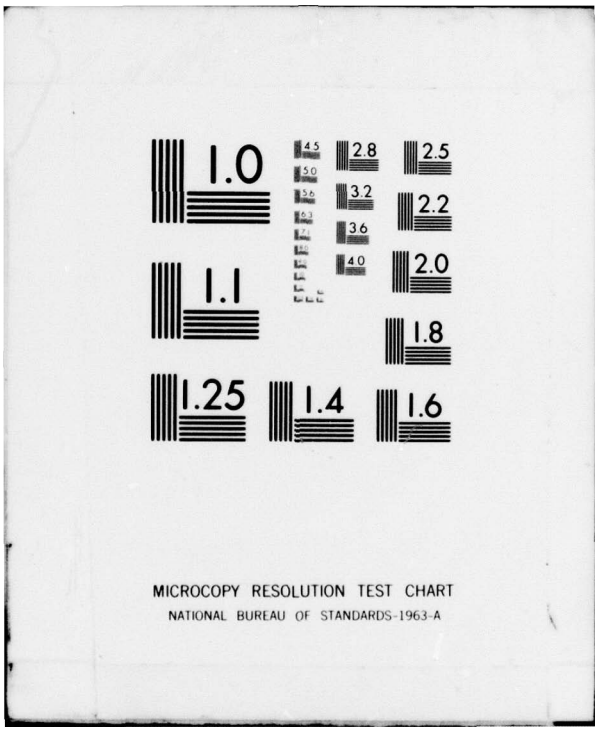
AD-A073 919 ELECTRONIC SYSTEMS DIV HANSCOM AFB MA F/G 15/7
AN INVESTIGATION OF RELIABILITY, MAINTAINABILITY, AND AVAILABIL--ETC(U)
MAR 79 J S GORDON

UNCLASSIFIED ESD-TR-79-139 NL

| OF |
AD
A073919

END
DATE
FILMED
10-79
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

ESD-TR-79-139

LEVEL II

AD A073919

AN INVESTIGATION OF RELIABILITY, MAINTAINABILITY, AND AVAILABILITY IN THE TACC AUTOMATION PROGRAM

John S. Gordon, Captain, USAF
TACC AUTO Engineering Division
Hanscom AFB, MA 01731

March 1979

Approved for Public Release;
Distribution Unlimited.

Prepared for

DEPUTY FOR COMMUNICATIONS AND INFORMATION SYSTEMS
ELECTRONIC SYSTEMS DIVISION (AFSC)
HANSCOM AIR FORCE BASE, MA 01731

LEGAL NOTICE

When U. S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

Do not return this copy. Retain or destroy.

This Technical Report has been reviewed and is approved for publication.

Thomas W Bailey

THOMAS W. BAILEY, Lt Col, USAF
Chief, Engineering Division

Robert I. Roseman

ROBERT I. ROSEMAN, Lt Col, USAF
Program Director, CAFMS
Deputy for Communications
and Information Systems

Charles P. Cabell Jr

CHARLES P. CABELL, JR, Col, USAF
Director
Combat Information Sys Directorate

FOR THE COMMANDER

William E. Thurman

WILLIAM E. THURMAN, Brigadier General USAF
Deputy
Communications & Information Systems

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER ESD-TR-79-139	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* AN INVESTIGATION OF RELIABILITY, MAINTAINABILITY, AND AVAILABILITY IN THE TACC AUTOMATION PROGRAM		5. TYPE OF REPORT & PERIOD COVERED In-House Report, Through March 1979 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) John S. Gordon, Captain, USAF		8. CONTRACT OR GRANT NUMBER(s) IN-HOUSE
9. PERFORMING ORGANIZATION NAME AND ADDRESS TACC AUTO Engineering Division Hanscom AFB, MA 01731		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Program Element Number 27412F
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Communications and Information Systems Electronic Systems Division (AFSC) Hanscom Air Force Base, MA 01731		12. REPORT DATE March 1979 13. NUMBER OF PAGES 37
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)* 12 36p.		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for Public Release; Distribution Unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Reliability	Reliability Models
Maintainability	Reliability Enhancement
Availability	Reliability Predictions
Redundancy	TACC Automation

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This report contains reliability, maintainability, and availability (RMA) information concerning RMA background and principles, RMA complexities encounted by the TACC Automation Program, and methods for enhancing RMA. Basic derivations and formulas are presented for modeling various redundant configurations. TACC Automation RMA complexities are discussed in terms of basic RMA definitions, system definition deficiencies, and RMA predictions. RMA enhancements are addressed in terms of RMA growth and RMA improvement.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

127100

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION I

INTRODUCTION

The Tactical Air Control Center (TACC) is the senior element of the Tactical Air Control System and is the facility through which the Air Force Commander exercises control of the Tactical Air Forces. The objective of the TACC Automation Program is to improve the decision-making process by replacing the current manual data handling systems with a computer controlled information processing, storage, display, and dissemination system. At the time this paper was begun, the program had gone through full scale development and had progressed to the point where transition to production was appropriate, pending a formal Production Decision. However, the System Specification values for Reliability, Maintainability, and Availability (RMA) were not yet finalized. The TACC Auto RMA value specification problem was due to a number of factors. These factors include the following:

a. Deletion of on-line diagnostic programs from the System Specification due to funding problems,

b. Reluctance of the user (Tactical Air Command) to accept the consequences that resulted from the agreed-upon deletion of the on-line diagnostic programs,

c. Increase of items in the system configuration,

d. Concerns by the supporting command (Air Force Logistics Command) that the system might not be logistically supportable,

e. Unavailability, due to funding constraints during tests and evaluations, of adequate maintenance procedure documentation and equipment spares,

f. Insufficient maintenance training for properly supporting tests and evaluations, and

g. Confusion about RMA, in general.

SECTION II

STATEMENT OF THE PROBLEM

The original goals of this paper were to investigate RMA principles, to explore the RMA complexities and problems unique to the TACC Auto Program, and to help determine the RMA values that should be used in the System Specification. This last goal is no longer appropriate since at the present time, the TACC Auto Program is undergoing a restructuring. Apparently, the program will be restarted and different, more modern hardware will be used. With the new restart in mind, the System Specification was rapidly finalized, with retention of the original RMA values. The finalized System Specification will be used, in some form, as guidance in the new effort. Eventually, when details of the new hardware are known, the appropriateness and achievability of the present TACC Auto RMA System Specification values will again need to be evaluated.

To help in the future effort that will be required for the specification of TACC Auto RMA values, this paper will present material to improve understanding of the problems involved with specifying TACC Auto RMA values. Specifically, this paper will address the following areas:

a. RMA background and principles,

b. RMA complexities unique to TACC Auto, and

c. Methods for enhancing RMA.

SECTION III

DISCUSSION

A. RMA BACKGROUND

1. Reliability

a. Reliability Model Theory. Figure 1 (1:18) illustrates the "bath tub" shape that is typical of electronic equipment failures. During the useful life period of the equipment, a constant hazard (or failure) rate is described by an exponential failure model as will be seen below:

$$\text{HAZARD RATE} \triangleq h(t) = \frac{\text{RATE OF FAILURE}}{\text{NUMBER OF SURVIVORS}}$$

$$= \frac{\frac{d}{dt}(N_{flr})}{N_{surv}} = \text{CONSTANT} \triangleq \lambda$$

The reliability, R(t), is defined as the probability of survival to any time t:

$$R(t) \triangleq \frac{N_{surv}}{N_{total}} = \frac{N_{surv}}{N_{surv} + N_{flr}}$$

In terms of R(t) and since

$N_{flr} = N_{total} - N_{surv}$,

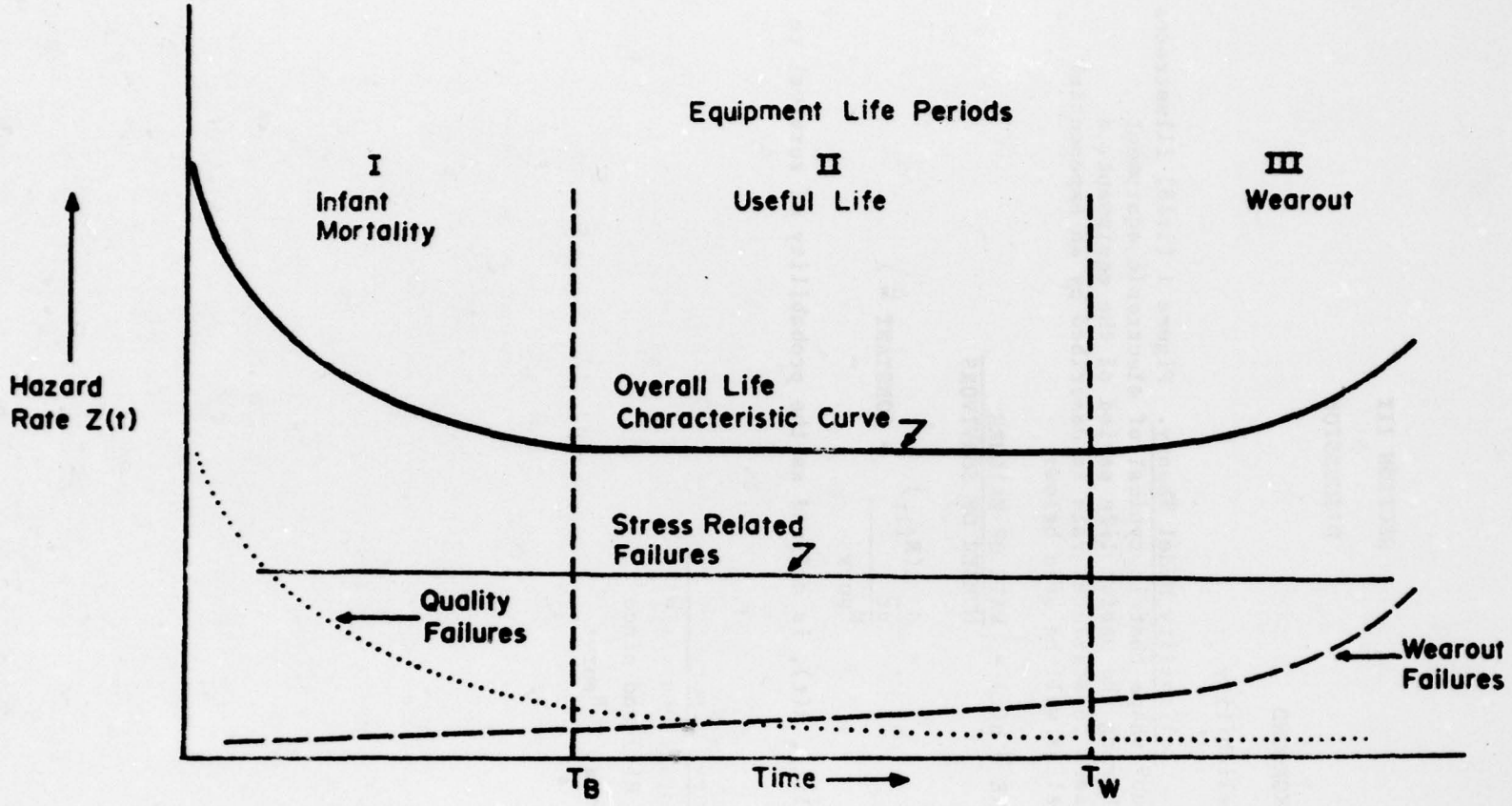


FIGURE 1

COMPONENTS OF FAILURE

$$h(t) = \frac{\frac{d}{dt}(N_{total} - N_{surv})}{N_{surv}} = \frac{-\frac{d}{dt}(N_{surv})}{N_{surv}}$$

$$= \frac{-\frac{d}{dt}(R \cdot N_{total})}{R \cdot N_{total}} = \frac{-\frac{dR}{dt}}{R} = \lambda$$

Re-arranging,

$\frac{dR}{R} = -\lambda\, dt$, integrating both sides,

$\ln R = -\lambda t$, which is equivalent to:

$R = e^{-\lambda t}$ this is the exponential relationship that was originally stated as being a result of the constant failure rate.

The failure density function, f(t), is defined as the probability that a failure will occur in the next time increment dt:

$$f(t) = \frac{\frac{d}{dt}(N_{flr})}{N_{total}} = \frac{\frac{d}{dt}(N_{total} - N_{surv})}{N_{total}} = \frac{\frac{-d}{dt}(N_{surv})}{N_{total}}$$

But the last expression is the negative of the derivative of R(t), so:

$$f(t) = -\frac{dR}{dt} = -\frac{d}{dt}(e^{-\lambda t}) = \lambda e^{-\lambda t}$$

The probability that a failure will <u>not</u> occur before time t_1 can be expressed as $P(t > t_1)$. In terms of f(t), this becomes:

$$P(t > t_1) = \int_{t_1}^{\infty} f(t)\, dt = \int_{t_1}^{\infty} \lambda e^{-\lambda t}\, dt = e^{-\lambda t_1}$$

The last result is equivalent to the R(t) expression evaluated at time t_1:

$$R(t_1) = e^{-\lambda t_1} = P(t > t_1)$$

The expected, or mean, value of the time to failure, E(t), can be found from the following expression (2:121):

$E(t) = \int_{-\infty}^{\infty} tf(t)dt$. For $t > 0$, and using $f(t) = -\frac{dR}{dt} = -R'$,

$E(t) = \int_{0}^{\infty} t\,(-R')dt$. Using integration by parts,

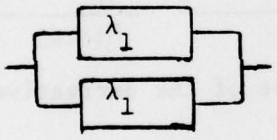
$E(t) = \int_{0}^{\infty} R\,dt = \int_{0}^{\infty} e^{-\lambda t}dt = \frac{1}{\lambda} \triangleq$ Mean Time Between Failure = MTBF

This last result, MTBF= $\int_{0}^{\infty} Rdt$, along with $R = e^{-\lambda t}$, will be used frequently in the following sections to find the MTBF of redundant systems.

b. Redundancy. The reliability of a system can be significantly enhanced through the use of redundancy, as will be shown below. Redundancy involves designing one or more alternate signal paths through the addition of parallel elements. Redundancy can be classified as active or standby (1:186). With standby redundancy, external elements are required to detect failures and to switch to an alternate element or path, to replace a failed element or path. With active redundancy, no external elements are required and the parallel units are always operating simultaneously.

Consider the following actively redundant units with identical failure rates:

ACTIVE REDUNDANCY (NO REPAIR)



$r_1 = e^{-\lambda_1 t}$

$MTBF_1 = \frac{1}{\lambda_1}$

The "system" represented by the above sketch will still be operational if either of the λ_1 units are still operating. The system reliability, R, can be expressed as:

R = 1 - (Probability that both units have failed). The probability that one of the units has failed is $1 - r_1$, and since the units are considered to be independent,

$$R = 1 - (1 - r_1)(1 - r_1) = 1 - (1 - r_1)^2.$$

Using the previously derived expression for MTBF, the equivalent MTBF of the actively redundant sytem is:

$$MTBF = \frac{1}{\lambda} = \int_{0}^{\infty} Rdt = \int_{0}^{\infty} [1 - (1-r_1)^2]\,dt$$

$$= \int_{0}^{\infty} [1 - (1 - e^{-\lambda_1 t})^2]\,dt = \frac{3}{2\lambda_1} = 1.5\ MTBF_1$$

In the general case where one unit out of a total of n units must operate, $R = 1 - (1 - r_1)^n$, and the system MTBF can again be found by integrating the R equation. Table 1 illustrates the enhancements that result from incrementally increasing the redundancy:

Table 1. ACTIVE REDUNDANCY (NO REPAIR)

n (Number of units)	MTBF IMPROVEMENT FACTOR	DIFFERENCE BETWEEN FACTORS
1	1.00	
2	1.50	0.50 (=1/2)
3	1.83	0.33 (=1/3)
4	2.08	0.25 (=1/4)
5	2.28	0.20 (=1/5)

As can be seen from Table 1, additional redundancy improves the reliability, but the magnitude of the improvement decreases as successive parallel units are added. Also, examination of the successive differences between the factors suggests the following general equation:

$$MTBF = MTBF_1 \sum (1 + 1/2 + 1/3 + 1/4 + 1/5 + \text{---})$$

$$= MTBF_1 \sum_{i=1}^{n} \frac{1}{i}$$

Another active redundancy situation is where at least "k out of n" parallel units must be in operation in order for the system to be considered operational. The reliability solution for this situation can be found by considering the binomial probability distribution. For example, if at least 8 out of 10 units must be operational, the system reliability is:

$$R = r_1^{10} + \binom{10}{9} r_1^{9} (1-r_1) + \binom{10}{8} r_1^{8} (1-r_1)^2$$

Using $r_1 = e^{-\lambda_1 t}$, $MTBF = \int_0^\infty R\, dt$ yields:

$$MTBF = \frac{2.98}{\lambda_1}$$

The above technique is straight forward, but a fairly long derivation yields the following simple result (3):

$$MTBF = \frac{MTBF_1}{\sum_{i=k}^{n} \frac{1}{i}}$$

There are two cases for standby redundancy: "operating" and "non-operating". In both cases, external elements must be able to detect failures and perform appropriate switching actions. However, with "operating" standby redundancy, all units are always "powered up". With "non-operating" standby redundancy, power is not applied to standby units until a failure is detected in the unit that was previously in operational use. In the general case, the reliability of the external detection and switching elements should be considered. However, if the external devices are considered to be much more reliable than the functional units, the results are as shown in Table 2:

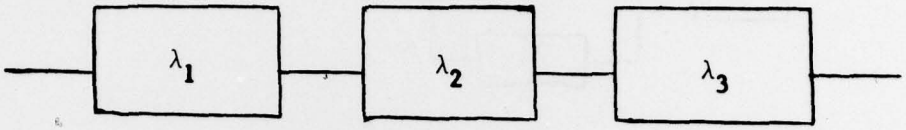
Table 2 STANDBY REDUNDANCY (NO REPAIR)

MTBF IMPROVEMENT FACTOR

n (Number of units)	OPERATING	NON-OPERATING	
1	1.00	1.00	(ASSUMES PERFECT
2	1.50	2.00	SWITCHING AND
3	1.83	3.00	DETECTION)
4	2.08	4.00	
5	2.28	5.00	

As would be expected, the MTBF improvement factors shown in Table 2 for operating standby redundancy are identical to the factors previously shown for active redundancy. The simple result for non-operating standby redundancy may seem intuitively obvious, but the actual derivation is non-trivial (4:238). One caution should be offered for the non-operating standby redundant case: the underlying assumption is that the failure rates on non-powered units are not changed due to environmental factors or aging effects that might occur during a long dormancy period.

c. Series Reliability. Consider the following system where all three units must operate in order to have a successful mission:



r_1 r_2 r_3

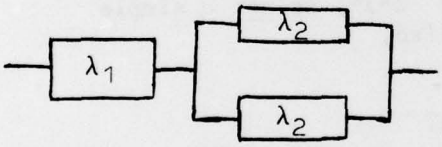
The overall system reliability is a product of the individual reliabilities: $R = r_1 \cdot r_2 \cdot r_3$, and the system MTBF is:

$$MTBF = \frac{1}{\lambda} = \int_0^\infty R\, dt = \int_0^\infty e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \cdot e^{-\lambda_3 t}\, dt$$

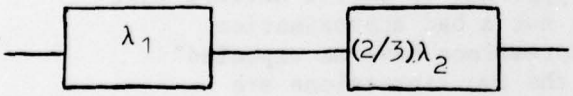
$$= \frac{1}{\lambda_1 + \lambda_2 + \lambda_3}$$

In words, the system MTBF of a series system can be found by taking the reciprocal of the sum of the individual failure rates.

d. Series-Parallel Reliability. Consider the following system composed of a series unit and two actively redundant units:



Since the failure rate of the parallel system is $(2/3)\lambda_2$, the following model "seems" intuitively appealing:

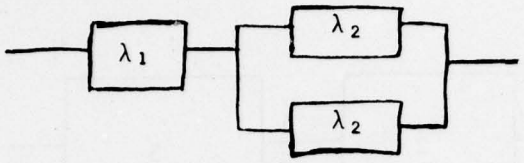


Using the previous results for serial system reliability,

$$MTBF = \frac{}{\lambda_1 + (2/3)\lambda_2}$$

IF $\lambda_1 = \lambda_2$, $MTBF = \frac{1}{\lambda_1 + (2/3)\lambda_1} = \frac{0.6}{\lambda_1}$

However, if we consider the same system again, but from the reliability integral viewpoint:



$$r_1 = e^{-\lambda_1 t} \qquad r_2 = 1 - (1 - e^{-\lambda_2 t})^2$$

$$R = r_1 \cdot r_2$$

$$MTBF = \int_0^\infty R\,dt = \int_0^\infty e^{-\lambda_1 t} \cdot \{1 - (1 - e^{-\lambda_2 t})^2\}\,dt$$

If we again let $\lambda_1 = \lambda_2$, the result is: MTBF = $\frac{2}{3\lambda_1}$, which conflicts with the previous result, that said: MTBF = $\frac{0.6}{\lambda_1}$

The reason for this "anomaly" is that the reliability equation for the parallel system, $r_2 = 1 - (1-e^{-\lambda_2 t})^2$, is <u>not</u> a simple exponential of the $e^{-\alpha t}$ form. Also,

$$h = \frac{-\frac{dr_2}{dt}}{r_2} \neq \text{CONSTANT}$$

In the former case, the "intuitive" approach in effect assumed that $r_2 = e^{-(2/3)\lambda_2 t}$. Actually, this is not a bad approximation for the actual r_2 equation: both expressions have an expected value of $3/(2\lambda_2)$, and the graphs of the two expressions are somewhat similar in shape. Due to the simplicity and fairly good results that are obtained, the approximate method is often used. A theorem attributed to Drenick (3) indicates that the approximate method always gives a conservative estimate of the actual MTBF of series-parallel systems.

2. Maintainability

Maintainability is often referred to in terms of the Mean Time To Repair (MTTR). Wheras the reliability (MTBF) is largely dependent on design, device physics, and component selection, MTTR also depends on external factors whose effects may be hard to quantify. These external factors include such items as built in test equipment (BITE), diagnostic computer programs, documentation of procedures to assist in fault isolation, ease of removal and replacement of faulty modules, and availability of spare equipment items.

As was the case with reliability, redundancy can have a significant role when maintainability is considered (especially when MTTR is defined as it is in TACC Auto). In the following sections, two maintainability situations will be considered: scheduled maintenance, and on-line repair.

a. Scheduled Maintenance. If the operational concept permits, scheduled, or preventive, maintenance can be performed. Preventive maintenance is most often associated with analog circuits that require periodic "tuning" to remain within tolerance limits. Since digital circuits are of primary interest in this paper, preventive maintenance shall be associated with the repair of redundant equipment. If all the "spare" redundant units are out of service for repair, the next failure will cause a system failure: if scheduled maintenance can be successfully performed on one or more of the failed spare units, then the next failure will not cause a system failure.

Preventive maintenance is not normally allowed in the TACC Auto System. Quite conceivably, "lulls" can be expected even in crisis situations. During the lulls, portions of the system could be "downed" to allow repair by the use of off-line diagnostics. Since lulls cannot be predicted beforehand, the user has been reluctant to accept an operational concept that would allow downtime for repair of redundant units. Whether official or not, such a concept would be beneficial in a real-life situation.

Table 3 (5:150) shows how a "one-out-of two" redundant system can improve it's effective MTBF if maintenance can be periodically scheduled to repair an offline unit before the on-line unit fails. "T" is the time between scheduled maintenance actions, and $MTBF_1$ is the MTBF of a single unit.

Table 3. REDUNDANCY WITH SCHEDULED MAINTENANCE

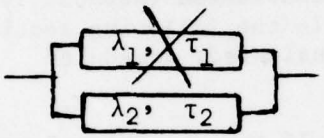
$T/MTBF_1$	$MTBF_1$ IMPROVEMENT FACTOR
0.1	10.97
0.5	3.04
1.0	2.08
1.5	1.79
∞	1.50

$$MTBF = \frac{\int_0^T R(t)dt}{1 - R(T)}$$

where:

$$R(t) = 1 - (1 - e^{-\lambda_1 t})^2$$

b. On-Line Repair. Consider the following redundant system:



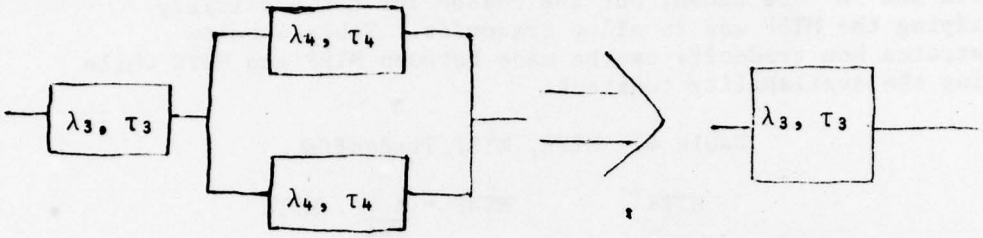
Assume that one of the units has failed, but that the system has been designed so that the surviving unit can continue to operate and perform the mission function while the failed unit is being repaired or replaced. In particular, assume that the first unit has failed, and that the Mean Time To Repair (MTTR) or replace this unit is time τ_1. With the second unit operating during the τ_1 repair/replacement action, the parallel system could only fail if the second unit also fails during the τ_1 time period that the first unit is being repaired/replaced.

Intuitively, the probability of mission failure for the parallel system should be small if the repair times are much less than the MTBF values. If, for example, the time between failures is $MTBF_1 = \frac{1}{\lambda_1} = 999$ hours, and the repair time is $MTTR_1 = \tau_1 = 1$ hour, then in any 1000 hour period, the probability that the first unit is out of service is:

$$\frac{MTTR_1}{MTTR_1 + MTBF_1} \qquad \frac{1 \text{ hour}}{1 \text{ hour} + 999 \text{ hours}} = 0.001$$

For system failure, both units would have to fail and the probability for the system failure would be a product of the individual out-of-service probabilities. If the second unit is identical to the first unit, then for the values cited previously, the probability for system failure would be $(0.001)^2$, or 0.000001.

The above result suggest that with "reasonable" ratios of MTBF and MTTR values, a useful approximation for the system model is to simply ignore redundant units if an on-line repair capability exists. This statement implies the following type of RMA model equivalencies:



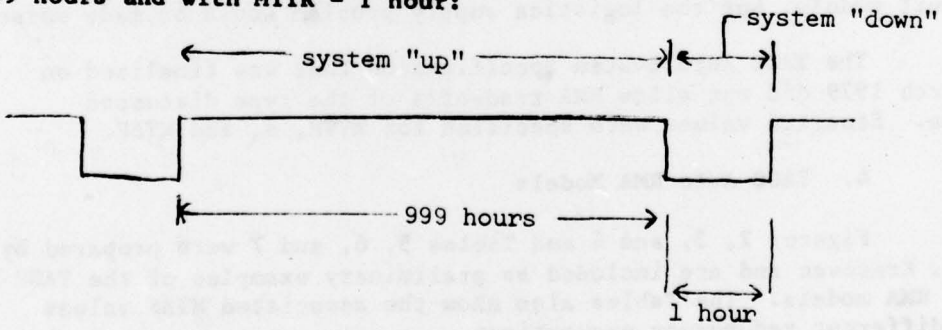
Assuming $MTTR_4 << MTBF_4$, and on-line repair

3. Availability

In the TACC Auto System Specification, the following definition is given for the Availability (A):

$$A \triangleq \frac{MTBF}{MTBF + MTTR}$$

As defined in TACC Auto, MTBF and MTTR have a zero contribution in the above equation from redundant equipment units if the redundant units have an on-line repair capability. A graphical example of the Availability definition in terms of mean times is offered below for MTBF = 999 hours and with MTTR = 1 hour:



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

$$= \frac{999}{999 + 1} = 0.999$$

The graph shows that the system is "up" 99.9% of the time.

An earlier draft of the TACC Auto System Specification included values for MTTR and "A", but did not include a value for MTBF. An MTBF value can of course be calculated from the Availability formula if MTTR and "A" are known, but the reason for not explicitly specifying the MTBF was to allow tradeoffs. Table 4 below illustrates how tradeoffs can be made between MTBF and MTTR while holding the Availability constant.

Table 4. MTTR, MTBF Tradeoffs

Availability (A)	MTTR (Hours)	MTBF = $\frac{A}{1-A}$. MTTR (Hours)
0.9990	0.6	599.4
0.9990	0.5	499.5

Referring to the first line of Table 4, assume the specified values are for an Availability of 0.9990, and an MTTR of 0.6 hours or less. For these values the "target" value for MTBF can calculated to be 599.4 hours. However, if this MTBF is difficult to attain, the second line of Table 4 shows that by improving the MTTR to 0.5 hour, the specification can still be met, even if the MTBF is as low as 499.5 hours.

If carried to extremes, the above types of tradeoffs could lead to the need for frequent maintenance actions due to low MTBF. Also, extreme improvements of MTTR might be achieved by swapping out whole subsystems. Swapping out whole substems would be faster than performing detailed diagnostics and taking the unit apart and putting it back together again in order to replace the one faulty circuit module, but the logistics supply problem would be made worse.

The TACC Auto System Specification that was finalized on 6 March 1979 did not allow RMA tradeoffs of the type discussed above. Separate values were specified for MTTR, A, and MTBF.

4. TACC Auto RMA Models

Figures 2, 3, and 4 and Tables 5, 6, and 7 were prepared by R. F. Krasovec and are included as preliminary examples of the TACC Auto RMA models. The Tables also show the associated MTBF values for different redundancy assumptions.

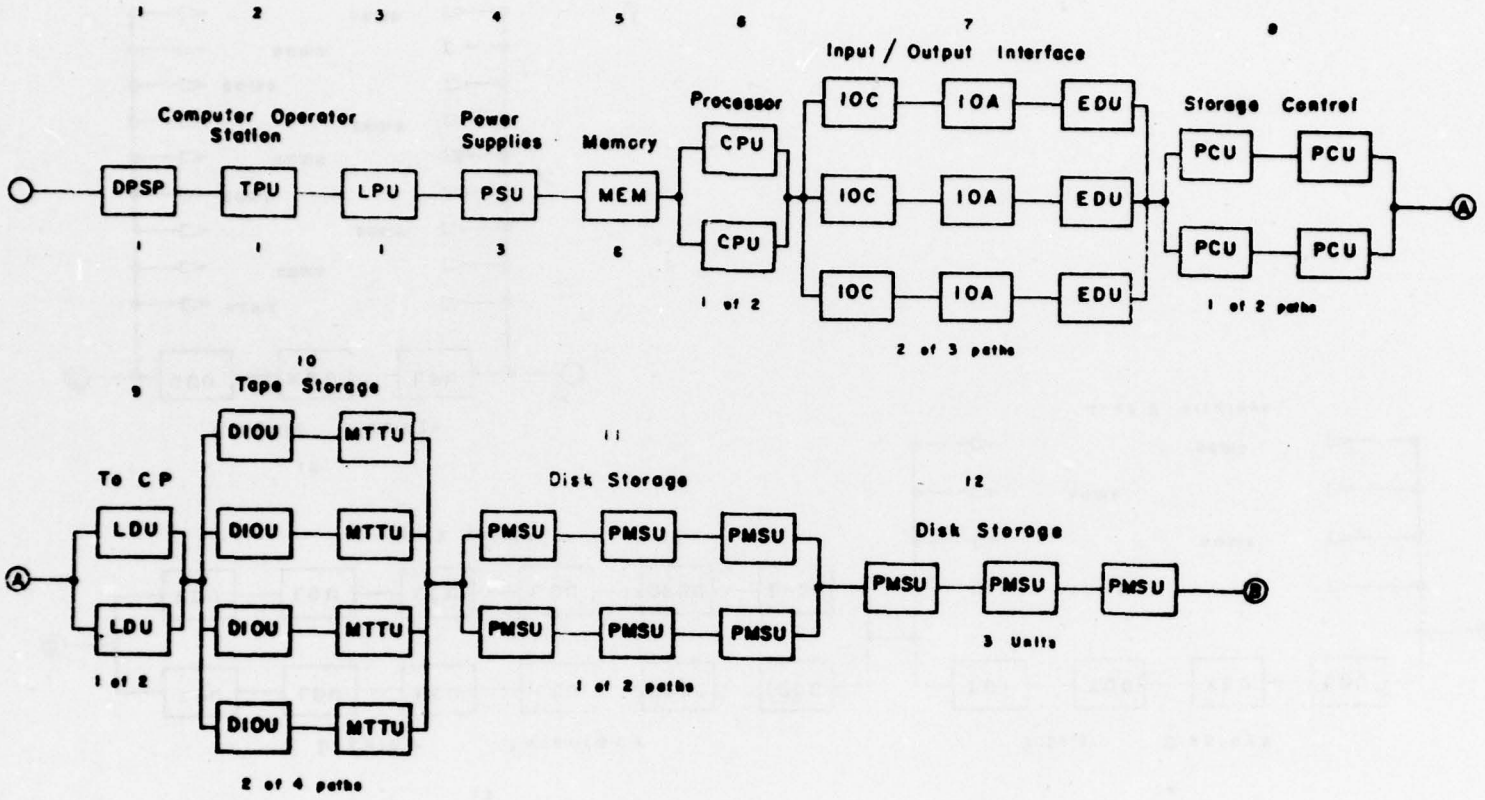


Figure 2 DP & D Equipment Reliability Model (sheet 1)

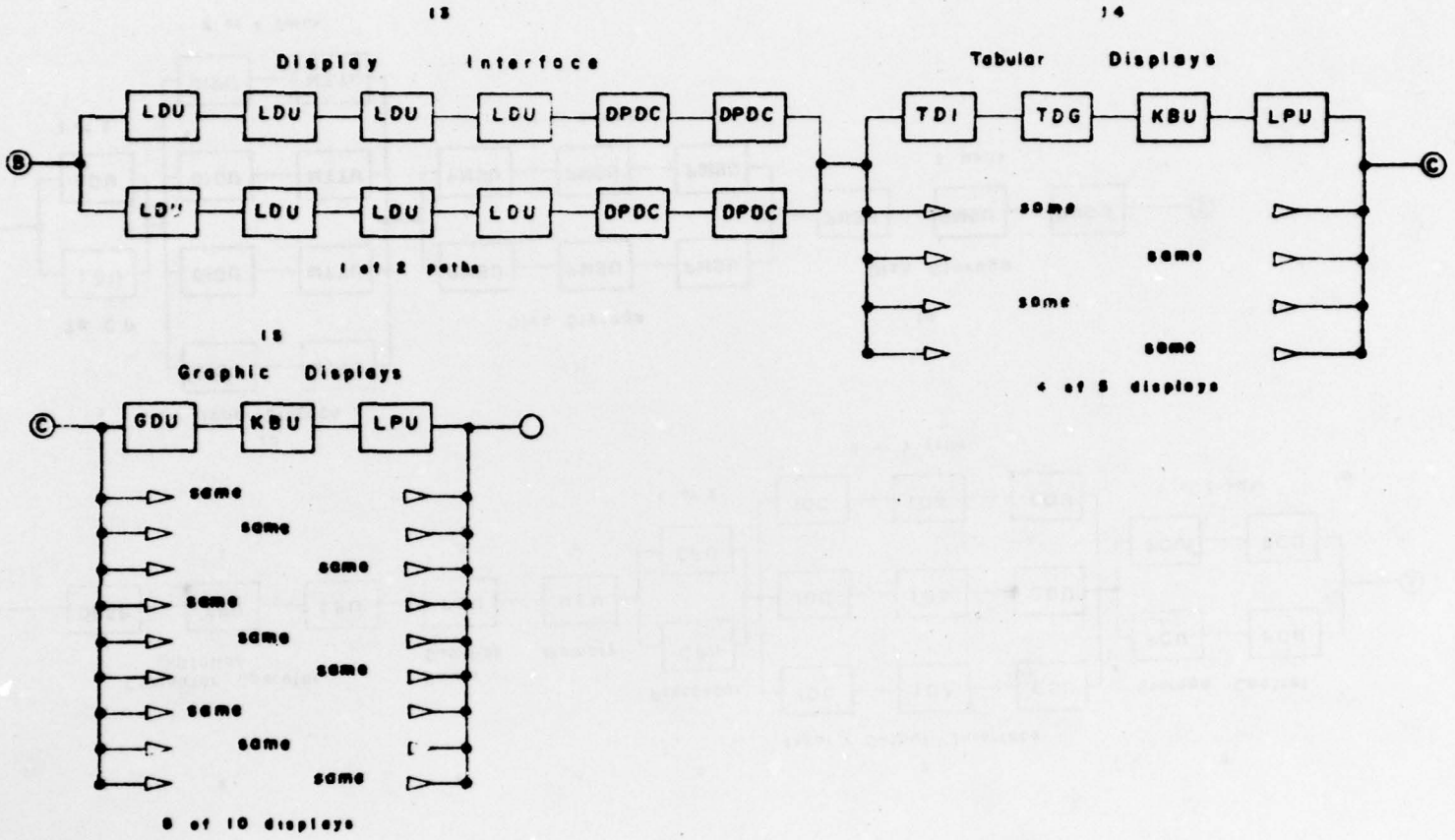


Figure 2 DP & D Equipment Reliability Model (sheet 2)

Table 5

DP&D Reliability Predictions

Group and Devices	Case 1 (All Devices)			Case 2 (Minimum Conf.)			Case 3 (Redundant)			Case 4 (On-Line Repair)		
	No.	FR	PC	No.	FR	PC	No.	FR	PC	No.	FR	PC
1 DPSP	1	76.2	0.4	1	76.2	0.5	1	76.2	0.9	1	76.2	2.7
2 TPU	1	290.7	1.4	1	290.7	1.9	1	290.7	3.3	1	290.7	10.4
3 LPU	1	159.8	0.7	1	159.8	1.1	1	159.8	1.8	1	159.8	5.7
4 PSU (3)	1	351.3	1.7	1	351.3	2.3	1	351.3	3.9	1	351.8	12.5
5 Memory (8)	1	780.8	3.7	1	780.8	5.2	1	780.8	8.8	1	780.8	27.8
6 CPU	2	528.8	2.5	1	264.4	1.8	1/2	176.3	2.0	1/2	0.0	0.0
7 IOC, IOA, EDU	3	688.5	3.3	2	459.0	3.1	2/3	275.4	3.1	2/3	0.0	0.0
8 PCU (2)	2	2463.2	11.7	1	1231.6	8.2	1/2	821.1	9.2	1/2	0.0	0.0
9 LDU (CP)	2	78.0	0.4	1	39.0	0.3	1/2	26.0	0.3	1/2	0.0	0.0
10 DIOU, MTTU	4	1154.4	5.5	2	577.2	3.8	2/4	266.4	3.0	2/4	0.0	0.0
11 PMSU (3)	2	2296.2	10.9	1	1148.1	7.6	1/2	765.4	8.6	1/2	0.0	0.0
12 PMSU (3)	1	1148.1	5.4	1	1148.1	7.6	1	1148.1	12.9	1	1148.1	40.9
13 LDU (4), DPDC (2)	2	1026.4	4.9	1	513.2	3.4	1/2	342.2	3.8	1/2	0.0	0.0
14 TDI, TDG, KBU, LPU	5	2986.0	14.2	4	2388.8	15.9	4/5	1327.0	14.9	4/5	0.0	0.0
15 GDU, KBU, LPU	10	7020.0	33.4	8	5616.0	37.3	8/10	2088.4	23.5	8/10	0.0	0.0
TOTAL FAILURE RATE		21048.4			15044.2			8895.1			2806.9	
MTBF (hrs.)		48			66			112			356	

Headings: No. - Number of required paths in each Group.
FR - Effective Failure Rate of each Group in failures per million hours.
PC - Percent contribution of Group Failure Rate to Total Failure Rate.

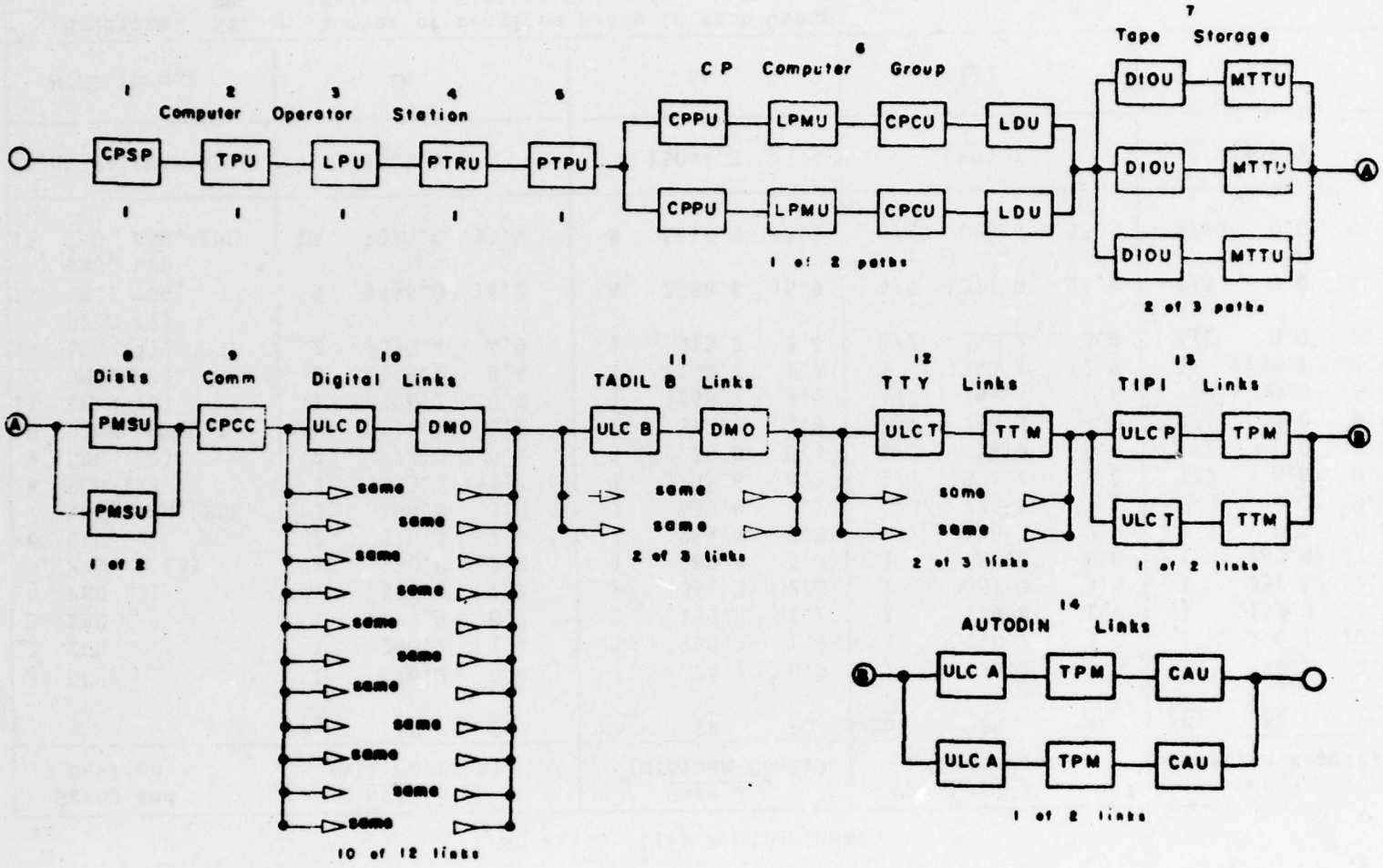


Figure 3 CP Equipment Reliability Model

Table 6

CP Reliability Predictions

Group and Devices	Case 1 (All Devices)			Case 2 (Minimum Conf.)			Case 3 (Redundant)			Case 4 (On-Line Repair)		
	No.	FR	PC	No.	FR	PC	No.	FR	PC	No.	FR	PC
1 CPSP	1	81.2	0.7	1	81.2	1.0	1	81.2	1.6	1	81.2	7.3
2 TPU	1	290.7	2.3	1	290.7	3.5	1	290.7	5.8	1	290.7	26.0
3 LPU	1	159.8	1.3	1	159.8	1.9	1	159.8	3.2	1	159.8	14.3
4 PTRU	1	74.1	0.6	1	74.1	0.9	1	74.1	1.5	1	74.1	6.6
5 PTPU	1	378.8	3.0	1	378.8	4.5	1	378.8	7.6	1	378.8	33.9
6 CPPU, LPMU, CPCU, LDU	2	2925.0	23.4	1	1462.5	17.5	1/2	975.0	19.6	1/2	0.0	0.0
7 DIOU, MTTU	3	865.8	6.9	2	577.2	6.9	2/3	346.3	7.0	2/3	0.0	0.0
8 PMSU	2	765.4	6.1	1	382.7	4.6	1/2	255.1	5.1	1/2	0.0	0.0
9 CPCC	1	133.7	1.1	1	133.7	1.6	1	133.7	2.7	1	133.7	12.0
10 ULC-D, DMO	12	3416.4	27.4	10	2847.0	34.1	10/12	1038.0	20.9	10/12	0.0	0.0
11 ULC-B, DMO	3	854.1	6.8	2	569.4	6.8	2/3	341.6	6.9	2/3	0.0	0.0
12 ULC-T, TTM	3	763.5	6.1	2	509.0	6.1	2/3	305.4	6.1	2/3	0.0	0.0
13 ULC-P, TPM, ULC-T, TTM	2	517.4	4.1	1	254.5	3.0	1/2	172.4	3.5	1/2	0.0	0.0
14 ULC-A, TPM, CAU	2	1252.6	10.0	1	626.3	7.5	1/2	417.6	8.4	1/2	0.0	0.0
TOTAL FAILURE RATE		12478.5			8346.9			4969.7			1118.3	
MTBF (hrs.)		80			120			201			894	

Headings: No. - Number of required paths in each Group.
FR - Effective Failure Rate of each Group in failures per million hours.
PC - Percent contribution of Group Failure Rate to Total Failure Rate.

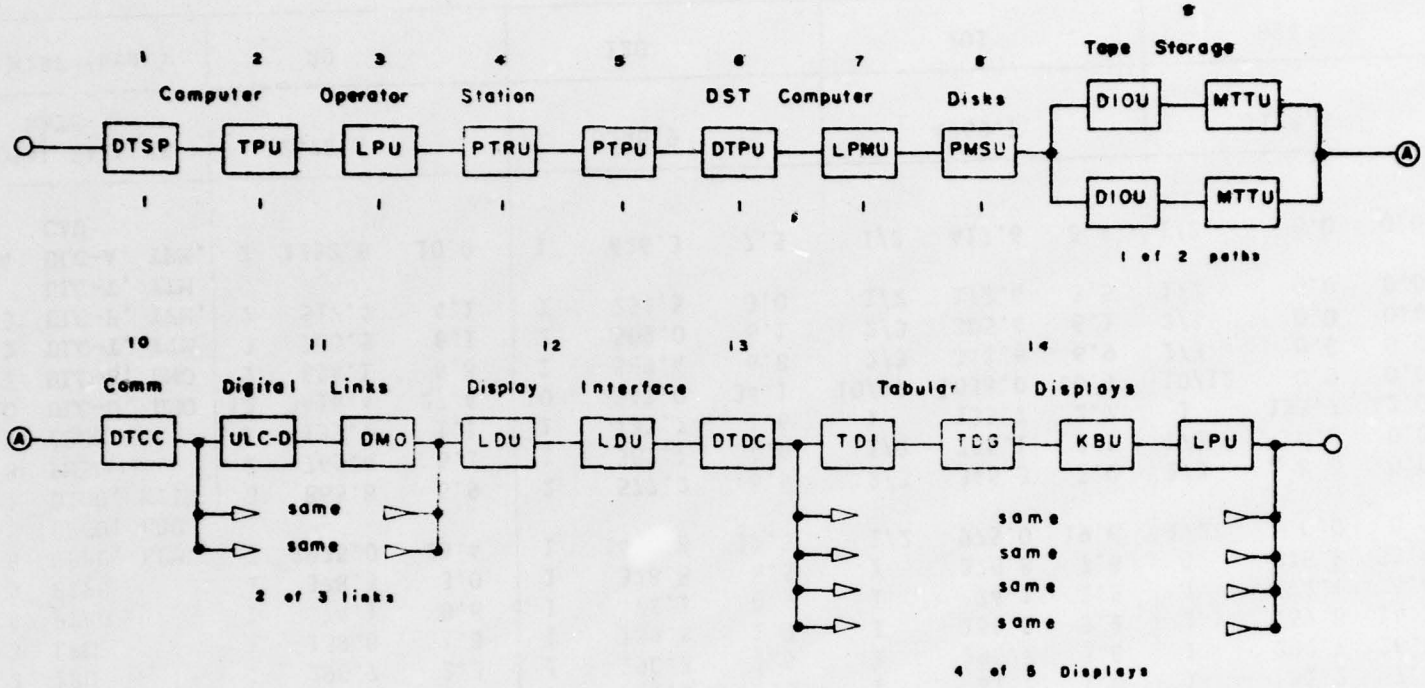


Figure 4 MDC (DST) Equipment Reliability Model

Table 7

MDC Reliability Predictions

Group and Device	Case 1 (All Devices)			Case 2 (Minimum Conf.)			Case 3 (Redundant)			Case 4 (On-Line Repair)		
	No.	FR	PC	No.	FR	PC	No.	FR	PC	No.	FR	PC
1 DTSP	1	73.2	1.0	1	73.2	1.0	1	73.2	1.6	1	73.2	2.7
2 TPU	1	290.7	4.1	1	290.7	4.8	1	290.7	6.3	1	290.7	10.6
3 LPU	1	159.8	2.2	1	159.8	2.7	1	159.8	3.5	1	159.8	5.8
4 PTRU	1	74.1	1.0	1	74.1	1.2	1	74.1	1.6	1	74.1	2.7
5 PTPU	1	378.8	5.3	1	378.8	6.3	1	378.8	8.2	1	378.8	13.8
6 DTPU	1	481.0	6.7	1	481.0	8.0	1	481.0	10.4	1	481.0	17.5
7 LPMU	1	619.6	8.6	1	619.6	10.3	1	619.6	13.4	1	619.6	22.6
8 PMSU	1	382.7	5.3	1	382.7	6.4	1	382.7	8.3	1	382.7	13.9
9 DIOU, MTTU	2	577.2	8.1	1	288.6	4.8	1/2	192.4	4.2	1/2	0.0	0.0
10 DTCC	1	66.9	0.9	1	66.9	1.1	1	66.9	1.5	1	66.9	2.4
11 ULC-D, DMO	3	854.1	11.9	2	569.4	9.5	2/3	341.6	7.4	2/3	0.0	0.0
12 LDU (2)	1	78.0	1.1	1	78.0	1.3	1	78.0	1.7	1	78.0	2.8
13 DTDC	1	142.3	2.0	1	142.3	2.4	1	142.3	3.1	1	142.3	5.2
14 TDI, TDG, KBU, LPU	5	2986.0	41.7	4	2388.8	39.9	4/5	1327.0	28.8	4/5	0.0	0.0
TOTAL FAILURE RATE		7164.4			5993.9			4608.1			2747.1	
MTBF (hrs.)		140			167			217			364	

Headings: No. - Number of required paths in each Group.
FR - Effective Failure Rate of each Group in failures per million hours.
PC - Percent contribution of Group Failure Rate to Total Failure Rate.

B. TACC AUTO RMA COMPLEXITIES

The following quotes (6:F-1) suggest the complexity of RMA problems:

> In a nutshell, the laboratory definition of failure is not compatible with the field definition. (Frank S. Stovall, Is MIL-STD-781B a Good Reliability Test Specification)
>
> A fault is a fault. A fault is not always a failure. (Carsten Boe, 1974 Reliability and Maintainability Symposium)
>
> Logistic burdens are expressible in terms of subunit failures even when such failures do not cause immediate system malfunction. (Everett L. Welker, The Basic Concepts of Reliability Measurement and Prediction)
>
> There must be an awareness that we can no longer consider system reliability as a purely statistical concern. It must be considered in the field operational context. (Jacques S. Gansler, Deputy Assistant Secretary of Defense, Materiel Acquisition, OASD (I&L)
>
> A designer may make reliability his initial consideration and then look for alternate approaches to achieving performance. (General Samuel C. Phillips, USAF (Retired))
>
> Holiday's Principles of Unreliability:
>
> a. MTBF is directly proportional to top management's attitude and support.
>
> c. Large portions of "reliability" dollars are invested in convincing the "power structure" to take corrective action on activities and failure modes ..... already well understood by the design and reliability specialist.
>
> h. Reliability specialist tend to communicate among themselves and not escalate problems for management attention and action.
>
> j. Human attention on daily problems and short term survival, clouds long term MTBF solutions.

Individual understandings of RMA may be hindered by the fact that certain aspects of RMA may appear to be rather intuitive. However, a lack of understanding of RMA complexities is not necessarily caused by the unavailability of information (6:v):

> Despite, however, the information available on the subject and the importance ascribed to reliability, there exists no single document to which the Air Force program director and staff can turn for guidance. Instead, they find a great number of Air Force/DOD reliability documents which have no common link tying them together. The result is that only those individuals already trained and skilled in reliability engineering are left to develop a reliability program for a given weapon system. Of course, the other functional managers within a program office affected by reliability (practically all of them!) can dig through the countless specifications, standards, regulations, and policy to attain a respectable understanding of reliability; and indeed many of them do just that. But this approach requires considerable time, a commodity in very short supply.

1. Basic RMA Definitions

One approach to complexity is to attempt to educate everyone to the required level of understanding. However, the new AFR 80-5 seems to admit the complexity of the RMA problem by mandating a completely different approach: people must use different definitions and terms, depending on the particular audience. Three separate sets of terms are required (7:2):

a. Program Decision Terms. Only these RMA terms are to be used in the presence of high-level decision makers. The terms should be used in Decision Coordinating Papers, Statements of Operational Need documents, and for Defense System Acquisition Review Councils. For these audiences, "Uptime Ratio" and "Mean Time Between Critical Failures (MTBCF)" must be used, instead of the equivalent "Availability" and "MTBF" terms that have been used in the TACC Auto Program. As a matter of interest, the concept of "MTTR" is non-existent in Program Decision Terms.

b. Program Management Terms. These terms include all of the Program Management Terms, plus others. The uses of these terms include operational and maintenance concepts, Program Management Directives, Program Management Plans, and test and evaluation

programs. These terms are also to be used in communications between the implementing, supporting, and using commands. The term "Mean Time Between Maintenance (MTBMa) is to be used: this term corresponds to "MTBF" as defined by MIL-STD-781C (but not as defined in TACC Auto).

c. Contract Terms. These terms may be defined by the implementing command for use with contractors, but the terms are not to be used between Air Force major commands, or with the Department of Defense. The term "MTBF" is to be used exclusively as a Contract Term. Audit trails must be established to relate Contract Terms to Program Management Terms. In the TACC Auto Program, the System Specification terms of MTBF, MTTR, and A have been identical to the contract terms.

A report on avionics reliability made the following comments on RMA definitional differences (8:10):

> The definitional differences observed are inherent to the differences in the failure criteria and time base used by the two communities, the AFLC which collects and analyzes the data, and the engineering community (AFSC and Industry) which establishes requirements, performs predictions, and conducts reliability demonstration tests.
> .....
> The review of the failure relevancy criteria revealed that there are two related, but differing, reliability characteristics responsible for the differences in failure classification criteria. These are the inherent reliability (engineering oriented), and the operational reliability (logistics support/operations oriented). Until these differences are clearly recognized and understood, confusion as to the meaning of MTBF will continue to exist.

Failure relevancy criteria problems have occured in the TACC Auto Program between the supporting and implementing commands. The problems may have been made worse by definitional differences. The TACC Auto System Specification modifies the MIL-STD-781C definition of a failure. Section 4.2.1.1.7.2.1 of the SS-001485D System Specification (9) specifically excludes malfunctions of redundant items from determinations of MTBF and MTTR, whereas MIL-STD-781C states that all failures that can be expected to occur in field service should be used to compute demonstrated MTBF (10:3).

The System Specification exclusion applies when the redundant item malfunction does not cause the overall performance to be interrupted or degraded below the specified required level.

2. System Definition Deficiencies

There are no overall system RMA requirements in TACC Auto: the RMA requirements are specified only in terms of the four major subsystems. The RMA specification apparently only applies to the hardware, and not to the software computer programs that of course are also essential to system operation. The only guidance on software errors in regards to RMA seems to be Paragraph 3.1.5.9 of MIL-STD-781C (10). This paragraph states that software errors will be chargable as equipment failures, but not if the errors are corrected and verified during the test. Typically, the "test" referred to is a diagnostic program for exercising the hardware: therefore, software errors in operational computer programs apparently do not affect RMA test demonstrations.

An argument could be made that operational software is part of the system, and therefore the System Specification RMA values should include the effects of software errors. This would present an allocation problem, since in TACC Auto the hardware contractor has no responsibility or control over the operational-software development being implemented by the using command.

Another area that the hardware contractor does not have control over is the crypto equipment that has been furnished by the Government. Apparently the cryptos are excluded from RMA calculations, although crypto failures would certainly affect the system operation.

The relationship of degraded mode operation to system failures for purposes of RMA calculations has not been explicitly defined for the present TACC Auto hardware configuration. For example, if one of the 15 displays is out of service, should the system be considered as "failed" for RMA calculation purposes, even though the mission would no doubt be continued? Similar questions can be asked about other equipment items such as magnetic disks and tapes, core memory modules, and alternate communication channels. Answers to such questions were sought as part of an RMA Conference (11).

3. RMA Predictions

Another complexity of RMA is that different RMA predictions can be made for the same points in time. If the type of prediction and the underlying assumptions are not explicitly stated, confusion can result. The different types of predictions include (6:36):

a. Analytical Predictions. These are based on part counts, complexity, historical data, and probability distributions.

b. Predictions Based on Number of Failure to Date. These assessments may be biased by the higher failure rates that typically occur at the beginning of a program.

c. Current-Extrapolation Predictions. These predictions are based on current failure rates and previous failures are ignored if design corrections have been made.

d. Predictions Based on Growth Curves. RMA can be enhanced by making design changes as failure modes are discovered during the design and development phases. Based on empirical historical data from various programs, formulas are available for predicting how RMA will increase as a function of time.

After the system has matured and stabilized, the predictions described above should yield similar results. However, during initial tests, the different predictions may vary greatly. One study of data collection efforts showed that the initial reliability of fielded equipment and systems is degraded from three to ten times the potential predicted during design (1:10).

The report on avionics reliability referenced earlier classified predictions in the following categories (8:1): 1) required 2) predicted, 3) demonstrated, and 4) field operational. The ratio of demonstrated MTBF to field MTBF was reported as ranging from 7:1 to 20:1. Even greated disparities were noted for the comparison of predicted MTBFs to field MTBFs. (This report also determined that differences between the field MTBF and the demonstrated or predicted MTBFs were due almost equally to the two factor of maintenance handling and operational use.)

If large magnitudes of RMA degradation are initially observed, as referenced above, significant concern can be expected. However, as stated in AFR 80-5, RMA terms are properly expressed in terms of mature system values. AFR 80-5 also states that for RMA purposes, a system is arbitrarily defined to be mature two years after the initial operational capability.

C. RMA EHNANCEMENTS

As is evident from the preceding sections, RMA can change with time, and a given RMA level is not necessarily achieved at the beginning of the life of a product. Screening and burn-in tests are methods that are sometimes thought to enhance RMA. In these tests, variation of physical, chemical, or electrical properties beyond some criteria make a part suspect for early or infant failure, and is a basis for rejecting the part. Screening and burn-in tests do not actually enhance the RMA of the product, but instead are a method to pick only the production items that meet our needs.

RMA enhancements, for the sake of emphasis, can be separated into RMA growth and RMA improvement (6:36). RMA growth results from design and material changes to correct failures detected during the design and development phases. Ideally, RMA growth should result in the attainment of the System Specification values. On the other hand, RMA improvement is an effort to make the RMA values better than the values that were originally specified. The following paragraphs will discuss TACC Auto efforts in both of these areas.

1. RMA Growth

The TACC Auto hardware has undergone several years of extensive use and testing since the beginning of the contract in 1972. Included were the Phase A and B developmental and initial operational test and evaluation programs. As a result of these activities, Deficiency Reports (DRs) have been initiated for many hardware problems. These problems were forwarded for action to a Deficiency Review Board (DRB) or a Production Configuration Working Group (PCWG). Many fixes were made, or were planned for the production hardware. High failure rate items were redesigned or replaced, and the production system promised to have much better RMA than had been experienced during development.

The development of microprocessor Programmable Read Only Memory (PROM) standalone fault isolation diagnostic programs for the production configuration could be considered as another area of RMA growth. These programs would allow on-line repair of equipment such as the graphical and tabular display units, and the Universal Line Controller portions of the communications equipment.

Support requirements such as provisions for adequate maintenance personnel training, provisions for detailed maintenance procedure documentation, enhanced system-level diagnostics,

additional support equipment, and adequate availability of spares have been lacking during the program development. The initial operational capability plus two years attainment of these support requirements could also be considered a part of the RMA growth.

2. RMA Improvement

As was mentioned previously, the deletion of the requirement for on-line diagnostics from the TACC Auto System Specification directly implied a change in RMA values that the user was reluctant to accept. Restoral of the on-line diagnostic capability would have required more funds and time than were available. During the last several months, efforts have been made to find RMA improvements that would result in RMA values that would approach the original specification values. The hardware area was not considered to have significant potential for RMA improvement beyond the RMA growth that would have resulted from the actions listed in the previous paragraphs, and high reliability components were already being used. The real payoff area seemed to be to make better use of the hardware redundancy (11).

The use of the existing redundant hardware would have required the creation of new software computer programs or perhaps the modification of existing computer programs. The computer programs would have had to be able to do some or all of the following functions, depending on the particular unit in question:

a. Detect faults,

b. Switch the system to the redundant/spare units, either automatically, or semi-automatically,

c. Update memory of redundant/spare units, either in real-time, or periodically, in order to allow graceful switching, and

d. Allow system operation while also allowing certain existing "off-line" diagnostic programs to "on-line" diagnose selected equipment items.

The above software-oriented approach for RMA improvement did not gain support from either the logistics support or the using command. The approach did not improve the supporting command situation since failures require logistics support, regardless of whether or not the operational mission is able to continue. Perhaps the main reason for the using command's reluctance to accept the software-oriented approach was due to the using command's role as the software development agency: the using command would have had to supply manpower for developing the software to make use of the redundant hardware units.

SECTION IV

SUMMARY

This paper has presented information that will be useful for future efforts in specifying Reliability, Maintainability, and Availability (RMA) values for the TACC Automation Program. Three main areas were addressed:

a. RMA background and principles. The information presented on RMA model theory pertained to TACC Auto, but the information is also relevant for many other systems as well. This paper presents, in a useable form, basic reliability mathematic derivations and simple formulas for calculating MTBF for various redundant configurations: this type of information requires a lot of effort to collect the information from the many sources. Also, much of the literature concentrates on probabilities rather than MTBFs. The literature also shows a reluctance to consider series-parallel RMA models, and the approximations involved. An engineering-oriented reader of this paper should be able to attain a fair amount of confidence in dealing with RMA problems, without the need of extensive additional training.

b. TACC Auto RMA complexities. This section presented information on the new Air Force Regulation AFR 80-5 that specifies how different RMA terms must be used for different audiences. Complexities and confusions unique to TACC Auto were presented concerning basic RMA definitions, system definition deficiencies, and the different RMA predictions that different groups can make and mis-communicate. The information presented in this section should be of special value to new personnel to the TACC Auto Program who have a need to be concerned about RMA.

c. RMA enhancements. This section discussed screening and burn-in, and emphasized the differences between RMA growth to attain specification values, and RMA improvement to go beyond the original design goals. The specific RMA enhancement planned for TACC Auto is presented: this information could be of use to other programs, as well as to future TACC Auto RMA efforts.

REFERENCES

1. Anderson, R. T. Reliability Design Handbook. RDH 376. Chicago: IIT Research Institute, 1976.

2. Meyer, P. L. Introductory Probability and Statistical Applications. Reading, MA: Addison-Wesly Publishing Company, 1970.

3. Krasovec, R. F. Class Notes from a Northeastern University Course on Reliability.

4. Polovko, A. M. Fundmentals of Reliability Theory. New York: Academic Press, 1968.

5. School of Systems and Logistics. Course Material for Reliability Course QMT372(AF). Wright-Patterson Air Force Base, OH.

6. Engineering and Support Division, Directorate of Maintenance, Engineering and Supply, Deputy Chief of Staff, Systems and Logistics, United States Air Force. An Introduction to Reliability. July, 1978.

7. AFR 80-5. Air Force Reliability and Maintainability Program. 9 August 1978.

8. Baker, R. L. and G. A. Kern. "Operational Influences on Avionics Reliability," The Journal of Environmental Sciences, September/October 1976.

9. SS-001485D, System Specification for the Tactical Air Control Center (TACC), 6 March 1979.

10. MIL-STD-781C, Reliability Design Qualification and Production Acceptance Tests: Exponential Distribution, 25 October 1977.

11. ESD/DCYO Letter. "Minutes of TACC Automation Reliability/Maintainability/Availability (R/M/A) Conference, 23-25 January 1979," 5 February 1979.