29p

N63-10536

CODE 1

NASA TN D-1558

NASA TN D-1558

TECHNICAL NOTE

A RELIABILITY MODEL AND ANALYSIS FOR PROJECT MERCURY -- 3-ORBIT MANNED AND UNMANNED MISSION

By William Wolman and Fred Okano

National Aeronautics and Space Administration
Office of Manned Space Flight

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON December 1962

A RELIABILITY MODEL AND ANALYSIS FOR PROJECT MERCURY -- 3-ORBIT MANNED AND UNMANNED MISSION

by

William Wolman

and

Fred Okano

National Aeronautics and Space Administration
Office of Manned Space Flight

SUMMARY

Based on test data of parts, components, and subsystems, the probability of successfully completing the mission and the probability of flight safety were desired for the Project Mercury 3-orbit mission. The purpose of this Technical Note is to give the development of a mathematical model, data requirements, and other assumptions used in the Mercury reliability evaluation. Although the model was developed for the evaluation of the Mercury mission, the approach is general and can be modified for other space system applications.

FOREWORD

The purpose of this Technical Note is to give in some detail the development of a mathematical model, data requirements, and other assumptions necessary for a reliability evaluation of the Project Mercury 3-orbit mission. It should be realized that the numerical results of a study of this type should be viewed and interpreted carefully and only within the context of the validity of the model and the other assumptions which have to be made.

It is only to the degree that the analytical model is able to describe the operation of a complex system adequately and the extent to which it is possible to estimate the reliabilities of systems, subsystems, components and parts of an overall system that the results obtained will adequately estimate the reliability of a mission.

It should also be borne in mind that the estimates of reliability obtained from test data are subject to inherent sampling variation. By this, we mean that if a given subsystem were tested in exactly the same manner under the same conditions at a different time, different results might have been obtained purely by chance. Reliability estimates for different subsystems and components are only point estimates of the true unknown reliabilities. In order to obtain some measure of the variability of the estimate of reliability of an overall system, it is usually necessary to compute a confidence or prediction interval. In the Mercury study this has not been possible because the analytical model is too complex. It is hoped that this can be accomplished with the aid of electronic computing equipment using Monte Carlo techniques in future analyses. Hence, numerical outputs of the model described should not be considered as exact numbers, but rather as estimates of the general level of the true unknown reliability.

A question that can be rightfully raised is to what extent does flight test information prior to a complete flight mission contribute to knowledge about the reliability of the system. Such flight test information does contribute additional test time for the subsystems and in that manner provides additional reliability information. However, relative to the total operating time of a ground test program, this is usually negligible. One may view a successful flight test program in the following manner. It represents a "de-bugging" phase for a system and shows to what extent a test program prior to the flight test has been realistic in duplicating the flight environment and exposing embryonic design weaknesses. If a prior flight test program is unsuccessful in several instances, then reliability estimates that would be obtained using the model and approach as outlined in this report can never be accurate since the assumptions used imply that the system is not plagued by problems of embryonic design or quality control failures. In interpreting the reliability estimates in the manner developed in the report, it should be realized that the estimates are based on the actual test program results obtained for the subsystems and components of the overall system. It is therefore possible that the reliability of the system is actually higher, but this is unknown unless it is so demonstrated. It is in this latter sense that estimates of reliability obtained from the type of data inputs for the model described in this report can be called "demonstrated estimates" and are therefore not necessarily the upper bound for the actual unknown reliability for a flight mission.

The model and methods used are in many ways idealizations of true system operation and the approach taken, namely, estimating overall system reliability on the basis of information on subsystems, components and parts, has its shortcomings. However, there exists at present no other means of assessing the reliability of a highly complex system using a rational approach and a quantitative basis, than by using an approach, at least similar in concept, to that used for the Mercury analysis described in the following pages.

Although the model was developed for the evaluation of the Project Mercury 3-orbit mission, the approach is general and can be modified for other space system applications.

CONTENTS

Fig.

A RELIABILITY MODEL AND ANALYSIS FOR PROJECT MERCURY -- 3-ORBIT MANNED AND UNMANNED MISSION

by

William Wolman and Fred Okano

INTRODUCTION

The Mercury reliability study was initiated in June of 1960 by the National Aeronautics and Space Administration in Washington, D. C. Its purpose was to provide overall estimates of reliability for the Mercury capsule and booster system for both the unmanned and manned missions as defined below. In addition, it was desired to highlight the areas of unreliability that exist in the system.

This study was divided into two phases: the unmanned mission and the manned mission. The unmanned mission was considered to be that which would be required of the Mercury capsule with the assumption that no astronaut was aboard but that the life support systems were required to function. The manned mission, on the other hand, assumed that the astronaut was aboard the capsule and that he could function as required.

The normal mission is defined as a 3-orbit mission from capsule umbilical drop to touchdown, while flight safety is defined as the successful completion of the normal mission or of any of the aborts possible at various times of the normal mission. An abort is defined as the necessity, due to some failure, to terminate the normal mission and bring the capsule to earth prematurely.

In order to complete this study, a number of assumptions are necessary. These assumptions are:

1. The cut-off date for the system and test data, as used in this study, is July 1, 1960. Since that date, additional testing has been performed and there have been some changes in the design of the system as well as changes in the mission ground rules.

2. The system considered consists only of the capsule from the period of capsule umbilical drop to touchdown and the Atlas booster (including Abort

Sensing and Implementation System). The study goes up to time of touchdown and does not include any aspect of the recovery operation. For example, the equipment necessary in the capsule itself, such as d-c power, which may be required in locating the capsule by recovery forces, is assumed to have to function only up to time of touchdown.

3. No failures are due to:

   a. Capsule structure
   b. Abort Sensing and Implementation System
   c. Ground support systems.

4. All subsystems and equipments are functioning perfectly at time of umbilical drop. That is, effective check-out procedures have eliminated all malfunctions present in the system and, moreover, no failures occur between check-out and umbilical drop.

5. The test program for all subsystems and components duplicates the actual environmental stresses of the mission. It is known that the environmental stresses cannot be completely duplicated; however, it has been assumed that the reliability of the subsystems is that which has been demonstrated by the various test programs.

6. The mathematical and statistical models used truly describe the mission. These models are discussed further in the following section.

7. If all subsystems function as designed, then the normal mission and safety reliabilities will be one. Failures will occur only in the equipments which do not function as intended.

8. Quality control failures are not involved in malfunctions. This means that contractor receiving, assembly, and check-out inspections will effectively identify all areas of malfunction. The failures that have been included in estimating the subsystem reliabilities are those that could occur during the mission. A failure, for example, which would result from a diode put in backwards should be detected during some phase of inspection and would therefore not be included. Also, failures that may occur at random are included since they may or may not be identified during inspection (whether or not corrective action has later been taken).

9. In those instances where the estimates of subsystems reliability is based on very sparse data, the subsystem is assumed to have passed the

acceptance criteria. Examples of these are the Reaction Control System and the Cabin Air Temperature Indicator.

10. As opposed to hardware, which, once it has failed cannot be repaired, the astronaut, if unable to perform at one time, can recover and perform his required functions in succeeding time periods.

11. Aborts from orbit are initiated at the end of orbit. Unless a catastrophic failure occurs, such as rapid oxygen depletion, this will actually be the case in order to maximize the probability of recovery after touchdown.

12. Except for the d-c and a-c Power Supply Systems and the systems specifically noted, all major systems listed below, comprising the overall Mercury system, are considered to be functionally and stochastically independent of each other for purposes of this study.

a. Booster
b. d-c Power System
c. a-c Power System
d. Environmental Control System
e. Telemetry
f. Attitude Control and Stabilization System, including retrograde initiation and retro-rocket firing *
g. Communications System
h. Capsule Tracking System, including C and S Band Beacons and Command Receivers
i. Tower Ring Separation
j. Escape Rocket Firing
k. Capsule Ring Separation
l. Posigrade Rocket Firing
m. Periscope Extension
n. Retrograde Package Jettison
o. Periscope Retraction
p. Drogue Chute Deploy
q. Antenna Fairing Ejection
r. Main Chute Deploy
s. Landing Bag Extension.

13. Both the telemetry and the communications systems are required during the mission.

*Includes Communications, Telemetry, and Capsule Tracking Systems during retrograde initiation and retro-rocket firing.

14. The astronaut is not required to orient the capsule during orbit at night in case of ASCS failure. However, he is required to perform this maneuver in daylight, including retrograde maneuver.

The times of initiation and completion of the normal unmanned mission, as well as the eight aborts, are shown in Fig. 1. The times for the manned mission are identical except that the unmanned abort C (tower-separation circuit failure) does not exist for the manned mission since the crew override which initiates this abort is the same override required to continue the normal mission.

The "overall" reliability diagram is shown in Fig. 2. The overall diagram depicts the systems that must operate, in their relative sequence, in order for the mission to continue or for an abort to succeed. The systems have been given "link numbers" for identification purposes. For example, link 1 is the booster operating from capsule umbilical drop to 8-inch lift-off; link 2 is the booster from lift-off to escape tower jettison. The aborts have been identified by having upper case letters corresponding to the abort (A through G) follow the link number.

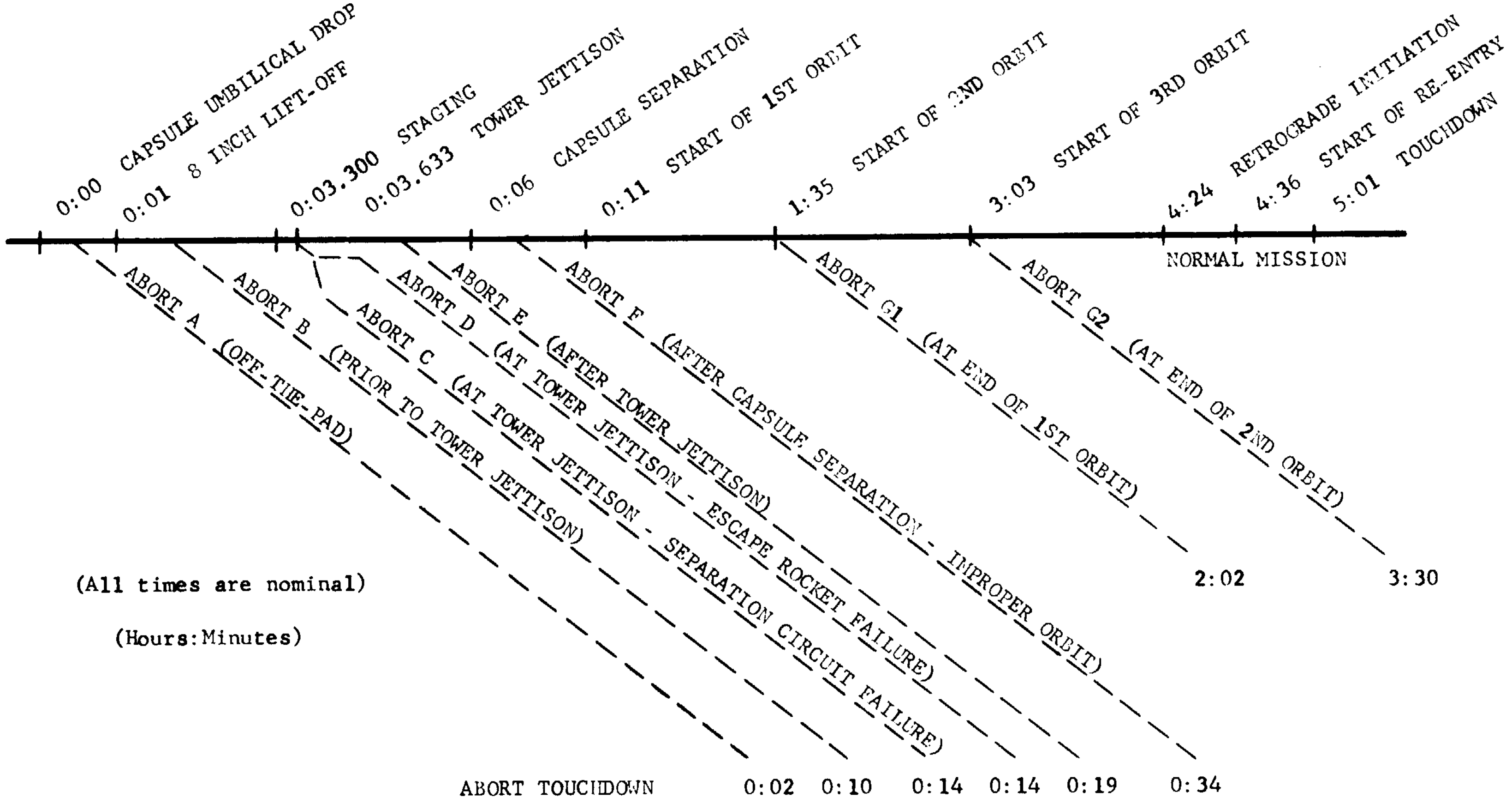
An example of the detail reliability diagram is shown in Fig. 3. Fig. 4 shows, in simplified form, the same system shown in Fig. 3. The various equipment identifications in Fig. 3 have been replaced by capital letters in order to facilitate mathematical computation of the system reliability. The mathematical representation of the system shown in Fig. 3 and 4 is given in Fig. 5. Figure 3-A is an abbreviated detailed diagram of a part of the Attitude Control System showing the crew inputs but from which all relays, switches, fuses, and other small parts have been omitted.

ESTIMATION MODELS

The probability models used in this study are as follows:

1. For continuous time operating devices it was assumed that the probability of a failure in time interval (0, h), assuming no failure at beginning of the interval, is given by

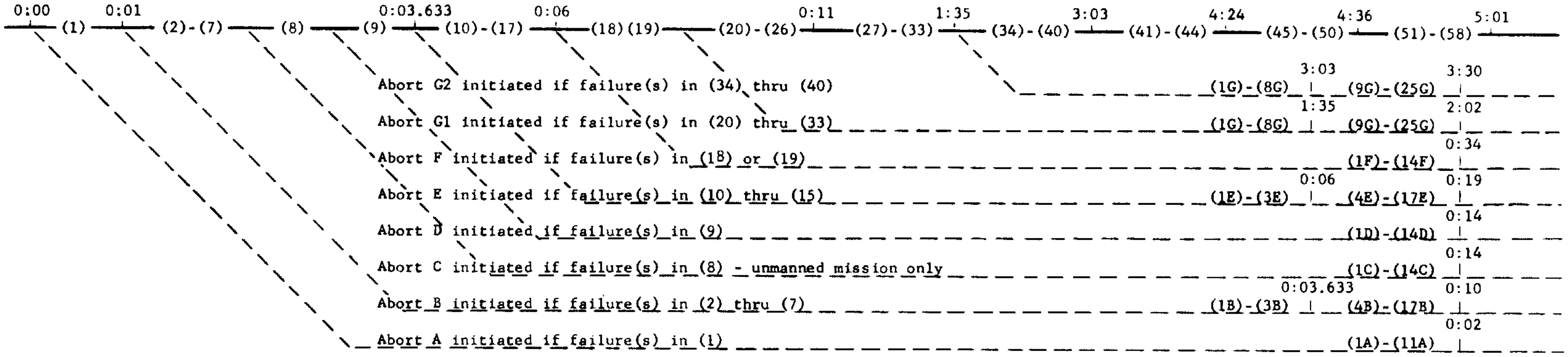
$$\lambda h + o(h)$$


0:00 CAPSULE UMBILICAL DROP
0:01 8 INCH LIFT-OFF
0:03.300 STAGING
0:03.633 TOWER JETTISON
0:06 CAPSULE SEPARATION
0:11 START OF 1ST ORBIT
1:35 START OF 2ND ORBIT
3:03 START OF 3RD ORBIT
4:24 RETROGRADE INITIATION
4:36 START OF RE-ENTRY
5:01 TOUCHDOWN
NORMAL MISSION
ABORT A (OFF-THE-PAD)
ABORT B (PRIOR TO TOWER JETTISON)
ABORT C (AT TOWER JETTISON - SEPARATION CIRCUIT FAILURE)
ABORT D (AT TOWER JETTISON - ESCAPE ROCKET FAILURE)
ABORT E (AFTER TOWER JETTISON)
ABORT F (AFTER CAPSULE SEPARATION - IMPROPER ORBIT)
ABORT G1 (AT END OF 1ST ORBIT)
ABORT G2 (AT END OF 2ND ORBIT)
2:02
3:30
ABORT TOUCHDOWN
0:02
0:10
0:14
0:14
0:19
0:34

(All times are nominal)

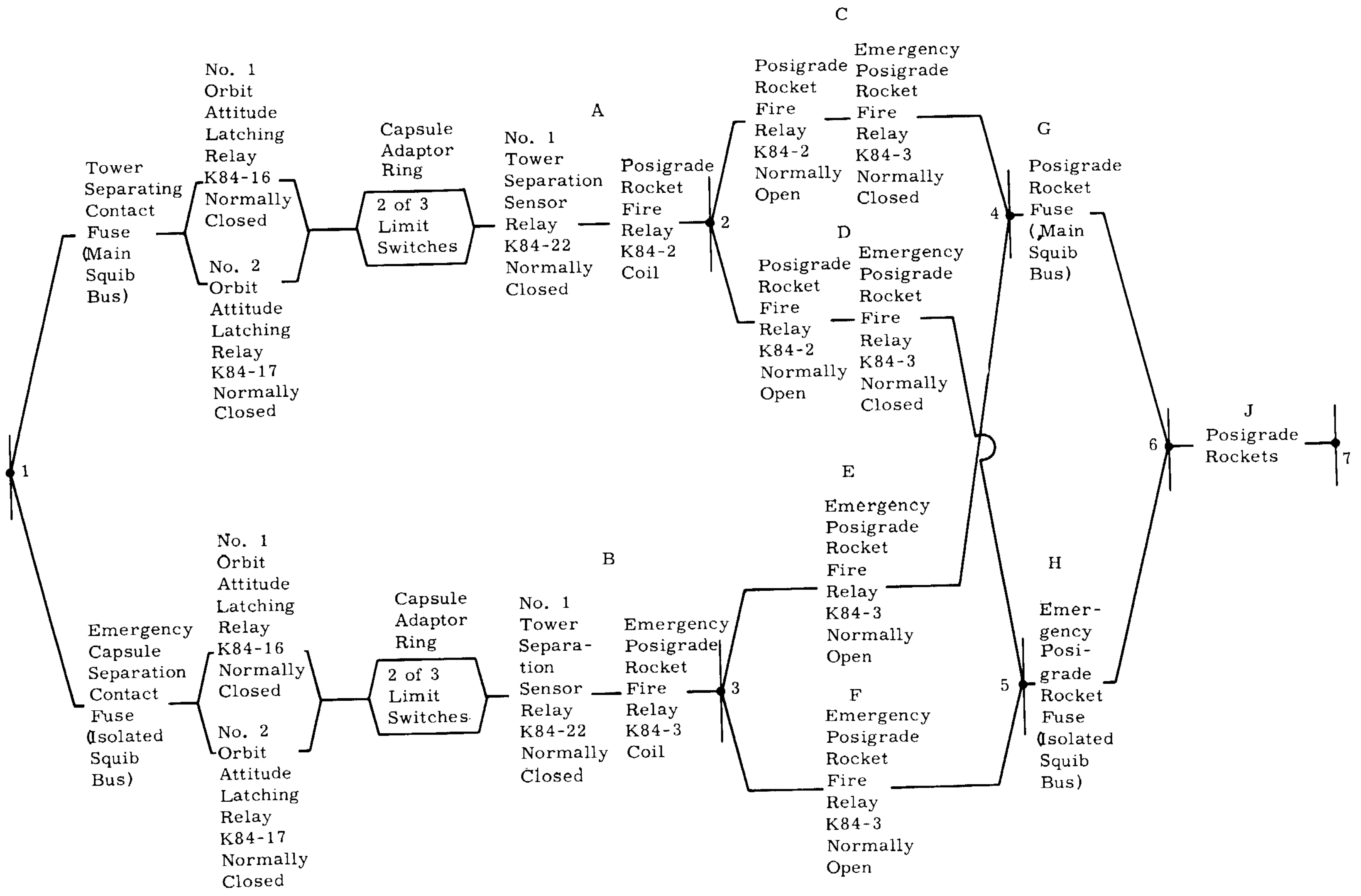
(Hours:Minutes)

Fig. 1 TIME SCHEDULE OF NORMAL MISSION AND ABORTS FOR PROJECT MERCURY


0:00
(1)
0:01
(2)-(7)
(8)
(9)
0:03.633
(10)-(17)
0:06
(18)(19)
(20)-(26)
0:11
(27)-(33)
1:35
(34)-(40)
3:03
(41)-(44)
4:24
(45)-(50)
4:36
(51)-(58)
5:01
Abort G2 initiated if failure(s) in (34) thru (40)
(1G)-(8G)
3:03
(9G)-(25G)
3:30
Abort G1 initiated if failure(s) in (20) thru (33)
(1G)-(8G)
1:35
(9G)-(25G)
2:02
Abort F initiated if failure(s) in (18) or (19)
(1F)-(14F)
0:34
Abort E initiated if failure(s) in (10) thru (15)
(1E)-(3E)
0:06
(4E)-(17E)
0:19
Abort D initiated if failure(s) in (9)
(1D)-(14D)
0:14
Abort C initiated if failure(s) in (8) - unmanned mission only
(1C)-(14C)
0:14
Abort B initiated if failure(s) in (2) thru (7)
(1B)-(3B)
0:03.633
(4B)-(17B)
0:10
Abort A initiated if failure(s) in (1)
(1A)-(11A)
0:02

System	Link Number	System	Link Number
Booster	(1), (2), (10), (18)	Tower Ring Separation	(8), (7A), (11B), (8C)
D. C. Power Supply	(3), (11), (20), (27), (34), (41), (45), (51), (1A), (1B), (4B), (1C), (1D), (1E), (4E), (1F), (1G), (5G), (9G), (17G)	Escape Rocket Firing Capsule Ring Separation Posigrade Rocket Firing	(9), (5A), (9B), (6C), (6D) (16), (4A), (8B), (5C), (5D), (8E) (17), (7D), (9E)
A. C. Power Supply	(4), (12), (21), (28), (35), (42), (46), (52), (2A), (2B), (5B), (2C), (2D), (2E), (5E), (2F) (2G), (6G), (10G), (18G)	Capsule Tracking Communications Periscope Extension	(19), (32), (39) (24), (30), (37) (25)
Environmental Control System	(5), (13), (22), (29), (36), (43), (47), (53), (3B), (6B), (3C), (3D), (3E), (6E), (3F), (3G), (7G), (11G), (19G)	Retro Package Jettison Periscope Retraction	(49), (6A), (10B), (7C), (8D), (13E), (7F), (15G) (50), (15E), (9F), (16G)
Telemetry	(6), (14), (23), (31), (38)	Drogue Chute Deploy	(55), (14B), (11C), (11D), (17E), (11F), (22G)
Attitude Control System, incl. Retro Rocket Firing	(7), (15), (26), (33), (40), (44), (48), (54), (13B), (10C), (9D), (10D), (10E), (11E), (12E), (14B), (16E), (4F), (5F), (6F), (8F), (10F) (5G), (8G), (12G), (13G), (14G), (20G), (21G)	Antenna Fairing Ejection Main Chute Deploy	(56), (9A), (15B), (12C), (12D), (18E), (12F), (23G) (57), (10A), (16B), (12C), (13D), (19E), (13F), (24G)
Abort Initiation	(3A), (7B), (4C), (4D), (7E)	Landing Bag Extension	(58), (11A), (17B), (13C), (14D), (20E), (14F), (25G)

Fig. 2 OVERALL RELIABILITY DIAGRAM FOR THREE-ORBIT MERCURY MISSION
(Link numbers are shown in parentheses)



1
Tower Separating Contact Fuse (Main Squib Bus)
No. 1 Orbit Attitude Latching Relay K84-16 Normally Closed
No. 2 Orbit Attitude Latching Relay K84-17 Normally Closed
Capsule Adaptor Ring
2 of 3 Limit Switches
A
No. 1 Tower Separation Sensor Relay K84-22 Normally Closed
Posigrade Rocket Fire Relay K84-2 Coil
2
C
Posigrade Rocket Fire Relay K84-2 Normally Open
Emergency Posigrade Rocket Fire Relay K84-3 Normally Closed
D
Posigrade Rocket Fire Relay K84-2 Normally Open
Emergency Posigrade Rocket Fire Relay K84-3 Normally Closed
4
G
Posigrade Rocket Fuse (Main Squib Bus)
Emergency Capsule Separation Contact Fuse (Isolated Squib Bus)
No. 1 Orbit Attitude Latching Relay K84-16 Normally Closed
No. 2 Orbit Attitude Latching Relay K84-17 Normally Closed
Capsule Adaptor Ring
2 of 3 Limit Switches
B
No. 1 Tower Separa-tion Sensor Relay K84-22 Normally Closed
Emergency Posigrade Rocket Fire Relay K84-3 Coil
3
E
Emergency Posigrade Rocket Fire Relay K84-3 Normally Open
F
Emergency Posigrade Rocket Fire Relay K84-3 Normally Open
5
H
Emer-gency Posi-grade Rocket Fuse (Isolated Squib Bus)
6
J
Posigrade Rockets
7

Fig. 3 EXAMPLE OF DETAIL DIAGRAM (POSIGRADE ROCKET FIRING AT :06)

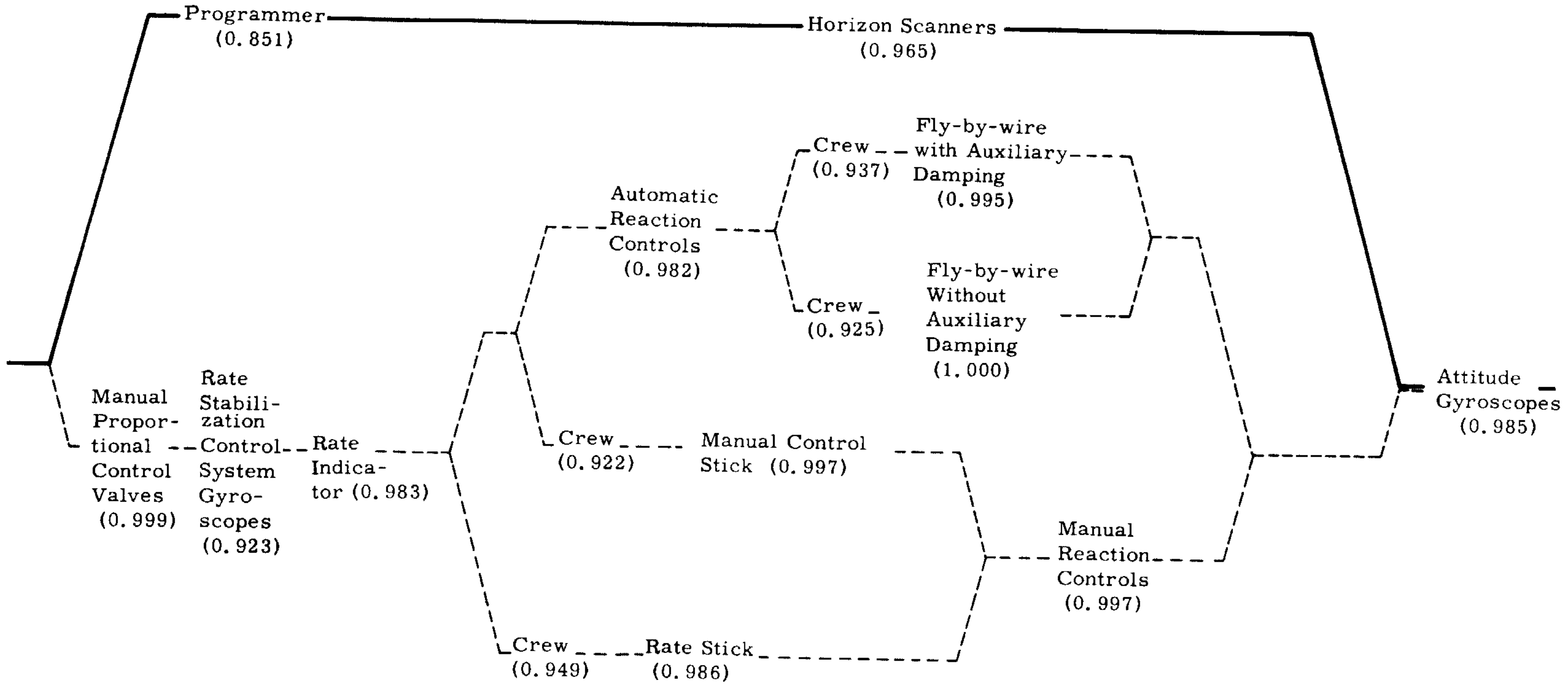


Fig. 3-A ATTITUDE CONTROL SUBSYSTEM-RESET ATTITUDE GYROSCOPES DURING THIRD ORBIT
(Omitting relays, switches, fuses, etc.)

Reliabilities are shown in parentheses. ▬▬ Automatic Mode: Reliability = 0.809. ----- Additional Crew Back-up: Reliability = 0.152. Total Attitude Control Subsystem Reliability = 0.961.

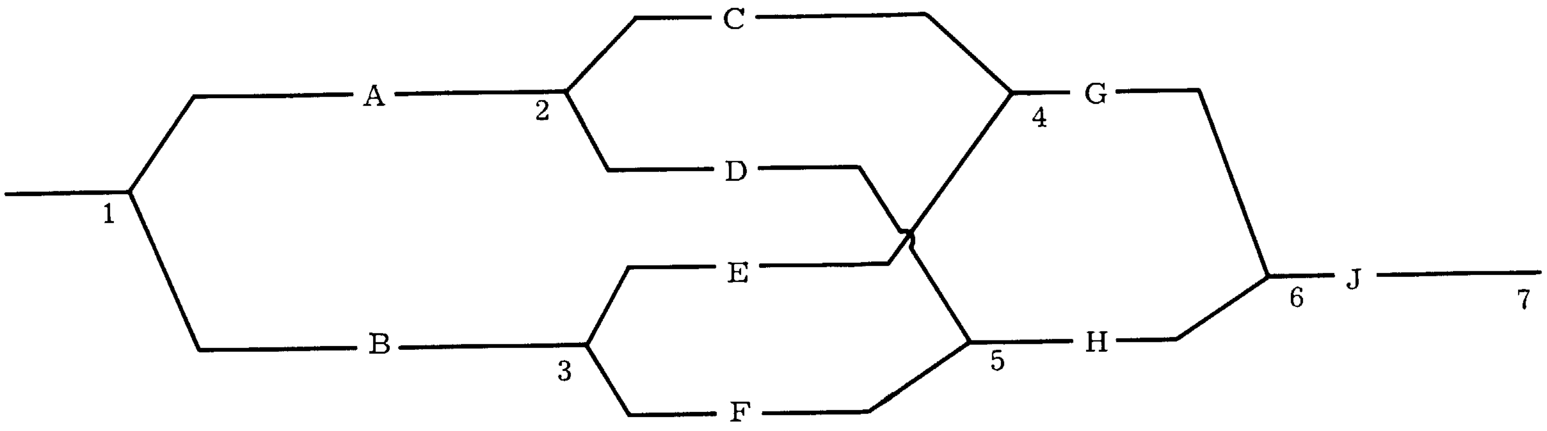


Fig. 4 SIMPLIFIED DIAGRAM OF DETAILED ATTITUDE CONTROL SUBSYSTEM-RESET ATTITUDE GYROSCOPES DURING THIRD ORBIT

NOTE: B is the normal mode of operation and A only functions if B fails.

Let $\Pr\left\{X\right\}$ = probability of event X.

Hence, the reliability of the posigrade rocket firing is:

$$\Pr\left\{\text{input at 1 results in output at 7}\right\} = \Pr\left\{\text{B successful; \underline{and} (E, G) or (F, H) successful; and J successful}\right\} + \Pr\left\{\text{B unsuccessful; \underline{and} A successful; \underline{and} (C, G) or (D, H) successful; and J successful}\right\}$$

$$= \Pr\left\{B\,(EG \text{ or } FH)J\right\} + \Pr\left\{\bar{B}A(CG \text{ or } DH)J\right\}$$

$$= \Pr\left\{BJ\right\}\left\{\Pr(EG) + \Pr(FH) - \Pr(EGFH)\right\} + \Pr\left\{\bar{B}AJ\right\}\left\{\Pr(CG) + \Pr(DH) - \Pr(CGDH)\right\}$$

Fig. 5 EXAMPLE OF RELIABILITY EQUATION (POSIGRADE ROCKET FIRING)

NOTE: A capital letter represents a successful event(s) and a capital with a bar, failure; also, the product of capital letters means the occurrence of all such events, for example, EG means E <u>and</u> G must occur.

where

$$\lim_{h \to 0} \frac{o(h)}{h} = 0 \qquad \text{and} \qquad h > 0.$$

This implies that the reliability for t units of time is

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

where $\lambda = 1/\theta$, that is, where λ is the reciprocal of the mean time to failure θ .

2. For these continuously operating devices the estimated mean time to failure is

$$\tilde{\theta} = \frac{T}{(r+1)}$$

where

T = total time accumulated on devices tested
r = number of failures observed
$\tilde{\theta}$ = an almost unbiased estimate of the true mean time to failure (reference 1).

3. For go-no-go devices it was assumed that the probability of k failures observed out of n tested is given by

$$\binom{n}{k} p^{k} (1-p)^{n-K}$$

where p is the constant probability of a device failing on a single trial.

4. For the go-no-go devices the estimated constant probability of failure is

$$\hat{p} = \frac{\text{number of failures observed}}{\text{number of devices tested}}$$

where $\hat{p}$ is an unbiased estimate of p, the true probability of failure. The estimated reliability of the device is obviously then $\hat{R} = 1 - \hat{p}$.

The basis for estimating reliability of parts, components, and subsystems consists of a summary of tests performed at the contractor's and subcontractor's plants, as well as failure reports from the field. The test data included in this summary satisfied the following three conditions:

1. The data must come from testing that duplicates or approximates the expected conditions of functioning that will be encountered on the 3-orbit manned mission.
2. The data must come from tests that have been performed for or are being applied to the Mercury project.
3. The data must come from the testing of equipment that is identical or similar to the equipment that will be actually used for the capsule of a 3-orbit manned mission.

The test information provided by the contractor represents the following types of tests:

1. Reliability tests
2. Vendor qualification tests when the type of testing exercises the equipment in the same manner as will occur on the mission
3. Pre-installation acceptance tests
4. Capsule system tests
5. Special tests, e.g., compatibility mock-up tests and manned environmental control system tests.

A total of 905 discrepancies were accumulated by July 1, 1960. Of this total, 107 were considered to be applicable as reliability failures for the unmanned and manned mission analyses. The remaining discrepancies were excluded for the following reasons:

1. Failure analysis indicates that the initial failure report or test procedure was in error.
2. Failure analysis indicates inspection or workmanship error, or gross mishandling. These failures are not due to the operation of the unit and would not occur during a mission.
3. Acceptance criteria were revised or deviated, allowing part to have unrestricted usage.
4. Effective corrective action for the failure has been incorporated.
5. Effect of failure on presently planned orbital mission is negligible.
6. Failure occurred as a result of exceeding the usable operating life of the component. The part in question entered a known wear-out stage that it will not be allowed to enter in actual usage.

7. Failure occurred during testing under environmental conditions in excess of specification requirements. Such failure is attributable to overstressing that would not occur in an actual mission.

8. Discrepancy is a measurable and nonvariable parameter of the particular unit. Units which have an unacceptable value will not be installed on manned capsules.

9. Testing was not considered applicable. The failure did not occur during one of the tests specified or was not a test of a complete assembly.

10. Test time was not available. The failure occurred during a test ordinarily considered, but time or cycling data were not available.

11. Component or part was not required in this study. The unit on which the failure has occurred is not essential, or is not required to function any time during the mission, or is an obsoleted unit.

In some instances the estimates of subsystem reliability were based on very sparse test data. In other cases the estimates of reliability were based on various kinds of test results, such as pre-installation acceptance tests, reliability tests, and qualification tests. Occasionally information from only one type of test was available. In some cases where information from more than one type of test was available, all test results were pooled in order to obtain an estimate of reliability. It is apparent from the data that in some cases heterogeneous test results have been combined. This could have been avoided by eliminating certain results. However, then there is the question of introducing other biases. In those cases, namely, where multiple tests are available for a given subsystem, one should interpret the estimate of reliability as an average over the various types of tests.

PROBABILISTIC MODEL

A recent paper by Wolman (reference 2) gave a general probabilistic model in a set-theoretic framework and was the basis for the Mercury analysis. This report will extend reference 2, which gave only the model for the normal mission, by including the abort situations. But first, let us summarize reference 2, using specific Mercury terminology.

The Mercury spacecraft is composed of the 19 major systems listed on page 3. It follows then that the reliability of the Mercury capsule is given by

$$\begin{aligned}\Pr\{\text{Mercury}\} &= \Pr\{abc\ldots s\}\\ &= \Pr\{a\}\cdot\Pr\{b|a\}\cdot\Pr\{c|a,b\}\ldots\Pr\{s|a,b,\ldots,r\} \qquad (1)\end{aligned}$$

where the lower case letters represent the major systems listed on page 3,

$\Pr\{X,Y,\ldots\}$ is the probability of success of systems X, Y, . . . ; and, also, $\Pr\{Z|A,B,C,\ldots\}$ is the conditional probability of success of system Z given the successful functioning of systems A, B, C, ... The reason for expressing the Mercury spacecraft reliability as the product of conditional probabilities is to take into account possible dependencies among systems. However, the amount of computations involved dictated making the assumption of independence among systems. The elements common to two or more systems were, in general, small parts with high reliabilities such as relay coils. Such small parts were counted as separate and independent entities in the systems.

Because the probability of the need to abort and the ability to abort varies during the mission and also because a number of the major systems operate in two different modes during the mission, the normal 3-orbit mission was divided into the time periods shown in Fig. 1.

Having the time periods, now let S_i represent the event that system α operates successfully from time t_0 to time t_i for $i = 0, 1, \ldots k_\alpha$ (t_{k_α} is time the need for system α to operate ends, and $\Pr\{S_i\}$ the probability of event S_i). Then, since successful operation of the system at time t_i implies successful operation of that system from time t_0 to time t_{i-1}, it follows that

$$S_i \subset S_{i-1} \qquad i = 1, 2, \ldots, k_\alpha \tag{2}$$

where S_i represents the set synonymous with the event S_i discussed above. Thus, the reliability of system α through time t_i is

$$\begin{aligned} \Pr\{S_i\} &= \Pr\{S_i\}\cdot\Pr\{S_2|S_1\} \ldots \Pr\{S_i|S_{i-1}\} \\ &= \Pr\{S_1\}\frac{\Pr\{S_2\}}{\Pr\{S_1\}} \cdots \frac{\Pr\{S_i\}}{\Pr\{S_{i-1}\}} \end{aligned} \tag{3}$$

One must therefore find $\Pr\{S_r\}$ for $r = 1, 2, \ldots, i$. If we let S_r^* be the set synonymous with the event that the system operates successfully from time t_{r-1} to t_r, then

$$S_i = S_1^* \cap S_2^* \cap \ldots \cap S_i^* \tag{4}$$

For the Mercury study, these intersections were obtained on electronic computers.

ABORT MODEL

Carrying the results in reference 2 one step further, we shall now give the probabilistic abort model used in the Mercury study.

Similar to the 3-orbit normal mission, the j'th abort (j is one of the aborts A through G2) is divided into time periods

$$0 = t_0 < t_1 < t_2 < \ldots < t_{i-1} < t_a < t_i < \ldots < t_{\ell_j} \qquad (5)$$

where t_{ℓ_j} is the time of touchdown for the j'th abort.

The flight safety reliability is then given by

$$\begin{aligned} \Pr\{\text{Flight Safety}\} &= \Pr\{\text{Successful 3-orbit normal mission}\} \\ &\quad + \sum_{\substack{\text{all mutually} \\ \text{exclusive aborts}}} \Pr\{\text{Need to abort and abort successfully}\} \\ &= \Pr\{\text{Successful 3-orbit normal mission}\} + \sum \Pr\{M_{i-1}\, \overline{M}_a\, m_a\, m_{\ell_j}\} \\ &= \Pr\{\text{Successful 3-orbit normal mission)} + \sum \Pr\{M_{i-1}\} \Pr\{\overline{M}_a \mid M_{i-1}\} \\ &\qquad \Pr\{m_a \mid M_{i-1}\, \overline{M}_a\} \Pr\{m_{\ell_j} \mid M_{i-1}\, \overline{M}_a\, m_a\} \end{aligned} \qquad (6)$$

where

M_{i-1} is event: normal mission to time t_{i-1}
$\overline{M}_a$ is event: failure of normal mission some time prior to t_a.
m_a is event: able to abort
m_{ℓ_j} is event: abort successfully through time of touchdown

and the summation is over all possible aborts.

The need to abort occurs whenever the normal mission cannot be continued. This depends on the mission ground rules determined in advance of the space flight, and in the case of the Mercury project, these ground rules were set by the Manned Spacecraft Center.

In Project Mercury, a number of systems possess both a normal and a minimum mode of operation. By this, it is meant that a system has a mode of operation, designated herein as the normal mode, through the first two orbits of the normal three-orbit mission. But, during the last of the three orbits, or during the time period at the end of which an abort is planned, the system possesses a backup or minimum mode of operation. The normal mode may be considered as the case where every subsystem must operate, whereas the minimum mode is the case where only enough subsystems operate so that the system operates successfully. As a simple hypothetical example, consider the case where the system consists of just two subsystems, A and B. The normal mode would require the successful operation of both A and B while the minimum mode would require the successful operation of either A or B. Under the mission ground rules mentioned above, an abort was deemed necessary when a failure occurred in a system such that a switch from a normal mode to a minimum mode was required.

The systems possessing normal and minimum modes are:

d-c Power Supply
a-c Power Supply
Environmental Control System (ECS)
Attitude Control System.

Table 1, when filled out, gives the probabilities of mission success and flight safety. In column 1 of Table 1, the probability of a normal mission to time t_{i-1}, $\Pr\{M_{i-1}\}$, is the product of the conditional and unconditional probabilities of the various systems, as discussed in Eq. (1). The systems considered in the calculation of $\Pr\{M_{i-1}\}$ are those that have operated successfully or else are operating in their normal modes to t_{i-1}. For example, let us assume that the spacecraft consists of just three systems and let these systems be denoted by A, B, and C. Then

$$M_{i-1} = (S_{i-1})_A \cdot (S_{i-1})_B \cdot (S_{i-1})_C$$

and

$$\Pr\{M_{i-1}\} = \Pr\{(S_{i-1})_A\} \cdot \Pr\{(S_{i-1})_B \mid (S_{i-1})_A\} \cdot \Pr\{(S_{i-1})_C \mid (S_{i-1})_B \cdot (S_{i-1})_A\} \tag{7}$$

where $(S_{i-1})_\alpha$ is the event that system α is operating in its normal mode to t_{i-1} or else has successfully completed its function at some time prior to t_{i-1}.

The probability of failure of normal mission at some time prior to t_a, $\Pr\{\overline{M}_a\}$, is, of course, the probability of a normal mission to time t_a subtracted from unity, i.e.,

$$\Pr\{\overline{M}_a\} = 1 - \Pr\{M_a\} \tag{8}$$

Table 1

PROBABILITIES OF MISSION SUCCESS AND FLIGHT SAFETY

	Probability of										
Time period	I Success up to beginning of period (U*)	II Success through end of period (U*)	III Abort being required (U-J*)	IV Being able to abort		V Successful abort		VI Abort failure		VII Being unable to abort	
				A (C*)	B (U-J*)	A (C*)	B (U-J*)	A (C*)	B (U-J*)	A (C*)	B (U-J*)
		**									
									Σ(VI-B)		Σ(VII-B)

$1 - [\Sigma(\text{VI-B}) + \Sigma(\text{VII-B})] = \Pr\{\text{Flight Safety}\}$

*U: unconditional; U-J: unconditional-joint; C: conditional

**Mission success

Again, $\Pr\{M_a\}$ is the product of the conditional and unconditional probabilities of the various systems as discussed in Eq. (1). The systems considered are those that have operated successfully or are operating in their normal modes to t_a.

The probability of a normal mission to the end of the time period t_i, $\Pr\{M_i\}$, is the product of the conditional and unconditional probabilities of the various systems. The systems considered are those that have operated successfully or are operating in their normal modes to t_i.

Since the successful completion of the normal mission through time t_a implies successful operation through t_{i-1},

$$M_a \subset M_{i-1} \tag{9}$$

where M_{i-1} and M_a are sets synonymous with the events discussed above and the unconditional probability of an abort being required is

$$\Pr\{M_{i-1} \overline{M}_a\} = \Pr\{M_{i-1}\} - \Pr\{M_a\} \tag{10}$$

The conditional probability of being able to abort, given that an abort is required, is

$$\begin{aligned} \Pr\{m_a \mid M_{i-1} \overline{M}_a\} &= \Pr\{M_{i-1} \overline{M}_a m_a\} / \Pr\{M_{i-1} \overline{M}_a\} \\ &= \frac{\Pr\{M_{i-1} m_a\} - \Pr\{M_a m_a\}}{\Pr\{M_{i-1}\} - \Pr\{M_a\}} \end{aligned} \tag{11}$$

since $\Pr\{A\overline{B}\} = \Pr\{A\} - \Pr\{AB\}$ and $M_a \subset M_{i-1}$.

Let S_a represent the event that a system operates successfully from time t_0 to time t_a and $\Pr\{S_a\}$ the probability of event S_a. Then, as before, $S_a \subset S_{i-1}$, where S_a represents the set synonymous with the event S_a discussed above. Now let s_a represent the event that the system operates, because of the occurrence of failure(s), in a minimum mode such that an abort is possible but the normal mission is discontinued. This means that

$$S_a \subset s_a \tag{12}$$

where again S_a and s_a represent sets synonymous with the events discussed above. That is, the normal mode S_a implies the possibility of a successful abort.

Letting systems B and C in Eq. (7) represent systems having both normal and minimum modes, the probability of the event $M_{i-1} m_a$ becomes

$$\begin{aligned} \Pr\{M_{i-1}\, m_a\} &= \Pr\{(S_{i-1})_A\, (S_{i-1})_B\, (S_{i-1})_C \cap (s_a)_A\, (s_a)_B\, (s_a)_C\} \\ &= \Pr\{(S_a)_A\}\, \Pr\{(S_{i-1})_B\, (s_a)_B \mid (S_a)_A\} \\ &\quad \Pr\{(S_{i-1})_C\, (s_a)_C \mid (S_a)_A\, (S_{i-1})_B\, (s_a)_B\} \end{aligned} \tag{13}$$

since

$$(S_{i-1})_A\, (s_a)_A = (S_{i-1})_A\, (S_a)_A = (S_a)_A$$

Also, since

$$\Pr\{M_a\, m_a\} = \Pr\{M_a\}$$

we have

$$\Pr\{M_a\} = \Pr\{(S_a)_A\}\, \Pr\{(S_a)_B \mid (S_a)_A\}\, \Pr\{(S_a)_C \mid (S_a)_A\, (S_a)_B\} \tag{14}$$

The intersections $(S_{i-1})_\alpha\, (s_a)_\alpha$ and their probabilities were obtained with the aid of electronic computers.

Since conditional probabilities obey the same general rules as unconditional probabilities, the conditional probability of being unable to abort, given the need to abort, is

$$\Pr\{\overline{m}_a \mid M_{i-1}\, \overline{M}_a\} = 1 - \Pr\{m_a \mid M_{i-1}\, \overline{M}_a\} \tag{15}$$

and the unconditional probability of this event is

$$\Pr\{M_{i-1}\, \overline{M}_a\, \overline{m}_a\} = \Pr\{\overline{m}_a \mid M_{i-1}\, \overline{M}_a\}\, \Pr\{M_{i-1}\, \overline{M}_a\} \tag{16}$$

The conditional probability of successfully completing an abort, given that an abort is required and that we are able to abort, is

$$\Pr\{m_{\ell_j} \mid M_{i-1}\, \overline{M}_a\, m_a\} = \Pr\{M_{i-1}\, \overline{M}_a\, m_a\, m_{\ell_j}\} \,/\, \Pr\{M_{i-1}\, \overline{M}_a\, m_a\} \tag{17}$$

In Project Mercury, the modes of operation, for the systems having both normal and minimum modes, are the same for both the ability to initiate and to complete the abort. Thus,

$$m_{\ell_j} \subset m_a \tag{18}$$

and so Eq. (17) becomes

$$\Pr\{m_{\ell_j} \mid M_{i-1}\,\overline{M}_a\,m_a\} = \frac{\Pr\{M_{i-1}\,m_{\ell_j}\} - \Pr\{M_a\,m_{\ell_j}\}}{\Pr\{M_{i-1}\,m_a\} - \Pr\{M_a\}} \tag{19}$$

The unconditional (joint) probability of successfully completing an abort is

$$\Pr\{M_{i-1}\,\overline{M}_a\,m_a\,m_{\ell_j}\} = \Pr\{m_{\ell_j} \mid M_{i-1}\,\overline{M}_a\,m_a\} \cdot \Pr\{M_{i-1}\,\overline{M}_a\,m_a\} \tag{20}$$

The conditional probability of failing to complete an abort, given that an abort is required and that we are able to, is

$$\Pr\{\overline{m}_{\ell_j} \mid M_{i-1}\,\overline{M}_a\,m_a\} = 1 - \Pr\{m_{\ell_j} \mid M_{i-1}\,\overline{M}_a\,m_a\} \tag{21}$$

and the unconditional (joint) probability of this event is

$$\Pr\{M_{i-1}\,\overline{M}_a\,m_a\,\overline{m}_{\ell_j}\} = \Pr\{\overline{m}_{\ell_j} \mid M_{i-1}\overline{M}_a\,m_a\} \cdot \Pr\{M_{i-1}\,\overline{M}_a\,m_a\} \tag{22}$$

ASTRONAUT PERFORMANCE EVALUATION

As for the probability that the astronaut will perform the proper overrides at the proper times, a team of five individuals, professionally qualified to assess man's performance capabilities, was formed to estimate them. These estimates were augmented, wherever possible, by experimental data gathered at the Aviation Medical Acceleration Laboratory of the Naval Air Development Center at Johnsville, Pennsylvania. Crew performance in high-performance airplanes was also taken into consideration.

A description of each manned override with its attendant failure indications and corrective action required was listed. Environmental conditions, astronaut performance information, and systems description during the overrides were also obtained. These were then evaluated by the individual panel members who made independent estimates of the astronaut's performance. The average of the five estimates for each override was then computed.

Because the ability of the astronaut to perform his overrides depends on whether his space suit is overpressurized or not, two sets of estimates were made. One set was the estimates based on the assumption that the astronaut's suit was properly pressurized, and the other, on the assumption that it was overpressurized.

As mentioned in assumption 14, page 4, the astronaut is not required to orient the Mercury capsule while in the earth's shadow. Therefore, the estimates for this maneuver, while out of the sun's light, were not used in this study. However, the panel considered these overrides to be much more difficult at night than in the daylight.

Having the two sets of averaged estimates (one for a normally pressurized suit and one for an overpressurized suit), the probabilities of having an overpressurized or a normally pressurized suit were then calculated. These served as weights to the two averages for each override, and an estimated probability for the astronaut's ability was then computed.

The method used will now be given. First, a list was made of causes that would result in an overpressurized suit. Then the probabilities of their failing were computed. Listed below are the items whose failures would result in an overpressurized suit:

Excessive cabin leakage
Cabin pressure control valve
Suit pressure relief valve
Suit pressure regulator relief valve.

It is obvious that an overpressurized suit.can be deflated by the astronaut's opening his face plate. However, under the mission ground rules, the astronaut cannot open his face plate unless the cabin has not leaked excessively and both of the following have failed:

Suit pressure relief valve
Suit pressure regulator relief valve.

Test data showed that the reliability of the suit pressure regulator relief valve is unity, and, hence, the need for the astronaut to open his face plate is obviated. However, let us develop the general formula for the percentage of time the astronaut will have an overpressurized suit.

Since the items whose failures would result in an overpressurized suit are all found in the Environmental Control System (ECS), we may set

$$\Pr\{ECS\} = \Pr\{ECS \cap (H \cup S) \cap (Op \cup Cl)\} \tag{23}$$

where ECS is the event that the ECS is working properly or else the set is synonymous with the event; H is the set synonymous with the event that the suit is overpressurized or "hard"; S is the set synonymous with the event that the suit is normally pressurized or "soft"; Op is the set synonymous with the event that the face plate is open; and Cl is the set synonymous with the event that the face plate is closed. The assumptions we have made in (23) are that $H \cup S = \mathfrak{S}$ and that $Op \cup Cl = \mathfrak{S}$ where $\mathfrak{S}$ is the whole space. That is, the suit is either hard or soft (and not partially overinflated) and the face plate is either opened or closed. By expansion, (23) becomes

$$\begin{aligned}\Pr\{ECS\} &= \Pr\{(ECS \cap H \cap Op) \cup (ECS \cap H \cap Cl) \cup (ECS \cap S \cap Op) \cup (ECS \cap S \cap Cl)\} \\ &= \Pr\{ECS \cap H \cap Op\} + \Pr\{ECS \cap H \cap Cl\} + \Pr\{ECS \cap S \cap Op\} + \Pr\{ECS \cap S \cap Cl\}\end{aligned} \tag{24}$$

since the four events are mutually exclusive. However, the probability of the first of these four events, viz, $H \cdot Op$ is zero. Therefore, the conditional probability that the suit is overpressurized, given that the ECS is working, is

$$\Pr\{ECS \cap H \cap Cl\} \,/\, \Pr\{ECS\} \tag{25}$$

The estimate of the astronaut's ability to perform an override is thus

$$\begin{aligned}\Pr\{Crew\} = {} & \frac{\Pr\{ECS \cap H \cap Cl\}}{\Pr\{ECS\}} \times \{\text{Ave. Est. for hard suit}\} \\ & + \frac{\Pr\{ECS \cap S \cap Op\} + \Pr\{ECS \cap S \cap Cl\}}{\Pr\{ECS\}} \\ & \times \{\text{Ave. est. for soft suit}\}\end{aligned} \tag{26}$$

The term "Average estimate for hard suit" is the average of the estimates of the astronaut's ability to perform this override while in an overpressurized or "hard" suit. The term "Average estimate for soft suit" is the average of the estimates of the astronaut's ability to perform this override while he is in a properly inflated or "soft" suit.

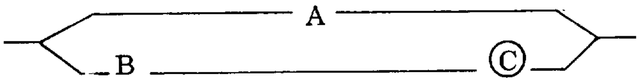
TWO TYPES OF CREW ACTION

In accordance with assumption 10, page 3, hardware working at time t_i implies that it has worked at t_{i-1} and hence

$$E_i \subset E_{i-1} \tag{27}$$

where E_x is the set synonymous with the event that equipment E has worked from t_0 to t_x. However, for the astronaut, the fact that he is able to perform his duties at t_i does not necessarily imply that he was able to do so at t_{i-1}. Hence, the electronic computer program had to recognize this. Moreover, the computer was required to recognize the fact that two types of crew actions were required: (1) the one-time action whereby the astronaut performed an action just once, such as throwing a switch; and (2) the continuing type of action where the astronaut continued his action for a length of time, e.g., orienting the capsule during orbit.

As an example, let us consider the following simple system:



The above figure shows that subsystem A is the automatic mode and that if A fails, then the astronaut performs his override, C, which activates subsystem B. For the 3-orbit Mercury mission, the subsystems are turned on at all times although the output from some of the subsystems may be zero. This may be likened to having a radio set turned on but at zero volume. Now, if the above system were to operate over two time periods, denoted by t_1 and t_2, then the probability of the system operating at t_2 is

$$\begin{aligned} \Pr\{S_2\} &= \Pr\{(A_1 \cup \bar{A}_1 B_1 C_1) \cap (A_2 \cup \bar{A}_2 B_2 C_2)\} \\ &= \Pr\{A_1 A_2 \cup A_1 \bar{A}_2 B_2 C_2 \cup \bar{A}_1 A_2 B_1 C_1 \cup \bar{A}_1 \bar{A}_2 B_1 B_2 C_1 C_2\} \end{aligned} \tag{28}$$

In (28), the third term in the right side bracket, viz., $\bar{A}_1 A_2 B_1 C_1$, is the null set since, by assumption, a piece of hardware cannot recover or be repaired, and, hence, the set $\bar{A}_1 A_2$ is obviously empty. For equipments A and B,

$$A_2 \subset A_1 \quad \text{and} \quad B_2 \subset B_1.$$

Hence, (28) becomes

$$\begin{aligned} \Pr\{S_2\} &= \Pr\{A_2 \cup A_1 \bar{A}_2 B_2 C_2 \cup \bar{A}_1 B_2 C_1 C_2\} \\ &= \Pr\{A_2\} + \Pr\{A_1 \bar{A}_2 B_2 C_2\} + \Pr\{\bar{A}_1 B_2 C_1 C_2\} \end{aligned} \tag{29}$$

as the sets are mutually exclusive.

Now, if the crew action, C, is a one-time action

$$\Pr\{C_1\ C_2\} = \Pr\{C_1\} \tag{30}$$

since the single action need not be repeated during the second time period. However, if C is a continuous action,

$$\Pr\{C_1\ C_2\} = \Pr\{C_1\} \cdot \Pr\{C_2\} \tag{31}$$

April 1962

REFERENCES

1 Epstein, B. Statistical Techniques in Life Testing, Chapter III, p. 3.62, 1959. Issued by the Office of Technical Services, U.S. Department of Commerce as PB 171580.

2 Wolman, W. Reliability Estimation for Space Systems. A paper presented before the Washington Chapter of the Institute of Radio Engineers Professional Group on Reliability and Quality Control, Washington, D.C., Sept. 14, 1961. Available as N62-16428 from the Office of Technical Services, U.S. Department of Commerce, Washington 25, D.C.

NASA-Langley, 1962