to MTTR are shown in Table 2. Values of MTTR can extend from fractions of a second in the case of automated repair to days if personnel or logistical delays are encountered.

Availability is defined as the ratio of time a computer system is functioning normally to the total time the system is in demand. Availability is also expressed in terms of MTBF and MTTR as

$$A = \frac{MTBF}{MTBF + MTTR} \tag{2}$$

ARCHITECTURAL DESIGN AND ANALYSIS

Safeguards computational requirements for current and projected nuclear facilities are modest and can be satisfied by stand-alone commercially-available minicomputers. An example is shown in Figure 1. One hundred and thirty-five hours of down time per year is not satisfactory for most information system functions, therefore, improvement is sought through redundancy. The following analysis follows that of Feller (2) for systems requiring at least m out of N parallel connected units functioning with, in general, differing Availabilities. For at least one unit functioning of four parallel units

$$A = S(1) - S(2) + S(3) - S(4) \tag{3}$$

and for at least two of four

$$A = S(2) - 2S(3) + 3S(4) \quad . \tag{4}$$

Intermediate terms S(1) through S(4) are expressed (for N = 4) as:

$$S(1) = A_1 + A_2 + A_3 + A_4 \quad (3)$$

$$S(2) = A_1A_2 + A_1A_3 + A_1A_4 + A_2A_3 + A_2A_4 + A_3A_4 \quad (6)$$

$$S(3) = A_1A_2A_3 + A_1A_2A_4 + A_1A_3A_4 + A_2A_3A_4 \quad (7)$$

$$S(4) = A_1A_2A_3A_4 \quad (6)$$

with the intermediate term coefficient in Table 3. Results for a variety of configurations are shown in Figures 2 through 5. Down time is reduced to a very tolerable level of four hours per year with commercially available units using double redundancy and to 0.05 hours per year with high reliability units designed by the Bell Telephone Company for their Electronic Switching System (ESS) Machines. Going to a "one in three" configuration increases reliability to that approaching the ESS machines while using less expensive commercial units.

It is possible and perhaps desirable to exploit the unused capacity of each unit by allowing it to function in a foreground/background processing mode. The work load demands of the voter functions shown in Figure 4 are relatively small yet these allow for automatic error detection. Since success measured by any "m of N" implies an independent method of decision, voters or comparitors detect data stream differences as single or multiple failures occur. With a single failure the remaining two consistent data streams are selected as being correct. With multiple failures, comparitor output shows merely lack of consistency between data streams. Subsequent analysis is required to determine which data are valid. This potential time delay may not be tolerable, so preference is given to the "two of three" architectures.

Advanced security provisions are being developed for minicomputers and are expected to be available commercially in FY 79. These will be modular in nature through the addition of additional hardware to a standard minicomputer mainframe and use of a modified operating system. This increased complexity in both hardware and software is expected to reduce the MTBF and increase the down time as shown in Figure 5. In redundant configurations however these secure computers are expected to have an acceptable reliability performance of 50 hours per year down time for the "two of three" configuration.

REFERENCES

1. Military Standardization Handbook Reliability Reduction of Electronic Equipment, MIL-HDBK-217B (September 20, 1974).

2. Feller, William, "An Introduction to Probability Theory and its Applications," John Wiley and Sons, Inc., New York, 3rd Edition 1968, p. 106.

Table 1. Summary of contributions to effective computer system MTBF. [3]

HARDWARE FAILURE

SOFTWARE FAILURE

POWER-LINE VOLTAGE INTERRUPTION AND TRANSIENTS

INCIDENT TRANSIENT ELECTROMAGNETIC ENERGY DUE TO LIGHTNING OR MAN-MADE SOURCES

AIR CONDITIONING FAILURE

HUMAN ERROR

ROUTINE PREVENTATIVE MAINTENANCE

Table 2. Factors related to the MTTR.

PERFORMANCE MONITORING TO IDENTIFY A FAILURE

AVAILABILITY OF TRAINED PERSONNEL

DESIGN AND LAYOUT OF THE COMPONENT

DIAGNOSTICS FOR FAULTY COMPONENT ISOLATION

AVAILABILITY OF SPARE PARTS

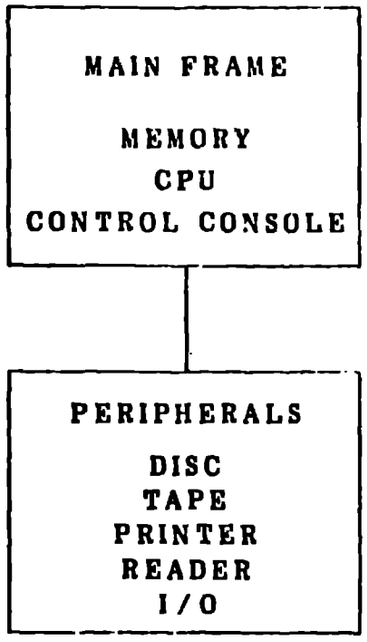
REMOVAL AND REPLACEMENT

REALIGNMENT OR RECALIBRATION WHEN REQUIRED

AVAILABILITY OF AUTOMATIC FUNCTION SENSING AND REDUNDANT COMPONENT SWITCHING

Table 3. Intermediate term coefficients for computation of Availability of composite computer configuration.

At Least m of ...	S(N)							
m	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)
1	1	-1	1	-1	1	-1	1	-1
2		1	-2	3	-4	5	-6	7
3			1	-3	6	-10	15	-21
4				1	-4	10	-20	35
5					1	-5	15	-35
6						1	-6	21
7							1	-7
8								1



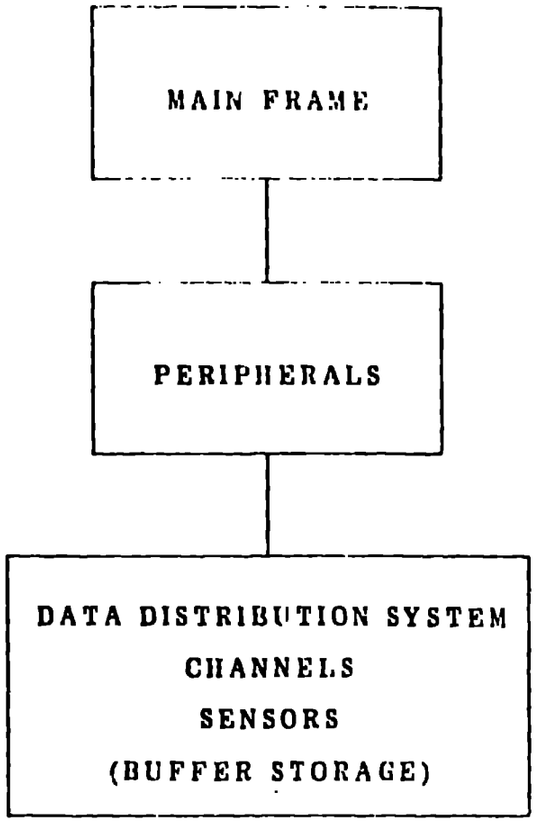
MTBF 830 hours

MTTR 13 hours

Availability .98457885

Down time 135 hours/year

Fig. 1. Basic computational unit.



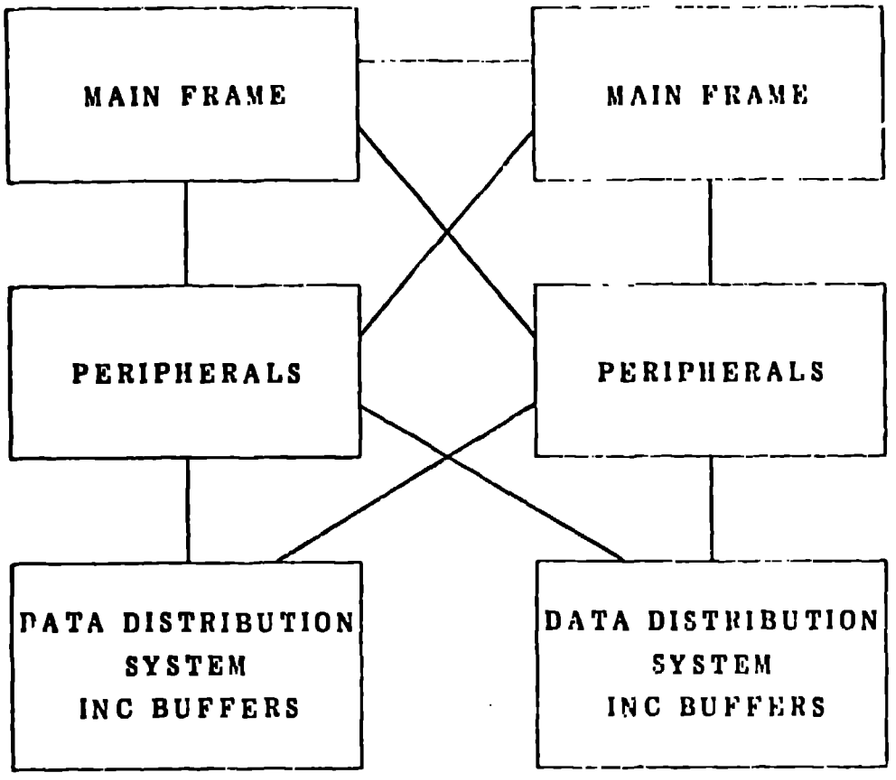
A = .96530

Down time 303 hours

With buffer storage A = .9787709

Down time 180 hours

Fig. 2. Computer with Data Distribution System



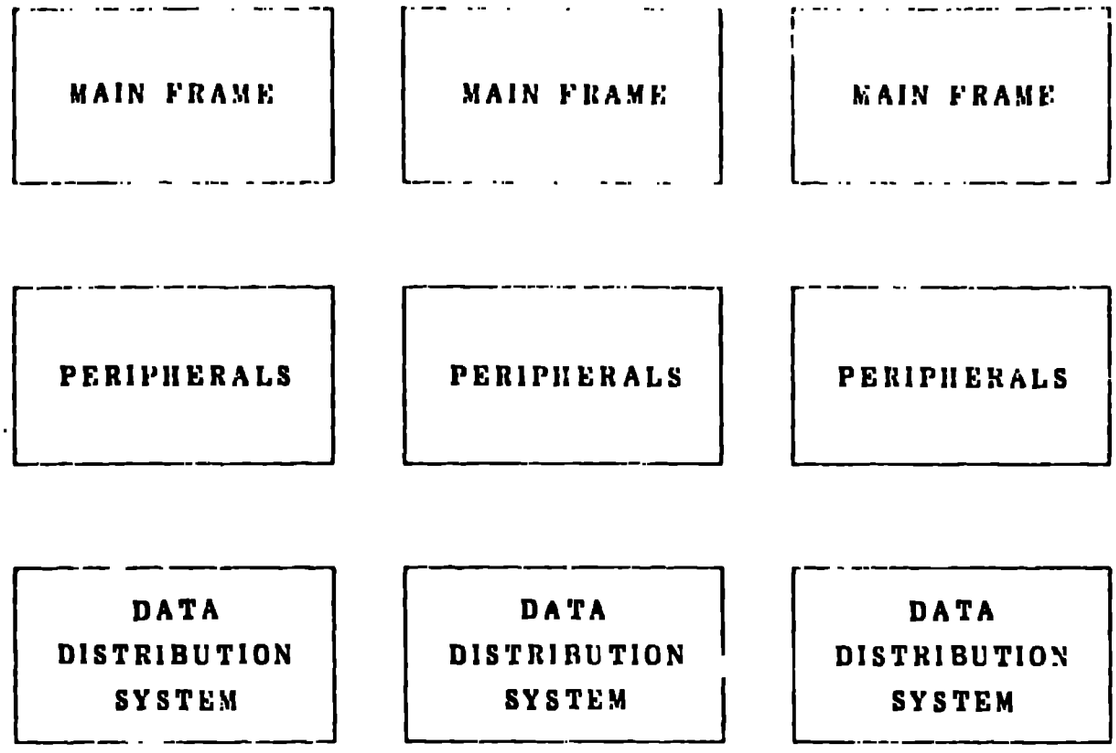
A = .99954933

Down time 4 hours per year

With high reliability designed units

Down time .05 hours per year

Fig. 3. Double redundancy.



Interconnection not shown consists of each voter, main frame, set of peripherals and data distribution system connected to all others.

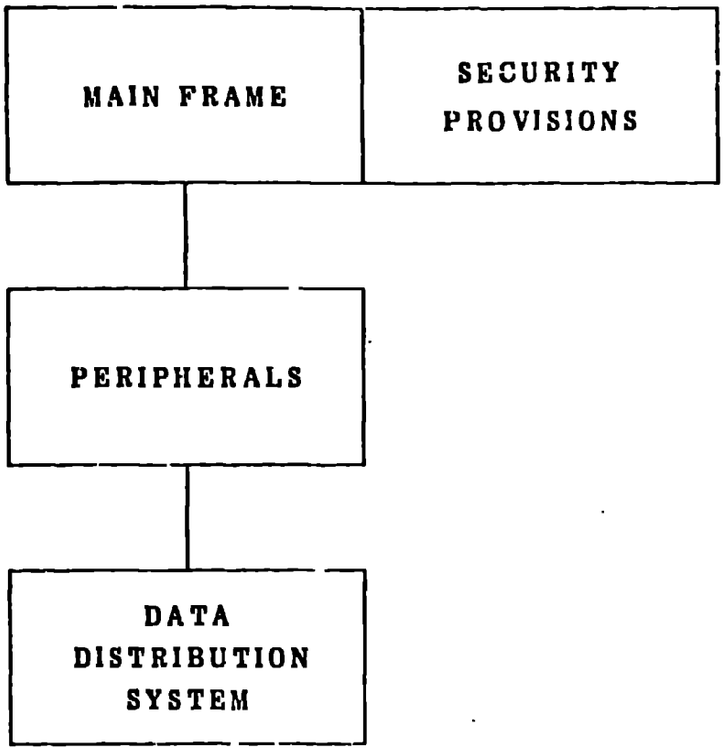
For at least one of three functioning A = .999993555

Down Time .6 hours per year

For at least two of three functioning A = .99866711

Down Time 12 hours per year

Fig. 4. Three parallel redundant paths.



MTBF = 600 hours
MTTR = 15 hours
A = .9756

With data distribution system
A = .95609
Down Time 385 hours per year

With double redundancy
A = .998071
Down Time 17 hours per year

With three paths (Fig. 6)

At least one of three
A = .99991534
Down Time 1 hour per year

At least two of three
A = .99438
Down time 50 hours per year

Fig. 5. Reliability projections for computer units with advanced security provisions.