The Space Congress® Proceedings

1971 (8th) Vol. 1 Technology Today And Tomorrow

Apr 1st, 8:00 AM

The Determination of Avionics Redundancy for Minimum Cost

Myron Kayton
Head of System Engineering, Space Shuttle Avionics, TRW Systems Group

William A. Klein
Reliability Staff Engineer, TRW Systems Group

THE DETERMINATION OF AVIONICS REDUNDANCY FOR MINIMUM COST

Dr. Myron Kayton
Head of System Engineering
Space Shuttle Avionics
TRW Systems Group
Redondo Beach, California

William A. Klein
Reliability Staff Engineer
TRW Systems Group
Redondo Beach, California

ABSTRACT

This paper describes an analysis of the level of redundancy of line repaceable units (LRUs) required for the Space Shuttle avionics system. The required number of LRUs is neither based on an arbitrary numerical probability nor on an arbitrary number of replicative units. Instead, a total cost to the program of each added LRU is calculated and the configuration that results in lowest program cost is selected.

The analysis includes the costs of developing and procuring hardware, and the annual maintenance expense. Cost penalties for weight and electric power consumption are imposed for each added LRU. Improvement in reliability is quantified in terms of the reduced costs due to fewer lost vehicles and fewer missions where the payload cannot be delivered. Realistic mission rules are used for determining when the payload cannot be safely delivered. The analysis allows a choice of high-reliability or low-reliability procurement policies for each LRU.

The results show that triply redundant Booster equipment and triply-redundant Orbiter equipment, are most cost effective, except for one additional inertial platform and central computer in the Orbiter.

1.0 INTRODUCTION

This report summarizes the analytic portion of a redundancy study performed for the avionics system as part of the Space Shuttle Phase B contract.

Redundancy is usually specified in either of two ways:

a) Specify the probability of successfully completing the mission and the probability of safe return. Redundancy of the equipment is then selected as necessary to meet the reliability goals.

b) Specify the level of redundancy, directly, such as the "no single-point-failure" rule of Apollo or the "fail-operational after the two most critical failures, fail-safe after the third (FO/FO/FS)" rule specified by NASA in the Phase B work statement.

Neither specification method is wholly satisfactory because costs are not taken into consideration. Some method that selects redundancy levels considering both reliability data and cost data is needed. This can be done by summing failure penalty costs, which decrease as redundancy increases, with initial and support costs, which increase as redundancy increases. This sum is called the Figure-Of-Merit Cost. This paper describes a method of redundancy selection by minimizing Figure-Of-Merit Cost. In order to make the method as general as possible, weight and energy penalties were included in the Figure-Of-Merit Cost. This method provides a procedure for identifying exceptions to the FO/FO/FS rule and for specifying numerical probabilities of System Safety and Success.

A computer program was developed that accepts cost and reliability data for the LRUs, and the mission parameters discussed in Section 2. It determines the redundancy level that minimizes the Figure-Of-Merit Cost, and calculates Buy-In Cost and the probabilities of safe return and of payload delivery. The program can also be used to evaluate the effect of operational parameters and design decisions on redundancy, reliability, and cost.

Many assumptions were made in order to apply this method of analysis to the shuttle. The assumptions were based on available data during Phase B and can be improved as the project continues. The computer program was designed to permit all parameters to be readily changed.

The next section describes the particular shuttle mission for which results are reported in this paper. It includes a discussion of the reliability model. Section 3 describes those aspects of the avionic system design that are pertinent to this study. Section 4 presents the cost model and the values of some of the cost parameters. Section 5 discusses the computer program and Section 6 summarizes the principal results. Sections 7 and 8 contain conclusions and acknowledgements.

2.0 MISSION DESCRIPTION

2.1 Mission Phases

The Space Shuttle has three types of mission:

a) Deliver or retrieve satellites

b) Conduct experiments while in orbit

c) Resupply a space station

The space station resupply mission is the one analyzed in this paper. The Booster launches both vehicles, separates, and returns to the launch site. The Orbiter continues into orbit, effects a rendezvous with the station and remains inertly docked. After approximately 6 days, the Orbiter undocks and returns to the launch site. The Orbiter and Booster flight profiles are shown in Tables 1 and 2. Flight phases during which switching transients are not tolerable are identified. For the Orbiter, the 12 hour ascent time is typical of an Apollo-type concentric flight plan. The nominal descent time is 4 hours. Studies were made of worst-case 24 hour returns and showed little difference from the results reported here.

Pre-launch and ground phases are not considered except to assume one ground failure per flight failure.

2.2 K Factors

The actual duration of each phase is multiplied by a k factor to produce an effective duration representing the environmental severity of each phase. Different k factors are used to allow for differing vibrational and thermal environments at various locations in the vehicle. In addition to the variation of k factors due to mission phase and location, the k factor depends on the type of LRU and its utilization. For each of 4 categories of LRU, factors are assigned depending on whether the equipment is off or on. The k factors range from 0.1 for unpowered electromechanical equipment in a non-vibrational environment to 500 for operating electromechanical equipment in a high-vibration environment.

Two effective mission durations are calculated for each LRU. One LRU of each redundant group is on at all times. The other LRUs are off except in critical phases when switching transients cannot be tolerated. These utilizations by mission phases are also used to calculate the amount of electrical energy consumed by each LRU.

2.3 Reliability Model

In order to calculate the role of each LRU in the total reliability, a reliability block diagram was made. Each function (e.g., communication) required for mission success was assigned its own Series Block, which contained all LRUs required to perform the function. Thus, if two or more LRU types are redundant to one another, then they must be considered together in a single Series Block. The product of all Series Block reliabilities gives the probability of mission success.

The minimum requirement for a successful mission is that the payload be delivered to the station and that crew and vehicle return safely to the primary landing site. A safe mission is identified as any mission in which crew and vehicle return safely to any approved shuttle landing site. Each LRU is identified as required either for safety or for success. For example, rendezvous aids are required for success whereas the central computers, navigation aids, and flight control actuators are for safety. Communications are considered to be required for safety in order to permit diversion from a bad weather airport since neither vehicle can hold and fly to an alternate field.

Exponentially distributed times to failure, i.e., constant failure rates, were used for all LRUs. This condition is approached more and more closely as (1) infant mortality failures are removed by procurement screening and/or burn-in; and (2) wear-out failures are avoided by effective preventive maintenance.

The expected number of failures per flight of each LRU is found by dividing the corresponding effective durations by the LRU's MTBF. These values are used in standby redundancy formulas to calculate reliabilities. This is an approximation, but a very close one based on past experience.

2.4 Mission Outcomes

Four possible mission outcomes are recognized in this analysis:

a) Nominal or successful mission (no abort, no loss).

b) Payload not delivered but no vehicle loss (abort, no loss).

c) Payload delivered, but vehicle lost during return flight (no abort, loss).

d) Vehicle lost prior to payload delivery (abort, loss).

A mission must be reflown if either outcome 2 or 4 occurs. The vehicle is lost if either outcome 3 or 4 occurs.

Some mission phases are omitted for an Orbiter which cannot deliver its payload due to early failures, see Figure 1. For the Orbiter, a decision that the payload cannot be delivered is possible up to the end of the docking phase and is not made until that point. If the payload is not delivered, the Orbiter immediately starts to return, beginning at the phase just after undocking and proceeding through the rest of the nominal mission. For the Booster, failures that would prevent the Orbiter from delivering the payload can occur only during boost, and a Booster abort continues with the same mission profile as a nominal mission.

If all Orbiter LRUs for a given success Series Block fail prior to docking, the payload is not delivered. This payload is also undelivered if only 1 or 2 (an input variable to the computer program) LRUs of a safety Series Block remain.

3.0 DESCRIPTION OF AVIONICS

The functions of the avionics are:

1) Traditional functions such as navigation, guidance and communication

2) Provide a data transmission and data processing service for control and checkout of vehicle systems.

Because communication between the avionics equipment is via the computer-controlled data buses, the computers and bus components are required for flight safety. The bus structure is such that any LRU can be operated at the same time as any other LRU. The power distribution system was not included in this study.

The study modeled the failure detection capabilities of the avionics system. When three or more redundant LRUs are on, failure detection is by comparison in the central computers. When two LRUs of a redundant group remain, failure detection relies more heavily upon built-in test within each LRU. This study assumed that the built-in test could identify 90% to 100% of the LRU failures, a fraction that can be chosen independently for each LRU (see Table 3).

4.0 COST PARAMETERS

4.1 Buy-In Cost

The Out-of-Pocket or Buy-In Cost of the shuttle avionics is defined as the initial investment in avionics hardware prior to the first operational flight. It is expressed as follows for each vehicle:

$$\text{Buy-In Cost} = 1/2\ (\text{Development Cost}) + (\text{Cost per Shipset})\ (N+3) + 5\ (\text{Cost per LRU})$$

where half of the development cost is charged to the Booster and half to the Orbiter, and where N is the number of operational vehicles. Two extra shipsets are required during the flight test program, a third shipset of spares is needed, and 10 LRU sets (5 for the Orbiter and 5 for the Booster) are used in ground testing. A shipset consists of 1, 2, 3, 4, or 5 LRUs of a given type depending on the level of redundancy.

4.2 Figure-Of-Merit Cost

The Figure-of-Merit Cost is a measure of the ten-year program cost. It consists of the Buy-In Cost plus support costs plus a penalty cost for failures. The Figure-of-Merit Cost includes all costs that vary with redundancy.

4.2.1 Support Costs

Support costs are:

a) Weight penalty = 5.8 K$/lb for the Booster
= 16 K$/lb for the Orbiter

This penalty is uniformly distributed over the life of the shuttle. The values are based on a 445 flight program.

b) Electric energy penalty = $17/kilowatthour for Orbiter or Booster

This penalty is uniformly distributed over the life of the shuttle. The values are based on a 445 flight program.

c) Maintenance costs - These consist of repair and replacement costs and are proportional to the average number of failures per flight. It was assumed that one false-alarm removal occurs for every genuine failure. Repairs and replacements were assumed to occur at a uniform rate during the program.

d) Cost of replacing worn-out equipment. Certain LRUs were assigned a wearout life, see Table 3.

The significant factors determining support costs of each LRU type for the results reported later are shown in Table 3, along with LRU procurement costs. These values are typical and do not necessarily represent the latest estimates. They presuppose an Apollo or high reliability procurement policy. In order to assess the effects of a different procurement policy, all LRU MTBF's were reduced by 80% and all LRU costs by 50%. The impact of this "commercial parts" policy is discussed in Section 6.

4.2.2 Failure Penalty Costs

A cost penalty was assessed for failure to deliver the payload and for vehicle loss. Section 2.4 shows the four possible outcomes of a mission. A successful mission has no failure cost. The cost of re-flying a mission (outcome 2 or 4) is 3.15 million dollars (including 1% amortization, plus range support costs). The cost of a lost vehicle and crew was estimated at 120, 130, and 225 million dollars for Booster, Orbiter, and both vehicles, respectively. This penalty includes half the original cost of the vehicle, and allowances for passenger insurance, crew retraining, cargo, and investigations. No quantitative value was attached to the loss of human lives.

The expected failure cost on any flight is:

$$\text{Failure Cost} = (\text{Reflown Mission})\ (\text{Probability that Mission must be Reflown}) + (\text{Lost Vehicle Cost})\ (\text{Probability of Lost Vehicle})$$

4.3 Time Distribution of Costs

All costs incurred prior to the first operational flight are referenced to an initial time two years prior to the first operational flight. All future costs are converted into their present value at the initial time at 10% interest per annum. In order to do this, their ten-year sum is multiplied by 0.46 (an input quantity to the computer program). By varying the interest rate in the analysis, the relative weighting between initial costs and derred costs can be varied.

5.0 COMPUTER PROGRAM

The analysis approach outlined in previous sections was formalized mathematically and coded in Fortran IV for TRW's time-shared CDC-6500. The program requires about 19,000 words of core, of which 4,100 words are overlaid twice during the course of a run. It uses 15 seconds of CPU time for the Booster case; and 22 seconds for the Orbiter, with its larger number of mission phases and larger number of LRUs.

The principal inputs to a run of this program are:

- Mission phase durations
- K factors, by phase, LRU location, and LRU utilization (on or off)
- Cost penalties for
  - Reflown mission
  - Lost vehicle
  - Weight
  - Energy
- Reliability model
- Number of good safety LRUs required to continue with payload delivery
- LRU data as in Table 3
- Interest rate, for discounting future costs

The principal outputs of a computer run are:

- Buy-In and Figure-of-Merit Costs for various equipment complements
- Probabilities of the four mission outcomes
- Equipment complement that gives minimum Figure-of-Merit Cost
- Sensitivity of Figure-of-Merit Cost to certain changes in the equipment complement

6.0 RESULTS

The results show the Figure-of-Merit Cost and the Buy-In Cost for a variety of different design parameters. Figures 2 to 4 show these costs as a function of equipment redundancy levels. Varying the minimum number of safety LRUs required to continue with payload delivery, the number of vehicles, and the operating time causes little change in the shape of the curves, though the absolute level of the curves changes.

Figure 2 shows the results for the Orbiter, assuming that the vehicle starts home, without delivering its payload, when only one of a safety type remains. The curve for Apollo-quality parts shows that levels of redundancy below 3 cause a rapidly increasing penalty, due to a rapidly increasing probability of a lost vehicle and crew. However, 3 sheets, FO/FO/FS, 4 sheets, and the optimum all give about the same Figure-of-Merit Cost.

The Buy-In Cost of the optimum and of the 3 sheet designs are equal, and are about 10% cheaper than FO/FO/FS and 4 sheet designs, which also are equal. The Orbiter high-reliability optimum, while mainly a 3 sheet design, calls for 4 IMUs and 4 central computers and 2 or fewer of all mission success LRUs.

The Booster results are plotted in Figure 3 for the same conditions as Figure 2. For high reliability parts, the 3 sheet and optimum designs coincide and are 10% cheaper in Buy-In Cost than are the FO/FO/FS and 4 sheet designs, which also coincide. Three IMUs and 3 central computers are selected. Even though the optimum Booster design is slightly less redundant than the optimum Orbiter design, the probability of losing a vehicle and crew is about 3 times higher for the Orbiter (0.00014 versus 0.000043 for the Booster). These differences are a result of the effective mission duration being 27 hours for the Booster and 139 hours for the Orbiter.

If the Orbiter crew's rule is to start home without having delivered the payload when 2 sheets remain instead of when 1 sheet remains, the probability of no payload delivery increases and the probability of crew safety also increases, as shown in Figure 4. Also, the high-reliability optimum moves to a generally higher level of redundancy.

Figures 2 and 3 also plot the results when commercial reliability parts are used. The Buy-In Cost of the Orbiter's commercial reliability optimum is 50% less than its high-reliability optimum (about 70 million dollars less). This may be an attractive feature despite the Figure-of-Merit Cost being 50% worse. The Buy-In Cost of the commercial reliability optimum Booster design is also about 50% less (55 million dollars less) than its high-reliability optimum, but in addition it offers a 90 million dollar reduction in Figure-of-Merit Cost.

The sensitivities of the optimum designs to a change in one LRU at a time from the optimum redundancy level to the next best alternative were also calculated. The percent rise in the Figure-of-Merit Cost is small, the largest being about 3% (this can represent total program cost increases of 4 or 5 million dollars).

7.0 CONCLUSIONS

The results show that NASA's FO/FO/FS guideline is very close to the optimum-cost design, though deviations for certain LRUs were found to be cost effective. For some LRUs, commercial equipment may be cost effective, particularly in the Booster.

As the shuttle program progresses, it is necessary to update the values of costs and MTBF for the LRUs. It is desirable to recalculate the probabilities of success and safety from time to time and to investigate their sensitivities to redundancy, timeline and operating rules. This computer program is a tool for analyzing changes quickly, and for examining their effects on program cost.

8.0 ACKNOWLEDGEMENTS

This study was part of the Phase B Space Shuttle study performed for the McDonnell-Douglas team, under direction of the Marshall Space Flight Center. The authors wish to thank Mr. George Scism, head of Avionic Systems Engineering for Space Shuttle at McDonnell-Douglas Eastern Division who contributed significantly to this study.

Table 1. Booster Mission Phases

	Phase	Duration (Hours: Minutes)
1.	Boost	0:03. 5
2.	Separate	0:00. 06
3.	Coast to Apogee	0:01. 1
4.	Maximum Lift	0:00. 8
5.	Maximum Deceleration	0:03. 4
6.	Aerodynamic Turn	0:03. 4
7.	Glide	0:06. 7
8.	Cruise	1:32
9.	Approach	0:05
10.	Roll-out	0:01

All phases of Booster flight require transientless switching.

Table 2. Orbiter Mission Phases

	Phase	Duration (Hours: Minutes)	Criticality: Switching Transients Allowable
1.	Boost	0:03. 5	N
2.	Separate	0:00. 06	N
3.	Burn	0:03. 2	N
4.	Coast	0:36	Y
5.	Burns	0:48	N
6.	Coast	12:00	Y
7.	Rendezvous	1:15	N
8.	Dock	0:08	N
9.	Docked, Power Off	144:06	-
10.	Docked, Checkout	2:00	Y
11.	Undock and Separate	0:08	N
12.	Burns	0:27	N
13.	Coast	4:00	Y
14.	Entry	0:44	N
15.	Transition	0:01. 3	N
16.	Cruise	0:04. 6	N
17.	Approach	0:08. 4	N
18.	Land	0:05	N

Y: Yes
N: No

Table 3. LRU Data

Safety	Success	LRU Name	MTBF (KHR)	Proc*** Cost (K$)	Wt. (Lbs.)	No. of Flights To Wearout	Failure** Detection Probability
X		IMU, Gimballed	3	175.0	60.0	40 (gyros)	.95
X		Star Tracker	12	200.0	47.0	75	.99
X		Stab. Aug. Sys. Elec.	10	150.0	12.0	148*	.95
X		Horizon Sensor	20	200.0	10.0	40	.98
X		ACS/OMS Elec., Fwd.	65	7.5	10.0	148	1.0
X		ACS/OMS Elec., Aft	65	7.5	10.0	148	1.0
X		Static Press. Sensors	50	25.0	2.5	148	1.0
X		Jet Engine Throttle	20	20.0	20.0	148	1.0
X		Control Stick	20	6.3	25.0	148	1.0
X		Rudder/Brake Pdls	20	12.5	20.0	148	.95
X		Rate Gyro Package	13	80.0	4.0	80	.90
X		TVC Electronics	10	80.0	8.5	148	.95
X		Tot. Temp. + Prsr. Sensors	50	25.0	2.5	148	1.0
X		SCU	22	40.0	7.0	148	.99
X		Central Computer	1	750.0	75.0	148	.99
X		ADI (attitude Dir. Indicator)	3	100.0	11.0	100	1.0
X		ILS Receiver (GS/Loc)	40	25.0	11.0	148	.95
X		DME Receiver	40	70.0	30.0	148	.95
X		VOR Receiver	40	175.0	10.0	148	.95
X		Radar Altimeter	10	70.0	21.0	148	.95
X		UHF Transceiver	40	100.0	30.0	148	1.0
	X	Display, Sym. Generator	1	280.0	32.0	148	1.0
	X	Attitude Hand Controller	20	175.0	15.0	148	1.0
X		Accel. Pkg (Flt. Ctl)	8	100.0	1.5	148	.90
X		Keyboard	10	50.0	3.0	148	1.0
	X	Display Crt	2	120.0	34.0	40	1.0
X		INS DIU	60	50.0	5.0	148	.95
	X	Transltn Hand Ctl	20	125.0	7.0	148	1.0
	X	S-Band Ranging	20	40.0	7.0	148	1.0
	X	S-Band Transceiver	69	200.0	14.2	148	1.0

* Maximum value allowed = 445 flights/3 vehicles

** Probability that vehicle is not immediately lost if next to last LRU fails.

*** For most LRUs, repair cost was taken as 10% of procurement cost, and replacement cost was taken as 5% of procurement cost.

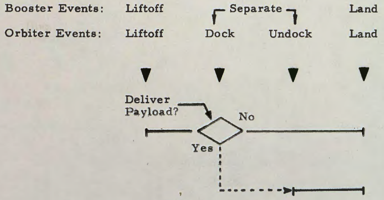

Figure 1. Mission Profile Possibilities

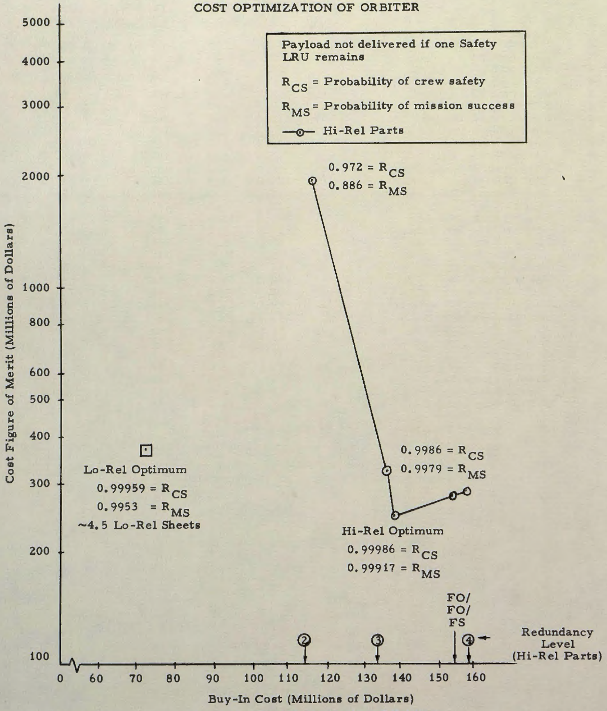

Figure 2. Cost Optimization of Orbiter

COST OPTIMIZATION OF BOOSTER

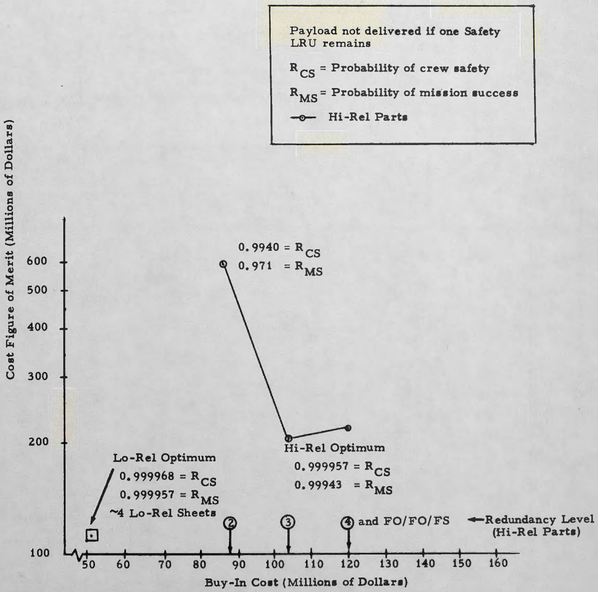

Figure 3. Cost Optimization of Booster

ORBITER OPTIMIZATION FOR GREATER SAFETY MARGIN

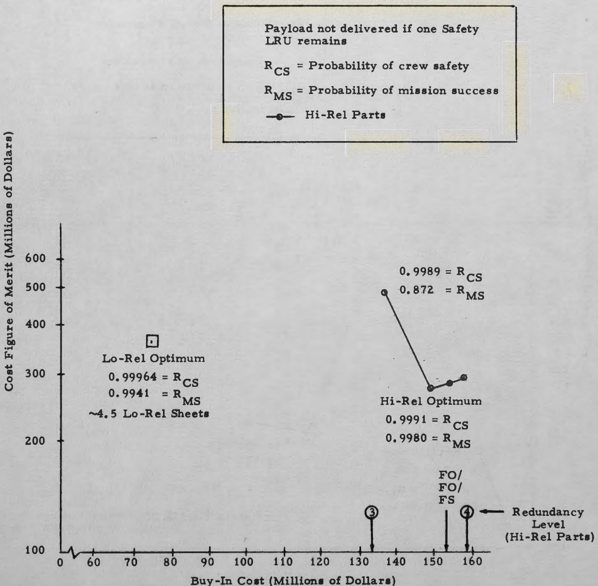

Figure 4. Orbiter Optimization for Greater Safety Margin