FINAL REPORT
PHASE II

N64-17675

300p.

ROCKET ENGINE ANALYZER AND DECISION INSTRUMENTATION (READI) INVESTIGATION

CODE-1

(NASA CR-55842)

Final Report, Phase II

OTS PRICE

XEROX $ 18.50 ph

MICROFILM $ 9.20 mf.

Prepared for

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

2 (NASA Contract No. NAS8-4003)

Prepared by

INFORMATION AND COMMUNICATIONS DIVISION
SPERRY GYROSCOPE COMPANY
Division of Sperry Rand Corporation
Great Neck, New York

NASA CR 55842

December 1963

FINAL REPORT,
PHASE II

ROCKET ENGINE ANALYZER AND DECISION INSTRUMENTATION (READI) INVESTIGATION

Prepared for

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

2 (NASA) Contract No. NAS 8-4003

Prepared by

2 INFORMATION AND COMMUNICATIONS DIVISION,
SPERRY GYROSCOPE COMPANY
2131472 Division of Sperry Rand Corporation
Great Neck, New York

ENGINEERING DEPARTMENT

E.S.Jolinea
R.L.Smith,
D.P.Blowney,
J.J. Best,
J.Harrison et al
P.G.Yiotis

cite 5
index 6

(NASA CR-53842;

OTS: $18.50 ph, $9.20 mf

~~Sperry Report No.~~ HB-9221-0035)

300p 0 refs

Copy No. 4

December 1963

ABSTRACT

17675 A

The Rocket Engine Analyzer and Decision Instrumentation (READI) concept comprises an on-board electronic system that analyzes the condition of a rocket propulsion system and, in the event of a malfunction, takes corrective action, either automatically or through the crew, in order to increase the probability of mission success and to insure the safety of the crew.

During the initial investigation, Phase I. which was conducted from February 1962 to January 1963, the following objectives were accomplished:

- The economic feasibility of the concept was demonstrated
- A design approach was developed
- The functional operation and equipment required for a typical system was investigated and a typical system was described.

Phase II of the investigation, the subject of this report, was initiated in January 1963 and was completed in January 1964. The following items were accomplished:

- An experimental READI system, designed for testing on an H-1 rocket engine, was constructed and subjected to extensive laboratory evaluation. This system incorporates a variety of transducers and signal processing techniques, as well as reliability enhancing techniques such as redundancy and self-check.
- The design procedure, which was outlined during Phase I, for defining the functional characteristics of a READI system for a

17615

particular mission-vehicle-engine complex was revised and improved. In particular, a procedure was developed for selecting the optimum system from all of the possible malfunction detection systems which could be devised.

With the completion of the experimental READI system at the end of Phase II. NASA is in a position to proceed with evaluation of the system on an operating engine. In these tests it will be possible to demonstrate that the READI system indicates correct alarms and that READI equipment failures do not cause false alarms.

The analytical studies during the second phase have re-substantiated the economic feasibility of the concept in a typical mission-vehicle-engine complex.

Author

FOREWORD

This Final Report on the Phase II investigation of the Rocket Engine Analyzer and Decision Instrumentation (READI) concept and equipment has been prepared for the National Aeronautics and Space Administration by the Information and Communications Division of the Sperry Gyroscope Company Division of Sperry Rand Corporation, Carle Place, New York, under Contract No. NAS 8-4003.

A final report covering the results of the first phase was issued in December 1962 as Sperry Report No. CA-4251-0160.

The program was initiated by Mr. H. Burlage, Office of Liquid Rockets, NASA Headquarters, Washington, D.C.

Messrs. D. Pryor and K. Chandler of the Propulsion and Vehicle Engineering Division of the Marshall Space Flight Center, Huntsville, Ala., have had technical cognizance of the program.

TABLE OF CONTENTS

Section		Page
I	INTRODUCTION	1-1
	1-1. OBJECTIVES AND GENERAL CONCEPT OF READI	1-1
	1-2. PHASE I INVESTIGATION	1-1
	1-3. OBJECTIVES OF THE PHASE II INVESTIGATION	1-2
	A. Task A	1-3
	B. Task B	1-3
	1-4. REPORT ORGANIZATION	1-3
II	SUMMARY OF READI CONCEPT AND VALUE	2-1
	2-1. READI CONCEPT	2-1
	2-2. TYPICAL APPLICATION	2-2
	2-3. PHYSICAL CONFIGURATION	2-2
	2-4. VALUE OF A READI SYSTEM	2-2
	2-5. OPTIMIZATION	2-3
	2-6. EFFECT OF VARIATION IN THE READI SYSTEM	2-5
	2-7. MISSION-VEHICLE-ENGINE DESCRIPTION	2-6
	2-8. CONCLUSIONS	2-8
III	SUMMARY OF READI DESIGN PROCEDURE	3-1
	3-1. PRELIMINARY STATEMENT OF DESIGN PROBLEM	3-1
	A. Design Problem 1	3-2
	B. Design Problem 2	3-5
	3-2. OUTLINE OF DESIGN PROCEDURE	3-14
	A. Malfunction Identification - Step 1	3-15
	B. Loss Computation - Step 2	3-18
	C. System Synthesis - Step 3	3-19
IV	DEVELOPMENT OF SYSTEM DESIGN TECHNIQUE	4-1
	4-1. INTRODUCTION	4-1
	4-2. MATHEMATICAL MODELS	4-2
	A. Mission Model	4-2
	B. Propulsion System and Vehicle Models	4-7
	C. Determination of Transition Probabilities for Malfunction Decision Pairs	4-13
	D. The READI Model	4-16
	4-3. COMPUTATION OF RISK	4-22
	4-4. DIGITAL COMPUTER COMPUTATION OF RISK	4-27
	4-5. SYSTEM SYNTHESIS PROCEDURE	4-30
	A. Introduction	4-30
	B. Preliminary Development	4-32
	C. Development of the Initial Include and Exclude Criteria	4-37

TABLE OF CONTENTS - Continued

Section			Page
IV		D. Iteration Procedure	4-40
	4-6.	SYMBOL LIST FOR SECTION IV	4-43
V	DEVELOPMENT OF EQUIPMENT		5-1
	5-1.	OBJECTIVES	5-1
	5-2.	SYSTEM COMPONENTS	5-1
		A. Introduction	5-1
		B. Transducer Requirements	5-2
		C. Functional Requirements of Processing Circuits	5-6
		D. Logic Circuits	5-14
		E. Packaging Requirements	5-17
	5-3.	DEVELOPMENT OF EXPERIMENTAL SYSTEM	5-19
		A. Introduction	5-19
		B. Malfunction Detection	5-19
		C. Self-Check and Redundancy Provisions	5-25
		D. Decision Rules	5-26
		E. Circuitry	5-31
		F. Equipment Configuration	5-33
	5-4.	SYSTEM LABORATORY TEST	5-36
		A. Objectives	5-36
		B. Description of System Test	5-36
		C. Test Equipment	5-37
		D. Transducer Signal Simulator	5-38
	5-5.	PRELIMINARY ENGINE TEST PLAN FOR EXPERIMENTAL SYSTEM	5-40
		A. Test Objectives	5-40
		B. Test Techniques	5-40
		C. Test Procedure	5-40
		D. Engine Test Stand Installation	5-45
VI	CONCLUSION AND RECOMMENDATIONS		6-1

CONTENTS - Continued

Appendix		Page
A	RISK CALCULATION FOR STAGE END STATE	A-1
B	MAPPING OF ENGINE FAILURE EFFECTS	B-1
C	DIGITAL COMPUTER PROGRAMS	C-1
D	PROPULSION SYSTEM DATA USED IN DESIGN AND EVALUATION OF READI SYSTEMS	D-1
E	CATALOG OF SIGNAL SPACE SEPARATIONS FOR H-1 ENGINE	E-1
F	EXPERIMENTAL SYSTEM LAB TEST PROCEDURE	F-1

LIST OF ILLUSTRATIONS

Figure		After Page
2-1	READI Simplified Block Diagram	2-2
2-2	READI Interface With Vehicle and Stage Subsystems for Typical Multi-Engine Stage	2-2
2-3	Typical READI Function Diagram	2-2
2-4	Second Stage 5-Engine READI	2-2
2-5	Mission and Crew Survival Reliability	2-4
2-6	READI Evaluation Criterion	2-4
2-7	Economic Feasibility of Typical READI for 3-Stage Launch Vehicle	2-4
2-8	Trail Systems Effectiveness vs Cost (Second Stage-EOC Phase)	2-6
2-9	Comparative Value of Optimum System	2-6
2-10	Sensitivity of Risk Reduction to Transducer Failure Rate λ_T (With Self-Check and Information Redundancy)	2-6
3-1	Risk Calculation With READI	3-4
3-2	Risk Calculation With No READI	3-4
3-3	Venn Diagram of Design Problem	3-8
3-4	READI Design Procedure	3-16
3-5	Part of Failure Effect Tree for F-1	3-16
3-6	Fuel Pump Discharge Pressure for Various Malfunctions	3-16
3-7	Emergency Mode Analysis (5-Engine Stage)	3-18
3-8	Computation of Losses	3-18
3-9	Final Effects Computation	3-20
3-10	Loss Vector Computation	3-20
4-1	Structure of Mission Model	4-2
4-2	Typical Phase Model	4-2
4-3	Construction of Stage Model	4-4
4-4	Construction of Stage Model (Non-Normal Initial Condition)	4-6

LIST OF ILLUSTRATIONS (Cont)

Figure		After Page
4-5	Treatment of Mission Terminating Nodes	4-6
4-6	Overall Mission Model	4-6
4-7	Computation of Risk at R (1, 2)	4-8
4-8	Portion of Malfunctions Effects Tree	4-8
4-9	Malfunction Effects Tree	4-10
4-10	Complete Set of Signal Space Separation for Model Propulsion System	4-12
4-11	Cost Model	4-22
4-12	General Flow Chart - Risk Computation	4-30
4-13	Simplified Flow Diagram System Synthesis Procedure	4-31
4-14	Possible Effects of Adding $V_n + 1$ to V1 + V2	4-36
4-15	Example of Transducer or Group	4-40
5-1	READI Simplified Block Diagram	5-2
5-2	Reliability Trends for Integrated and Conventional Circuits	5-8
5-3	Processing Circuit Level D-C Input (Temperature)	5-10
5-4	Processing Circuit Frequency Input (RPM)	5-12
5-5	Frequency-To-Analog Converter TG101	5-12
5-6	Processing Circuit Frequency-Amplitude Input (Vibration)	5-12
5-7	Processing Circuit - A-C Input (Pressure)	5-12
5-8	Low Level Comparator, Schematic Diagram	5-14
5-9	Micrologic Elements	5-14
5-10	Logic Flow and Circuit Diagram	5-14
5-11	Four Stage Counter	5-16
5-12	Time Delay Circuit	5-16
5-13	Sample Pages From Detection Techniques Catalog	5-20
5-14	H-1A Engine Schematic Diagram	5-20
5-15	Signal Processing Diagram for H-1 Rocket Engine	5-32
5-16	Turbopump Signal Processing Circuit, A5 (V9.1)	5-32
5-17	Main Chamber Vibration Signal Processing Circuit	5-32
5-18	Turbine Speed Signal Processing Circuit N5 (V2.1, V2.2)	5-32
5-19	Gas Generator Thermocouple Signal Processing Circuit T6 (V3.1, V14.1.1)	5-32
5-20	Main Chamber Pressure Signal Processing Circuit, P1 (V2-1)	5-32

LIST OF ILLUSTRATIONS (Cont)

Figure		After Page
5-21	Low Flow Signal Processing Circuit Q12 (V7.1)	5-32
5-22	Lox Injector Pressure Signal Processing Circuit, P7-P1 (V5.1, V7.1)	5-32
5-23	Fuel Injector Pressure Signal Processing Circuit, P8-P1 (V5.1, V8.1)	5-32
5-24	Fuel Flow Signal Processing Circuit Q11 and P8-P1 (V8.1)	5-32
5-25	Gear Case Pressure Signal Processing Circuit, P4 (V15-1)	5-32
5-26	Blast Pressure Signal Processing Circuit, dPs/dt	5-32
5-27	Turbine Exhaust Pressure Signal Processing Circuit, P5 (V14.1)	5-32
5-28	Heat Exchange Exit Thermocouple Signal Processing Circuit, T10 (V14.1)	5-32
5-29	Low Level Comparator C101	5-32
5-30	Decision Logic Circuit Diagram	5-32
5-31	Typical Pressure Transducers Used in Experimental READI	5-34
5-32	Velocity-Type Vibration Transducer	5-34
5-33	V-Logic Module	5-34
5-34	Four-Stage Counter Module	5-34
5-35	Blast Pressure (dPs/dt) Signal Processing Module	5-34
5-36	Lox Injector Pressure, P7-P1, Signal Processing Module	5-34
5-37	Electronic Chassis Assembly for Experimental READI	5-34
5-38	Electronic Chassis Wiring for Experimental READI, Bottom View	5-34
5-39	Electronic Unit for Experimental READI - Reinforced, Pressurized Case Design	5-34
5-40	System Test Block Diagram	5-38
5-41	Thirty-Channel Binary Event Recorder, Sanborn Model 361	5-38
5-42	Transducer Simulator (Hinged Cover Removed)	5-40
5-43	System Junction Box (Closed)	5-45
5-44	System Junction Box - Open View of Terminal Board Panel	5-45
5-45	Engine Test Set-Up for READI Evaluation	5-45
5-46	Electronic Assembly Unit for Experimental READI, Outline Drawing	5-45
5-47	System Junction Box, Outline Drawing	5-45

LIST OF ILLUSTRATIONS (Cont)

Figure		After Page
B-1	Stage Velocity Characteristics	B-2
B-2	Propulsion System Failure Mode Parameters	B-3
B-3	Transition Probabilities as a Function of Thrust and Propellant Flow Losses	B-8
C-1	Flow Chart Failure Event Routine Enumeration	C-2
C-2	Main Routine	C-4
C-3	Subroutine Risk	C-4
C-4	Sample Output of the Risk Computation Routine	C-5
D-1	READI Model Engine, Fluid Schematic	D-2
D-2	READI Model Engine, Electrical Schematic	D-2
D-3	Malfunction Detection Chart	D-10
D-4	Programmed Decisions - All Systems	D-10
D-5	Overall Mission Model	D-10
F-1	Signal Sensitivity of Vibration Transducer (Velocity Pickup Type)	F-2
F-2	Signal Sensitivity for Turbine Speed (N5)	F-2
F-3	Signal Sensitivities for Lox and Fuel Flow	F-2

LIST OF TABLES

Table		Page
3-1	Assigned Losses - Design Problem No. 1	3-2
3-2	Effect of Transducer Redundancy on Error Probability - Design Problem No. 1	3-4
3-3	Effect of Transducer Redundancy on Risk - Design Problem No. 1	3-4
3-4	Malfunction Probabilities - Design Problem No. 2	3-5
3-5	Assigned Losses - Design Problem No. 2	3-5
3-6	Malfunction Detector Coverage - Design No. 2	3-6
3-7	Summary of Example Design Problem	3-11
4-1	Phase Transitions	4-5
4-2	Definition of Transition Probabilities	4-14
4-3	Development of Transition Probabilities	4-15
4-4	Development of Doubly Redundant Sensors Representation	4-19
4-5	Definition of Terms $P(m_{i;\ q,p}{}^{S}{}_{L;\ q,p})$	4-23
4-6	Probability of Propulsion System Malfunction and System Failure Events $P(m_{i;\ q,p}{}^{S}{}_{L;\ q,p})$	4-24
4-7	Definition of Risk Components	4-28
5-1	Comparison of Transducer Requirements for Ground Test and Telemetry and READI Applications	5-3
5-2	Transducer Signal Groups	5-5
5-3	Key to Symbols Used in Subsequent Tables and Text	5-21
5-4	H-1 READI Programmed Decisions for 8-Engine Cluster	5-30
5-5	Multiengine Failure Probabilities	5-31
5-6	Experimental H-1 READI System Transducers	5-42
5-7	Experimental READI System Evaluation, H-1 Engine Test, Engine Malfunction Test Program	5-43
B-1	Symbols	B-8
C-1	FORTRAN Symbols - Tracer Routine	C-2
C-2	Subroutine Symbols	C-5
D-1	Pressure Budget Model Engine at 100-Percent Thrust	D-2
D-2	Failure Probability Data by Major Subsystem	D-4

LIST OF TABLES - Continued

Table		Page
D-3	READI Model Engine Malfunction Summary	D-5
D-4	Propulsion System Loss Data for Mission Phase 4 (Prime Mission Engine-Out Capability to Cut-Off)	D-8
D-5	Transducer Characteristics	D-9
D-6	Transition Probabilities	D-11
D-7	Mission and Crew Survival Reliabilities	D-11
F-1	Non-Alarm Simulator Settings	F-2

SECTION I

INTRODUCTION

1-1. OBJECTIVES AND GENERAL CONCEPT OF READI

The function of READI is to sense abnormal operation of rocket engine propulsion systems and take remedial action. The end objective is to improve the likelihood of accomplishing mission objectives, including the safe return of the crew on manned flights. For the purposes of this study, the propulsion system is considered to include the rocket engine itself, and the associated pumps, controls, tankage, tankage pressurization system, and thrust vector actuation means.

READI is primarily an on-board system that will sense signals from the propulsion system directly. However, it will also exchange information with other equipment, such as the guidance and control system, propellant utilization system, telemetry system, ground checkout system, and other associated systems. On manned missions, some READI decisions will be made by the crew on the basis of appropriate READI displays.

In addition to the remedial action commands that READI supplies to the engine, it may also provide command inputs to the engine for in-flight testing, for checkout of parts of the propulsion system prior to use, or for double-checking a malfunction indication while the engine is operating. On longer missions for which an in-flight repair capability exists, READI will localize and indicate the required repair operation.

1-2. PHASE I INVESTIGATION

The first phase of the READI investigation was undertaken in February 1962 and was completed in January 1963. This phase was devoted primarily to developing and evaluating the READI concepts. The evaluation was divided into three main areas:

- Determination of economic feasibility
- Development of a design approach
- Familiarization with the functional operation, and equipment required for a typical system.

An equipment configuration was described in the final report* for the propulsion system of a five-engine cryogenic second stage. It consisted of 130 sensors, several of which were redundant, together with signal processing and logical elements to select the best alternate action for a given malfunction and status of the mission. Both parallel and sequential computing techniques were used to achieve maximum flexibility and reliability. Special reliability techniques, such as transducer self-check and redundancy, were incorporated to achieve the functional and reliability requirements determined by the design procedure.

These design and equipment approaches were then applied to a representative mission-vehicle-engine combination. The results indicate that the application of the READI concept to launch vehicles offers a substantial potential return in reduction of mission risk.

1-3. OBJECTIVES OF THE PHASE II INVESTIGATION

The second phase of the READI investigation was undertaken in January 1963. The primary objectives were to apply the system design techniques developed in Phase I, and to show in detail how a system would be implemented to achieve the desired reliability and flexibility for application to present and future rocket engines. These broad objectives have been divided into two tasks:

- Task A - Equipment Development
- Task B - Application Investigation.

- - - - - - -

*Details of Phase I are in Final Report, Phase I, Rocket Engine Analyzer and Decision Instrumentation (READI) Investigation, Vol. I and II, furnished by Sperry Gyroscope Company to National Aeronautics and Space Administration under Contract No. NAS 8-4003.

A. TASK A

Task A, which represented about 65 percent of the Phase II program funding, involved the following activities:

- Functional design of an experimental system for ultimate test on a rocket engine during a series of hot-firing engine tests. The primary task was the compilation of a set of malfunction indicators, the selection of transducers, the definition of signal processing requirements and alternative actions to be taken for each malfunction indication
- Detailed investigation of circuitry required to accomplish signal processing, self-check, and decision operations
- Design and construction of the experimental system, followed by a laboratory demonstration of the functional and reliability aspects of the system
- Preparation of a preliminary engine test plan for evaluation of the experimental system on the selected engine.

B. TASK B

Task B, a continuation of the analytical portion of the investigation, included the following activities:

- Re-appraisal of the models used in the design and evaluation of READI systems
- Development of an effective analytical approach for evaluating overlapping engine-condition indicators, such as low thrust or low chamber pressure, which can result from a number of malfunctions
- Development of an improved digital computer procedure for optimizing the design of a READI system.

1-4. REPORT ORGANIZATION

Section II of this report contains a brief description of the READI concept and discusses the value of READI to a typical mission/vehicle complex. Section III contains a summary of the READI design procedure illustrated with some simple examples. Section IV presents the details of the design procedure as it would be applied to the design of actual

READI equipment for an actual mission/vehicle complex. Section V discusses the results of the equipment development and presents the detailed design of the system developed for use on the hot-firing tests of the H-1 engine early in 1964.

Section VI presents the conclusions and recommendations for continuing investigation, development, and test of the READI concept and equipment. The appendices contain detailed information on calculations performed and procedures employed in the READI investigation.

SECTION II

SUMMARY OF READI CONCEPT AND VALUE

2-1. READI CONCEPT

The Rocket Engine Analyzer and Decision Instrumentation concept (READI) is an on-board system for application to rocket propulsion systems. Its function is to detect malfunctions of the rocket propulsion system during operation and to initiate the proper remedial action in case such a malfunction is detected. The end objective is to improve the probability of accomplishing the mission objectives, including the safe return of the crew in the case of manned flight.

A simplified block diagram of an example READI system is shown in figure 2-1. For the purposes of READI, the propulsion system for a particular stage is taken to include the engines, tankage, pressurization system, and the thrust vector control. Each of these systems is monitored by a number of transducers. Possible transducers include chamber vibration transducers, explosion detectors, flow meters, valve position indicators, and pressure indicators. The output of each transducer employed is processed by an associated signal conditioning circuit which normalizes the form and magnitude of the transducer output. Each of these voltages is converted to a discrete 0, 1 form by comparison with stored references, and these discrete signals are then processed by the remedial action logic. In addition to examining the discrete signals, the remedial action logic also examines certain conditioning signals, as shown in figure 2-1. If a propulsion system malfunction is indicated, the remedial action logic selects the proper remedial action. The remedial action selected is either indicated to the crew via a suitable display or, in those cases where time does not permit crew participation, is initiated immediately via existing engine control elements.

2-2. TYPICAL APPLICATION

The subsystems monitored by a READI system in a typical five-engine stage of a launch vehicle are shown in figure 2-2. Also shown in this figure are the signals monitored from each subsystem, and the output interface through which remedial actions is initiated.

Some typical malfunctions and remedial actions that could be taken are shown in figure 2-3. These remedial actions are designed either to restore a failed function, to draw upon redundant capability, or simply to limit the consequences of the malfunction.

For example, combustion instability at ignition may be cured in some engines by simply shutting down the engine and going through a re-start cycle. Shutdown alone may be adequate for the same malfunction near stage cut-off, since the required stage velocity increment may be achieved with one engine out by burning the residual propellants in the other engines.

If the combustion instability cannot be cured, and engine-out capability is not available, the appropriate READI action would be to shut down all engines and initiate the abort sequence. This would limit the consequences of the malfunction to the loss of the mission and allow the crew to make a safe abort. The READI remedial action or decision logic will automatically consider mission status inputs, such as time-to-go, in arriving at the most appropriate decision as shown in figure 2-3.

2-3. PHYSICAL CONFIGURATION

Physically, READI will comprise sets of transducers and a number of electronic packages as illustrated in figure 2-4. Multi-engine stages will have one signal processing unit on each of the five engines, plus a central unit that receives the common inputs from the vehicle and coordinates the five engine units. Single engine stages will require only one signal processing unit.

2-4. VALUE OF A READI SYSTEM

Two familiar indices of performance which are good measures of the value of READI are:

- The likelihood of mission accomplishment, or mission reliability
- The likelihood of safe return of the crew, or crew survival reliability.

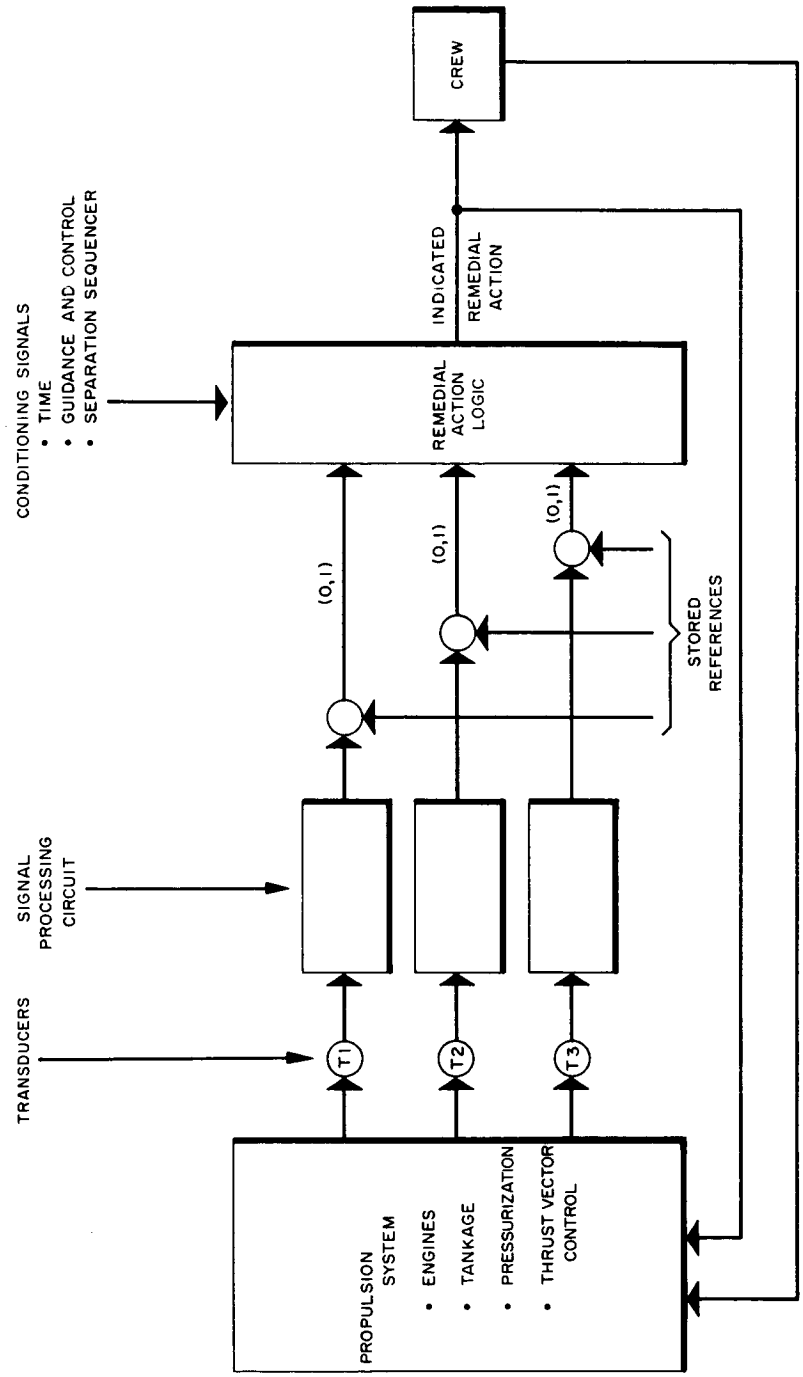


FIGURE 2-1. READI SIMPLIFIED BLOCK DIAGRAM

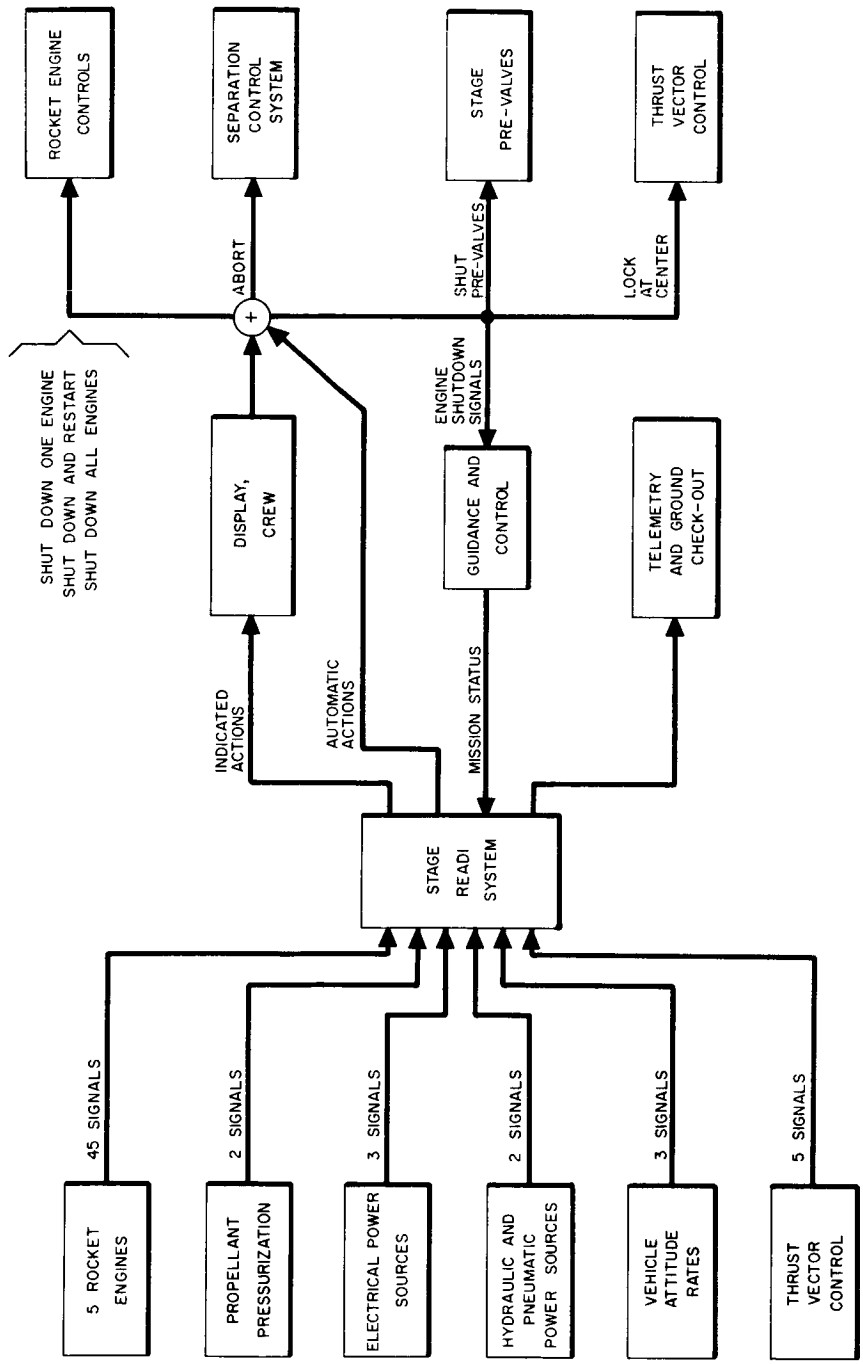


FIGURE 2-2.
READI INTERFACE WITH VEHICLE AND
STAGE SUBSYSTEMS FOR TYPICAL MULTI-ENGINE STAGE

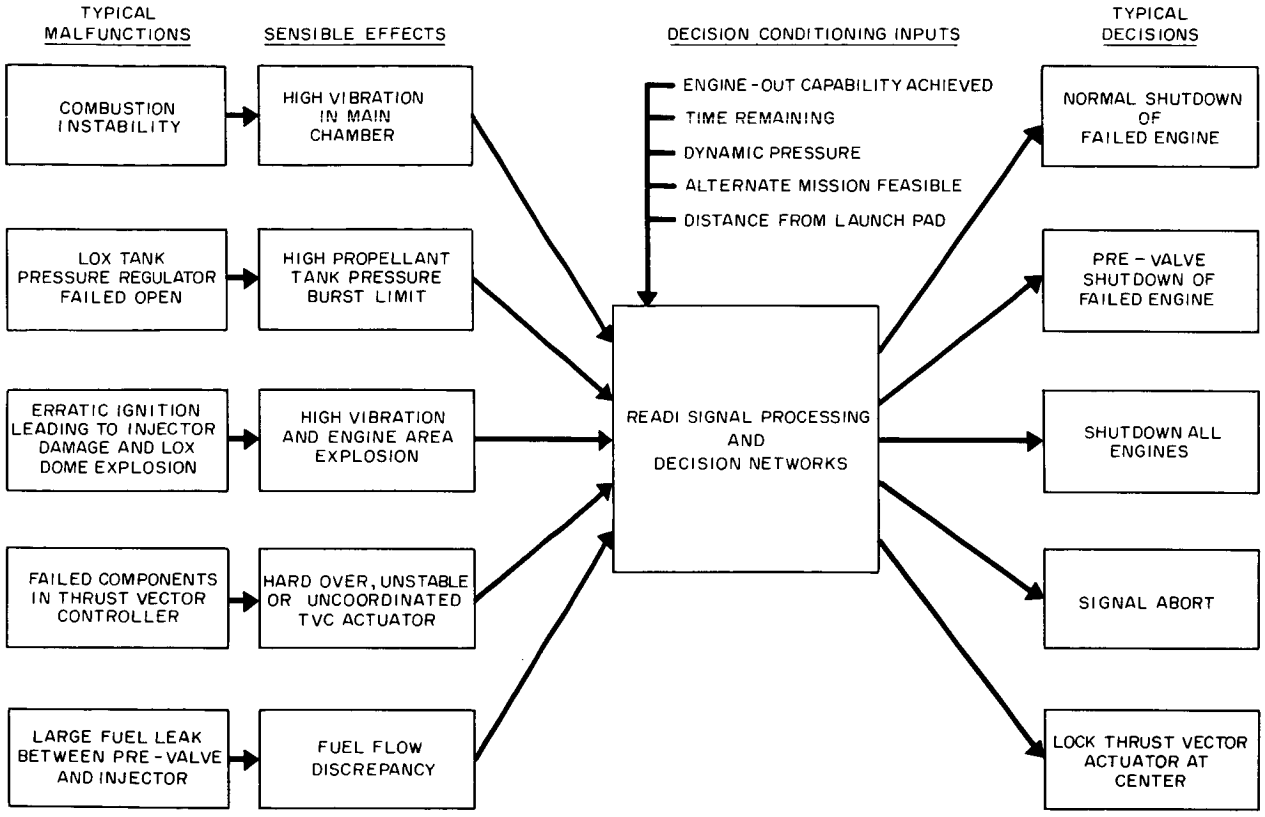


FIGURE 2-3
TYPICAL READI FUNCTION DIAGRAM

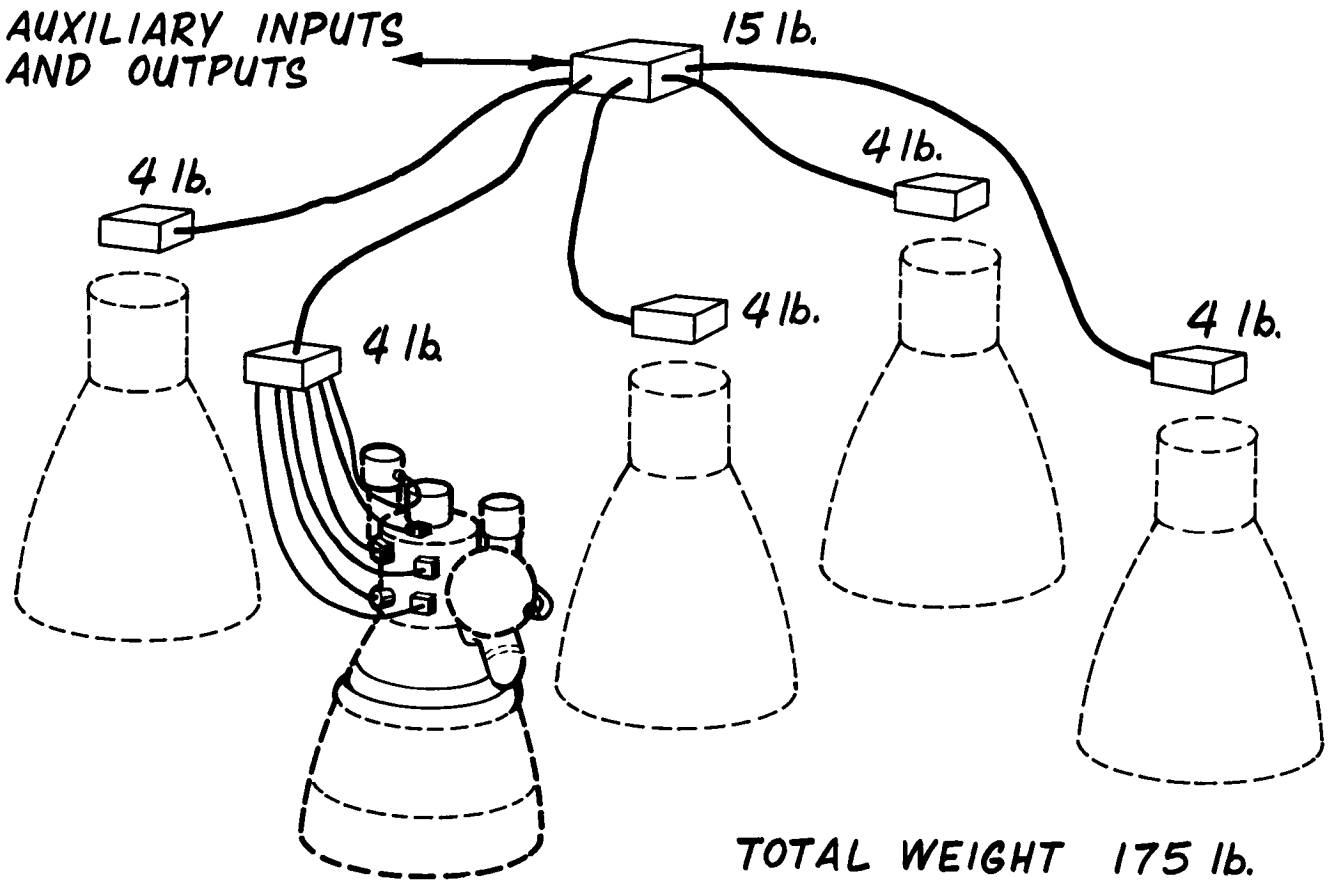


FIGURE 2-4
SECOND STAGE 5-ENGINE READI

Figure 2-5 shows the results obtained when a well-designed READI system is applied in each of the first three stages of a typical large launch vehicle, compared to the same vehicle without READI. It will be noted that there is an increase both in the crew survival reliability (from 0.947 to 0.986) and in the mission reliability (from 0.883 to 0.927). The design of READI can be optimized to emphasize different degrees of crew safety versus mission reliability. As indicated in figure 2-5, when the trade-off is properly executed both factors can be increased. The increase in crew survival reliability results from the ability of READI to shut down an engine, or engines, and initiate abort when necessary to save the crew. The increase in mission reliability comes about from the ability of the READI system to capitalize on the alternative capabilities which are inherent in the launch vehicle stages.

An appreciation of the value of READI can be gained by noting that it would require a 4 to 1 reduction in the basic engine failure rate to achieve the same increase in crew survival reliability that the READI system contributes.

The launch vehicle model used for these analyses is similar in many respects to Saturn V. and the assumed mission is a lunar injection operation. A brief description of the mission-vehicle-engine models used is presented in paragraph 2-7.

2-5. OPTIMIZATION

For system optimization purposes the use of mission reliability or crew safety is inconvenient. These two indices must be combined into one and expressed in a dimension that can be traded off against the equipment complexity required to achieve the desired reduction in risk to crew and risk to mission.

In general, the more READI equipment that is used the greater will be the reduction in risk; however, the rate of return will be reduced drastically beyond some point. The optimum system will be the one for which a more comprehensive system is not justified by the risk reduction achieved. Equipment complexity and risk reductions can be given the same dimensions by assigning an equivalent cost to the equipment and expressing risk in terms of the reduction in average cost of performing the mission.

To establish the functional characteristics of the optimum READI system, the total cost of performing a mission may be divided into two

components: the fixed cost of the vehicle (the launch costs, the prorated development*, etc), and an element which reflects the risk to crew and mission, as shown in figure 2-6. The crew risk can be weighted by a factor λ_c that accounts for its importance relative to the mission in making the READI design trade-off. Thus risk equals the value of the mission (takes as unity) times the sum of the probability of mission loss, and λ_c times the probability of crew loss.

$$\left[\text{Risk} = 1 \quad P(\text{Mission Loss}) + \lambda_c \quad P(\text{Crew Loss})\right]$$

Combining of crew and mission considerations is utilized, however, only after some established minimum level of crew survival reliability has been achieved. The concept of combined risk is discussed in more detail in Appendix A.

The objective of READI is to increase the likelihood of successful mission accomplishment and safe return of the crew. Re-stated in terms of the above defined index of performance, the objective is to reduce the risk component of the average cost in figure 2-6.

To perform a cost trade-off, the risk to crew and mission has been computed with and without READI in each stage of a 3-stage vehicle. The risks are 0.21 with READI and 0.62 without READI. The fixed launch cost is taken as 30 million dollars per vehicle, assuming a 20-vehicle development and launch operation. Figure 2-7 shows the economic trade-off with and without READI in all three stages for a crew-to-mission value ratio, λ_c, of 10. A significant net saving of 32 million dollars is possible. This exceeds the fixed launch cost of the vehicle. The total cost of READI is about $700,000 for the three stages.

The λ_c trade-off factor was set at 10 for purposes of optimizing the design of the READI systems in the three stages of the launch vehicle. This trade-off resulted in READI systems which increased both crew survival and mission reliabilities. Even with a λ_c of zero, however, which corresponds to an unmanned mission, the decrease in mission risk alone exceeds the cost of READI. and the use of the system is justified.

- - - - - - -

*The fixed cost was taken to include negative aspects of READI, including not only the hardware cost, but the weight penalty, developmental cost and maintenance costs.

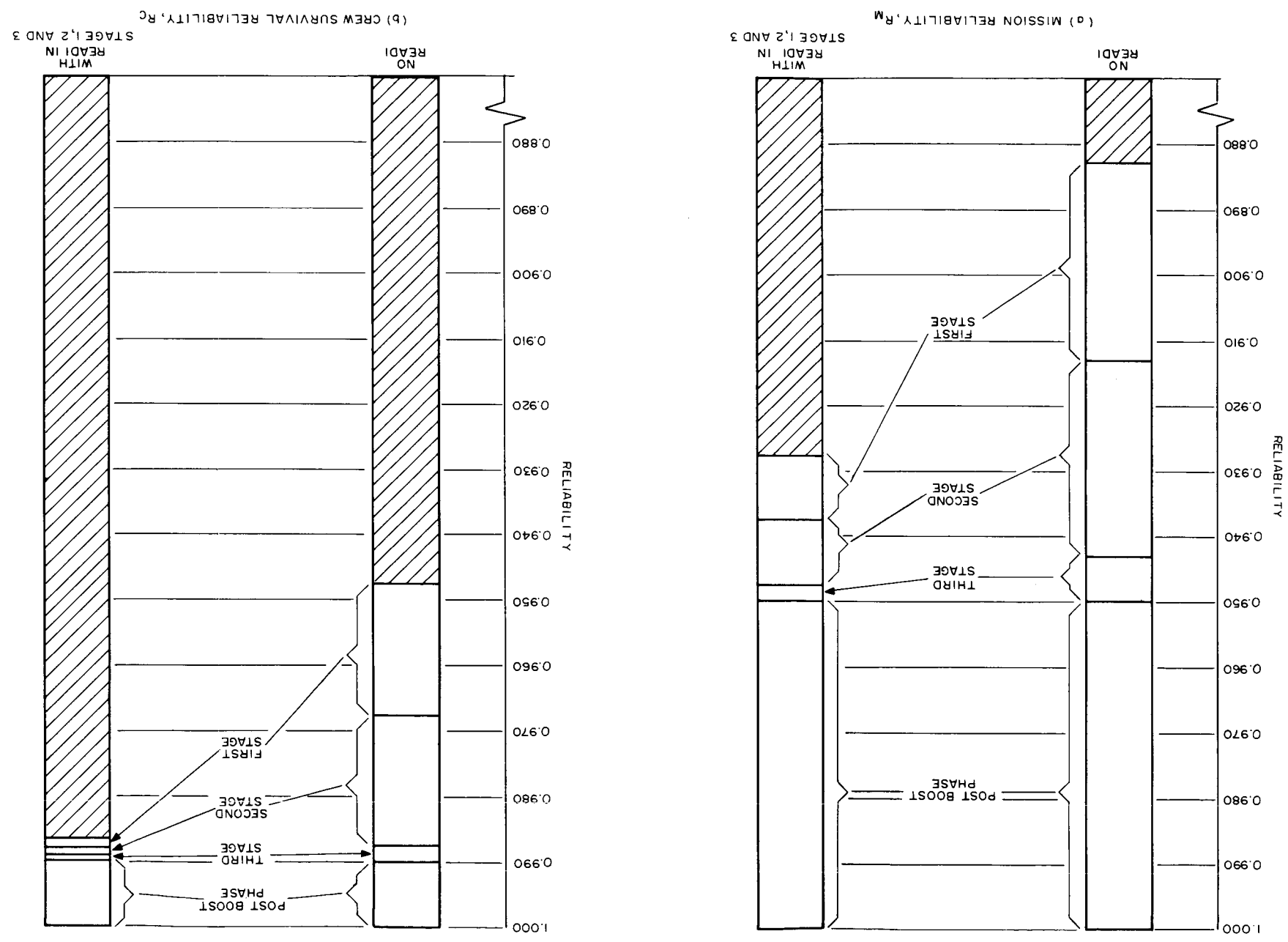


FIGURE 2-5
MISSION AND CREW SURVIVAL RELIABILITY

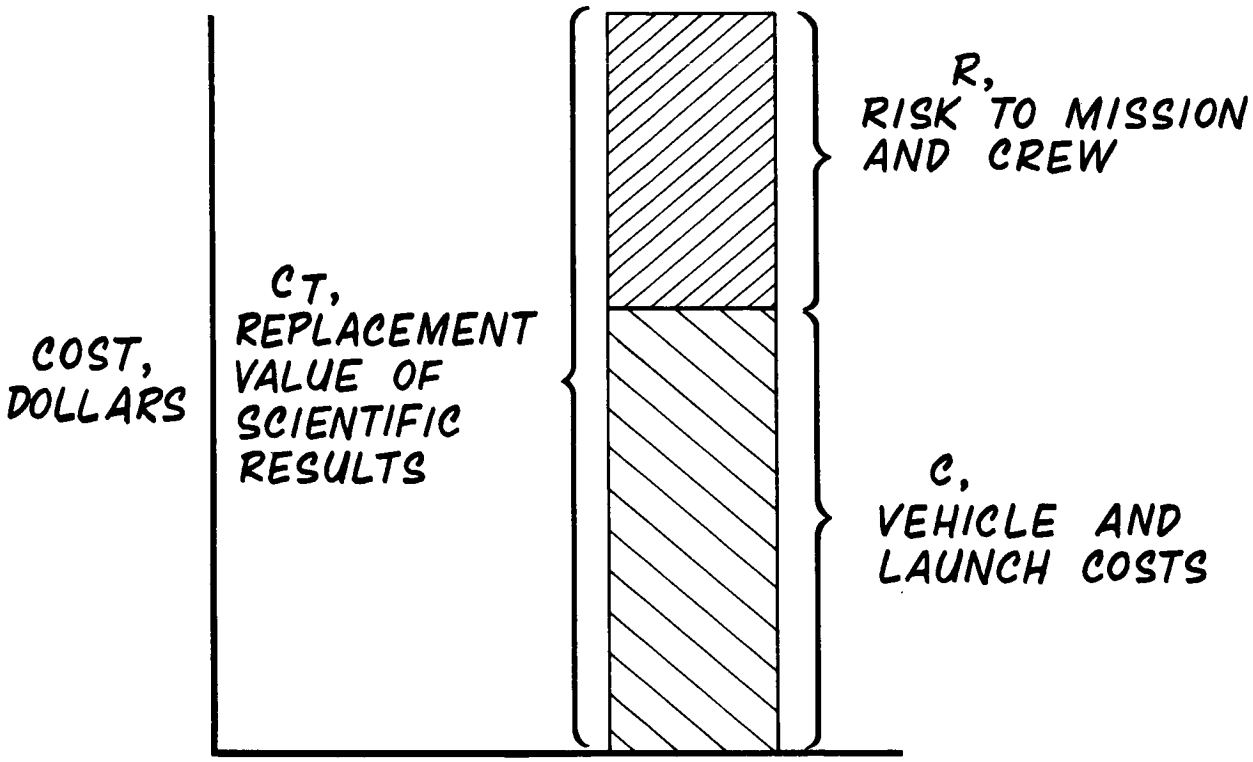


FIGURE 2-6
READI EVALUATION CRITERION

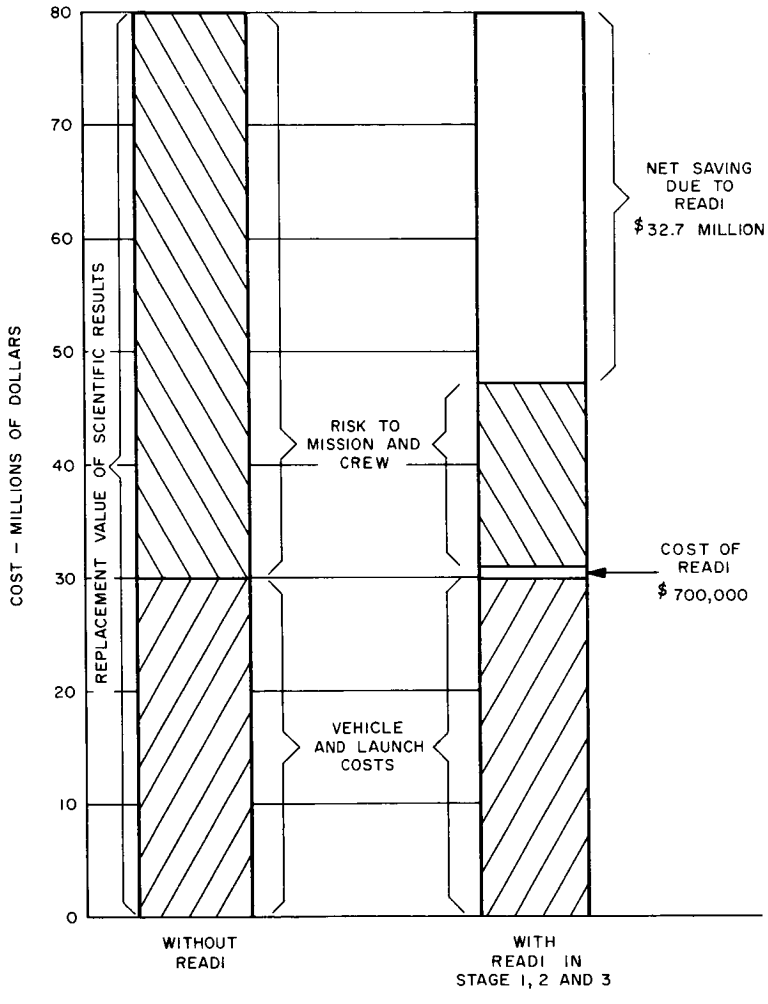


FIGURE 2-7
ECONOMIC FEASIBILITY OF TYPICAL
READI FOR 3-STAGE LAUNCH VEHICLE

2-6. EFFECT OF VARIATION IN THE READI SYSTEM

The READI systems implied in figures 2-2 and 2-5, which indicated the advantages of READI, are optimum systems, their functional performance having been defined by the results of a synthesis procedure. This procedure is described in Section III and is derived in detail in Section IV.

Briefly, the synthesis procedure identifies the optimum system from all of the possible systems which might be devised for a given application.

The technique used to identify the optimum system utilizes a set of testing criteria which eliminate trial systems from consideration by proving that the optimum system must contain certain combinations of transducers. The technique does not, except in trivial cases, pinpoint the optimum system. It does, however, reduce the number of combinations to a small group of systems which are then subjected to a more exhaustive evaluation using a digital computer. The selection of the optimum system, No. 6, from a group of 10 systems in a typical final evaluation is shown in figure 2-8. This optimization was performed for a phase of second stage engine operation which accounted for about 40 percent of the unreliability of the engines. The optimum system for this phase uses six transducers per engine and costs about $210,000, half of which is a developmental cost prorated over 20 vehicles. The best system for the whole second stage burning period uses about 9 transducers per engine and monitors an additional 8 signals from the stage. The cost of this system is approximately $300,000.

The vertical scale of figure 2-8, risk factor, is the difference between the total risk for that system and risk which would be obtained if no malfunction had occurred during the interval of engine operation being considered.

The optimum system in figure 2-8 has associated with it a risk factor of 0.0104. This can be partitioned into categories which identify, in a meaningful manner, sources of risk factor. The bar graph of figure 2-9 shows this breakdown. A comparison is made with the risks for no READI, a very simple READI design which would monitor only combustion instability and shut down when it occurred, and the perfect READI which monitors all malfunctions and always takes the proper remedial action.

Several observations may be made regarding figures 2-8 and 2-9:

- Since the systems shown in figure 2-8 result from an initial screening process all are fairly good. However, on a cost basis, the final selection is certainly worth the analytical effort.
- It is possible to make the READI system too simple, as shown by the high risk factor associated with the "Simple System."
- The risk increment due to unreliability in READI equipment is relatively small because the optimum READI system makes extensive use of information redundancy and self-check methods. As shown in figure 2-10, a 10 to 1 increase in the assumed average transducer failure rate does not noticeably degrade the effectiveness of the system.

2-7. MISSION-VEHICLE-ENGINE DESCRIPTION

The value of READI in decreasing the risk of a launch operation depends on the nature of the particular mission, vehicle and engines, and the cost and reliability of the READI equipment components. For the purpose of illustrating the net worth of READI. certain mission, vehicle and engine characteristics have been defined. As far as possible these characteristics have been chosen to be consistent with present and near-future launch vehicle systems. A brief description of the salient features of the propulsion system, vehicle and mission used in the READI design study previously described is presented here. A more detailed description is given in Appendix D.

The assumed failure characteristics of the engine are equivalent to a relatively mature engine with a total failure rate of about 0.01 per mission. With no remedial action, this rate would be distributed among four failure categories as follows:

(1)	Failure to start	10×10^{-4}
(2)	Premature safe shutdown	20×10^{-4}
(3)	Explosion	40×10^{-4}
(4)	Severe off-design operation	30×10^{-4}.

The ability of READI to affect risk reduction is a strong function of the availability of remedial actions that can be taken should a malfunction occur. The available remedial actions are assumed to be:

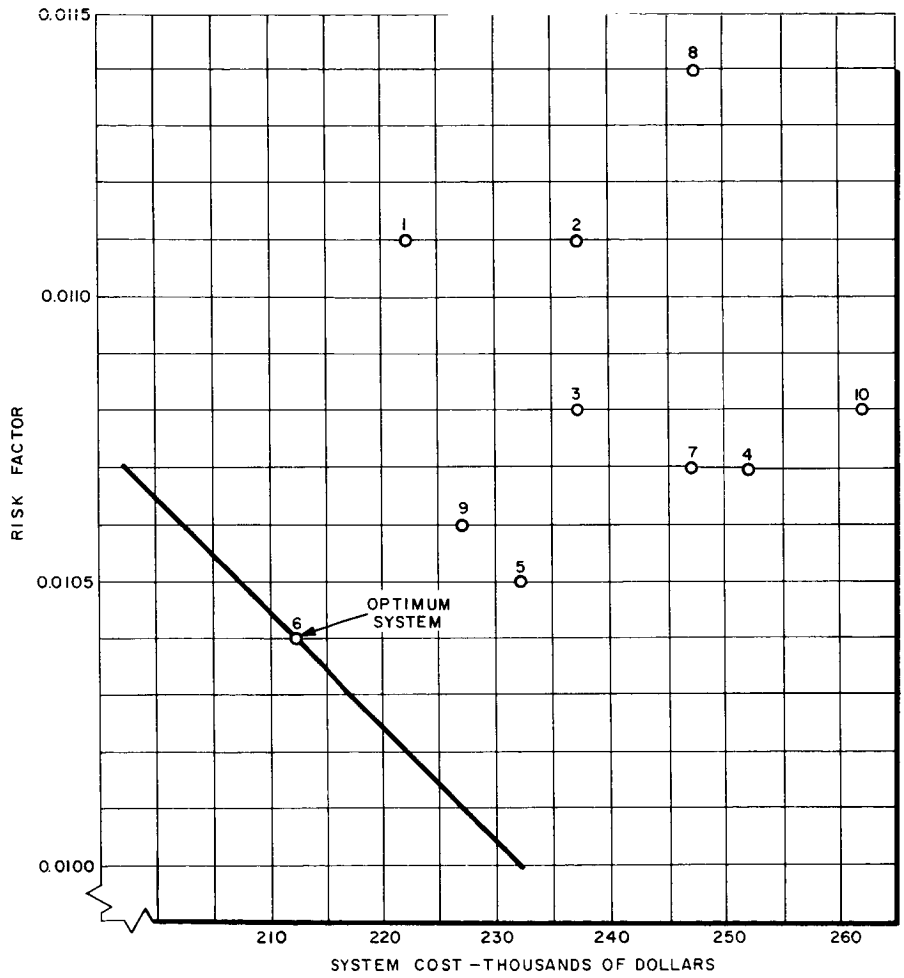


FIGURE 2-8
TRIAL SYSTEMS EFFECTIVENESS VS COST (SECOND STAGE-EOC PHASE)

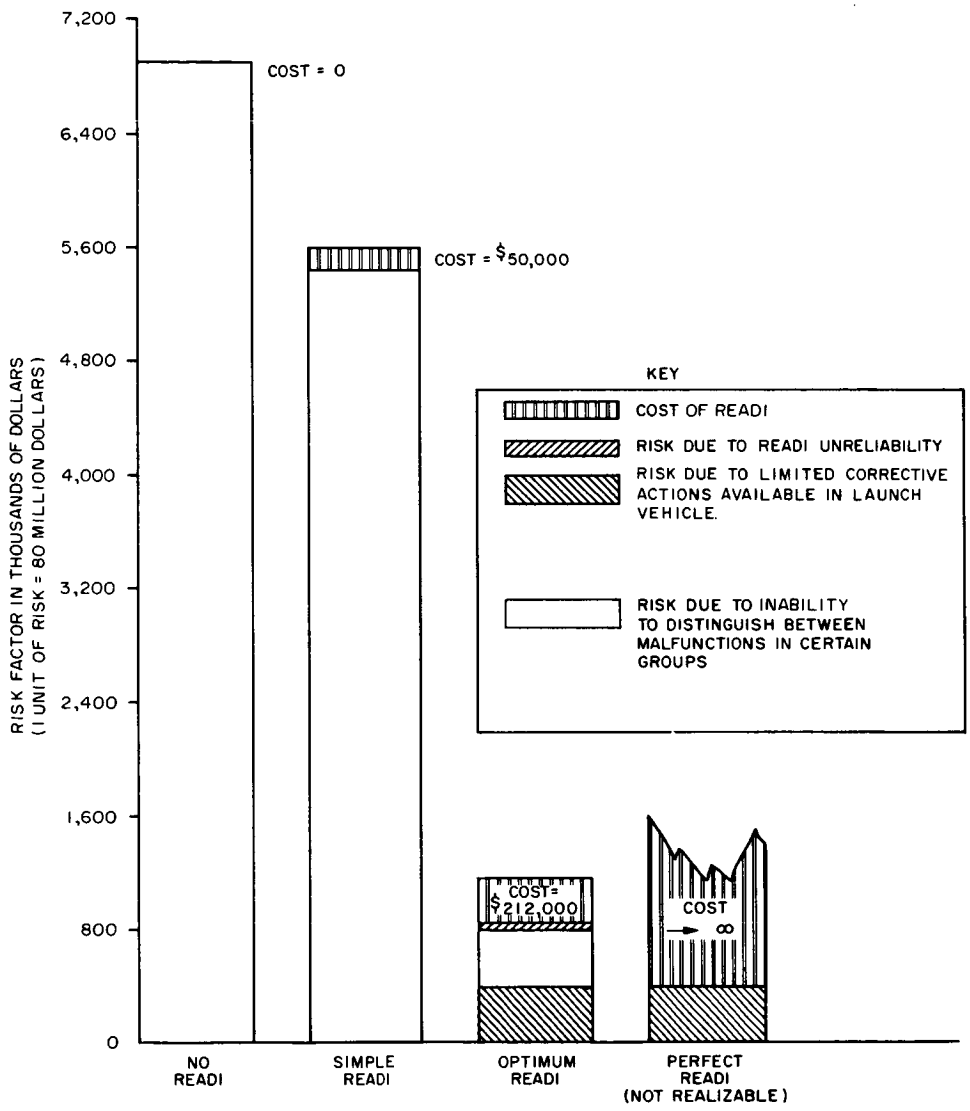


FIGURE 2-9
COMPARATIVE VALUE OF OPTIMUM SYSTEM

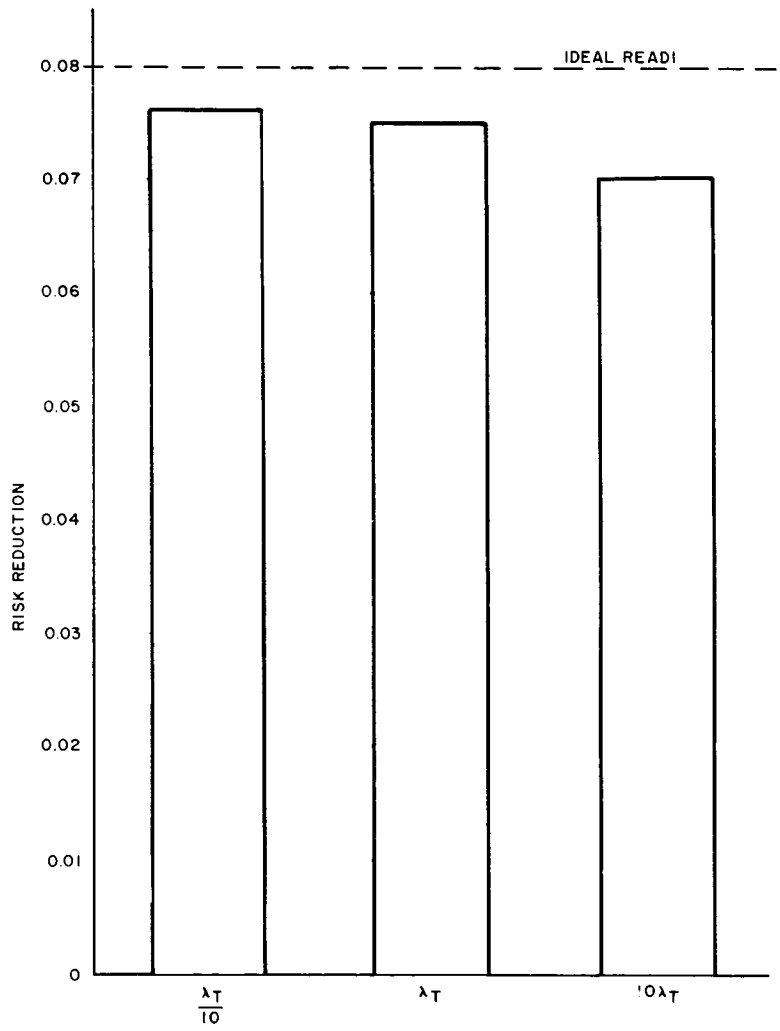


FIGURE 2-10

SENSITIVITY OF RISK REDUCTION TO TRANSDUCER FAILURE RATE λ_T (WITH SELF-CHECK AND INFORMATION REDUNDANCY)

(1) Shutdown - single engine

(2) Pre-valve shutdown - single engine

(3) Shutdown and restart - single engine

(4) Shut down all engines and initiate abort.

To determine the effect of propulsion system malfunctions and READI decisions on vehicle performance, some way must be found for evaluating the effect of a particular event (malfunction/decision) on the ultimate success of the end objectives. To accomplish this task, a mathematical model of the mission is required. Such a model has been devised and is described in Appendix D.

The mission and vehicle characteristics which were used in the design of READI are noted below.

The possible mission end conditions were:

- Successful prime mission, safe return of crew
- Successful alternate mission, safe return of crew
- Aborted mission, safe return of crew
- Aborted mission, crew lost

Many possible chains of events are possible between the start of the mission and termination at one of these end conditions. If each of the possible end conditions is assigned a weighting factor, or loss, an expected loss or risk is given by the summation of each end state loss multiplied by its probability of occurrence.

In assigning end state losses the value of attaining prime mission objectives was set equal to 1.0. The relative value of attaining alternate mission objectives and the crew-to-mission value ratio were assumed to be 0.2 and 10.0, respectively. Therefore, the resulting losses for each of the four end conditions are:

Mission End Condition	Loss
Prime Mission/Crew Safe	0.0
Alternate Mission/Crew Safe	0.8
Aborted Mission/Crew Safe	1.0
Aborted Mission/Crew Lost	11.0

The value of a particular READI function is determined by the manner in which it changes the probabilities of reaching each of the end states.

2-8. CONCLUSIONS

The results of the application of READI to the assumed mission, vehicle and engine shows that READI can have a substantial potential values; however, these results cannot be generalized to apply to all launch operations since the nature of the equipment and mission may differ substantially from the model assumed here.

The application of a READI system to the three stages of the typical launch vehicle described herein may be justified by the:

- Increase in crew survival reliability (from 0.947 to 0.986)
- Increase in mission reliability (from 0.883 to 0.927).

Perturbations of assumed input information indicated that the value of the READI system is effected and the nature of the optimum READI configuration changes. However, within reasonable limits of input information, the concept retains a positive pay-off.

SECTION III

SUMMARY OF READI DESIGN PROCEDURE

3-1. PRELIMINARY STATEMENT OF DESIGN PROBLEM

It is not intuitively apparent exactly what malfunctions should be monitored in a rocket engine. Even if a method is devised to specify the malfunctions requiring coverage by the READI system, additional questions regarding the use of information and component redundancy and self-check methods must be resolved. An orderly design procedure is therefore required.

It is the purpose of the design procedure to determine the optimum READI equipment configuration for application to a particular vehicle and mission. The optimum READI is defined as the READI system, chosen from the set of all possible READI systems for the particular vehicle which, when applied to the mission and vehicle, yields the minimum value of the sum of risk*plus READI system cost. That is, choose the READI system which results in the maximum pay-off when compared to the same mission and vehicle with no READI system.

As has been stated in Section II, it is the function of READI to detect propulsion system malfunctions and to make decisions as to the proper corrective action. Thus, to compute the risk portion of the optimization criterion, it must be determined what effect each malfunction/decision pair has on the probability of achieving each mission end state and thus the resultant mission risk. It is also necessary to be able to relate the transducers employed by a particular READI system, and their associated processing circuitry. to the true cost of developing, producing, and

- - - - - - -

*Risk to crew and risk to mission.

installing the system on a given vehicle or set of similar vehicles. The methods for accomplishing these two objectives are outlined in paragraph 3-2 and discussed in detail in Section IV. However, before proceeding to these discussions, it is well to first consider the two following design problems.

A. DESIGN PROBLEM 1

Consider first the problem of deciding whether or not to put an explosion detector on a rocket engine. Assume that a transducer capable of detecting propulsion system explosions in time to initiate an abort exists. (Such a transducer might sense a high ambient pressure rate.) Further assume that the probability of an engine explosion is 0.001 and that the explosion detector has the following failure characteristics.

- Probability of explosion detector false alarm is 0.001
- Probability of explosion detector missed alarm is 0.010.

If only two alternative decisions are available (continue the mission or abort the mission), then a loss is assigned for each malfunction/decision pair. For the purposes of this problem these are assigned as follows:

Table 3-1. Assigned Losses - Design Problem No. 1

Malfunction	Decision	
	Continue	Abort
Explosion	11	2
No Explosion	0	2

In assigning these losses, a crew-to-mission value ratio of ten has been employed. It is assumed that if an explosion takes place and no abort action is initiated, the crew and the mission will be lost. Finally, it is assumed that if an abort action is initiated the mission will be lost and a probability of 0.1 exists that the crew will also be lost.

First of all it must be decided whether to continue or abort when the explosion detector indicates an explosion. When the explosion detector indicates an explosion, the probability of an explosion may be computed using Bayes law. Doing this one obtains about 0.5 for this probability and, therefore, 0.5 for the probability of no explosion, given that the explosion detector indicates an explosion. Now the risk for each decision is computed, given that the explosion detector indicates an explosion.

Risk is formally defined as the sum of the products of the probability of a given event and the loss inflicted at the occurrence of that event. Thus letting

(1) P(A|B) be the probability of A. given B

(2) R(CC|D) be the risk of C. given D

(3) L(E.F) be the loss incurred at the occurrence of malfunction/decision pair (E.F),

we have

$$\begin{aligned} R(\text{Continuing}|\text{Exp Det}) &= P(\text{Exp}|\text{Exp Det})\ L(\text{Exp, Continuing}) + \\ &\quad P(\text{No Exp}|\text{Exp Det})\ L(\text{No Exp, Continuing}) \\ &= (0.5)\ (11) + (0.5)\ (0) \\ &= 5.5. \end{aligned}$$

and

$$\begin{aligned} R(\text{Aborting}|\text{Exp Det}) &= P(\text{Exp}|\text{Exp Det})\ L(\text{Exp, Aborting}) + \\ &\quad P(\text{No Exp}|\text{Exp Det})\ L(\text{No Exp, Aborting}) \\ &= (0.5)\ (2) + (0.5)\ (1) \\ &= 1.5. \end{aligned}$$

Thus, since R(Aborting Exp|Det) is the smaller of the two risks, it is chosen to abort when the explosion detector indicates an explosion.

Having decided what course of action to take when the explosion detector indicates an explosion, we must now examine the reduction in mission risk obtained by the inclusion of an explosion detector. Consider first the case when an explosion detector is included. The computations in this case are shown in figure 3-1. In this case the risk is 41×10^{-4}. Consider next the case when no explosion detector is included. The computations in this case are shown in figure 3-2. In this case the risk is 110×10^{-4}. Thus a risk reduction of 69×10^{-4} is obtained by including an explosion detector.

Now as a final step the cost of adding an explosion detector to the rocket engine must be compared to the above risk reduction. First, suppose the adjusted cost of an explosion detector is $10,000. Then, in order to compare this figure to the risk reduction, it is necessary to be able to express the unit of loss in dollars. Inspection of table 3-1 shows

that one unit of loss represents the loss of the vehicle and its mission. Thus we associate the replacement cost of the vehicle and mission with one unit of loss. This is taken here as 50 million dollars. Thus a risk reduction of 69 X 10^{-4} represents an expected saving of $345,000, which is certainly far in excess of the $10,000 cost of the explosion detector. Therefore, an explosion detector should be included in this case.

It should now be considered whether it is worthwhile to employ redundant explosion detectors to reduce the probability of missed or false alarms. A second transducer may be added either in parallel or in series, or three transducer may be used in a voting configuration. In parallel only a single transducer need indicate an explosion to give an alarm, while in series both transducers must indicate an explosion to give an alarm. On this basis the false and missed alarm probabilities shown in table 3-2 were obtained.

Table 3-2. Effect of Transducer Redundancy on Error Probability - Design Problem No. 1

Explosion Detector Configuration	Probability of False Alarm	Probability of Missed Alarm
None	-	1.00
Single Detector	0.001	0.01
2 Series Detectors	Negligible	0.02
2 Parallel Detectors	0.002	Negligible
3 Voting Detectors	Negligible	Negligible

Using these probabilities the risks shown in table 3-3 were obtained.

Table 3-3. Effect of Transducer Redundancy on Risk - Design Problem No. 1

Explosion Detector Configuration	Risk
None	110.00 X 10^{-4}
Single Detector	40.88 X 10^{-4}
2 Series Detectors	21.80 X 10^{-4}
2 Parallel Detectors	59.96 X 10^{-4}
3 Voting Detectors	20.00 X 10^{-4}

Thus a decrease in risk of 19.08 X 10^{-4}. or $95,400, is obtained by adding a second explosion detector in series with the first explosion

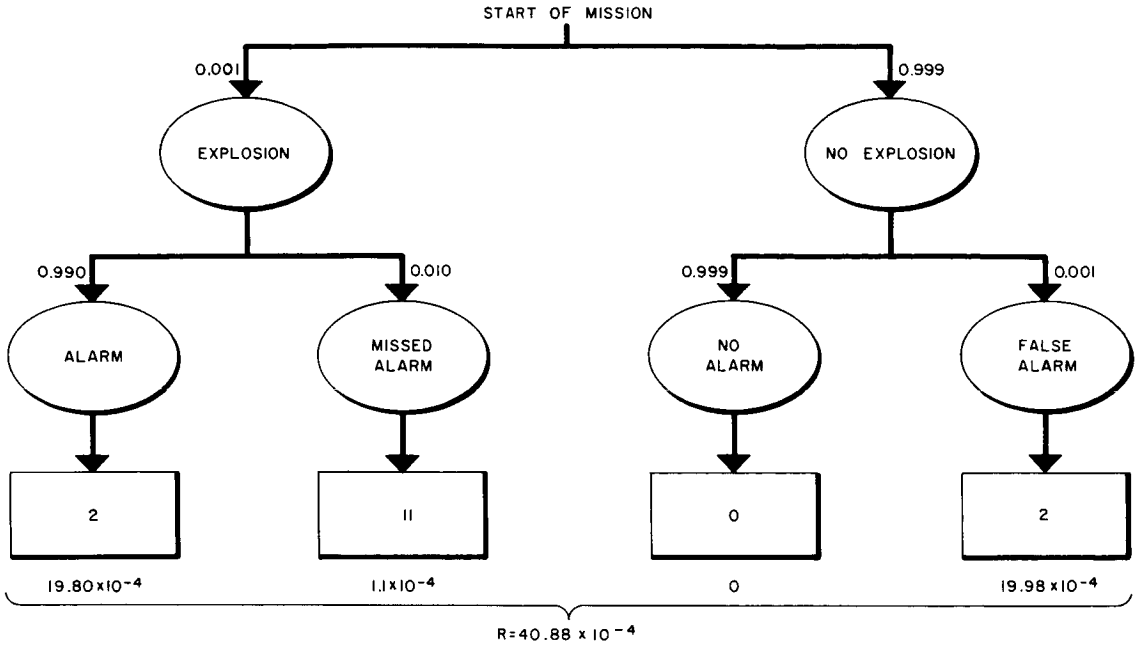


FIGURE 3-1
RISK CALCULATION WITH READI

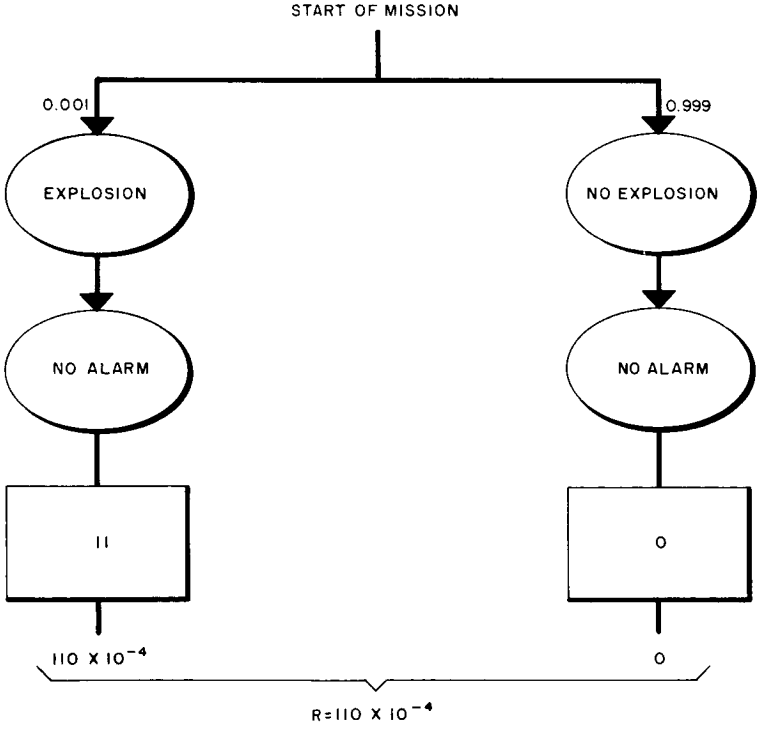


FIGURE 3-2
RISK CALCULATION WITH NO READI

detector. Therefore, at least a second explosion detector should be added, since the adjusted cost of an explosion detector is $10,000. It is important to note that adding the second detector in parallel, rather than in series, increases rather than decreases the risk.

Although the use of a third detector results in maximum risk reduction, the performance is not sufficiently improved over that obtained with two series detectors to justify the extra complexity:
$(21.80 - 20.00)10^{-4} \times \$50 \times 10^{6} < \$10,000$

This example points up the fact that the READI design problem has many aspects. In the above simple example, the following information was used:

- The probability of occurrence of the propulsion system malfunction
- The losses for each malfunction decision pair
- The failure probabilities of the READI transducer
- The adjusted cost of the READI transducer
- The replacement value of the vehicle and mission.

In this example the decision to include an explosion detector was reached in a fairly straightforward manner. This is because no other means of detecting an explosion was considered. Thus it was not necessary to decide on the means by which an explosion would be detected. Further, only one malfunction was considered. In order to see the complications which arise if there is more than one way to detect several malfunctions, the following example will be considered.

B. DESIGN PROBLEM 2

Assume that there are three malfunctions as shown in table 3-4.

Table 3-4. Malfunction Probabilities - Design Problem No. 2

Malfunction		Probability of Occurrence per Mission
Number	Name	
m_1	Lox Pressurization Failure	2.0×10^{-4}
m_2	Gas Generator Rupture	1.1×10^{-4}
m_3	Turbine Erosion	3.4×10^{-4}

Also assume that three READI decisions are available, i.e., continue the mission, shut down a selected engine, or abort the mission. The assigned losses for each malfunction/decision pair are as follows:

Table 3-5. Assigned Losses - Design Problem No. 2

Malfunction		Decision		
Number	Name	d_o Continue	d_1 Shut down One Engine	d_2 Abort
m_1	Lox Pressurization Failure	11.0	11.0	2.0
m_2	Gas Generator Rupture	0.3	1.0	2.0
m_3	Turbine Erosion	6.0	1.5	2.0

The method used in assigning the losses will be explained in paragraphs 3-2, 4-2, and 4-3. Finally, assume there are three malfunction detectors, the coverage and adjusted cost of which are as follows:

Table 3-6. Malfunction Detector Coverage - Design No. 2

Malfunction Detector			Malfunction		
Number	Name	Variable Cost (*) (dollars)	m_1 Lox Pressurization Failure	m_2 Gas Generator Rupture	m_3 Turbine Erosion
V_1	Low Turbine Speed	2000	1	1	1
V_2	Low Chamber Pressure	3000		1	1
V_3	Low Gas Generator Temp	2000	1	1	

*A $20,000 fixed cost will be added to the variable transducer costs to account for development and other nonvariable costs.

In this table a "1" indicates that the malfunction is picked up by the malfunction detector.

In order to be better able to visualize the problem of finding the optimum combination of malfunction detectors in this case, a new representation of the set of malfunctions and malfunction detectors, based on the Venn diagram often used in mathematical logic, is introduced. In this representation the propulsion system malfunctions are represented by points in the plane. To each such malfunction point is associated a list containing

$$\left[L(d_o\ m_i) - L(d_k\ m_i)\right]\ P(m_i),$$

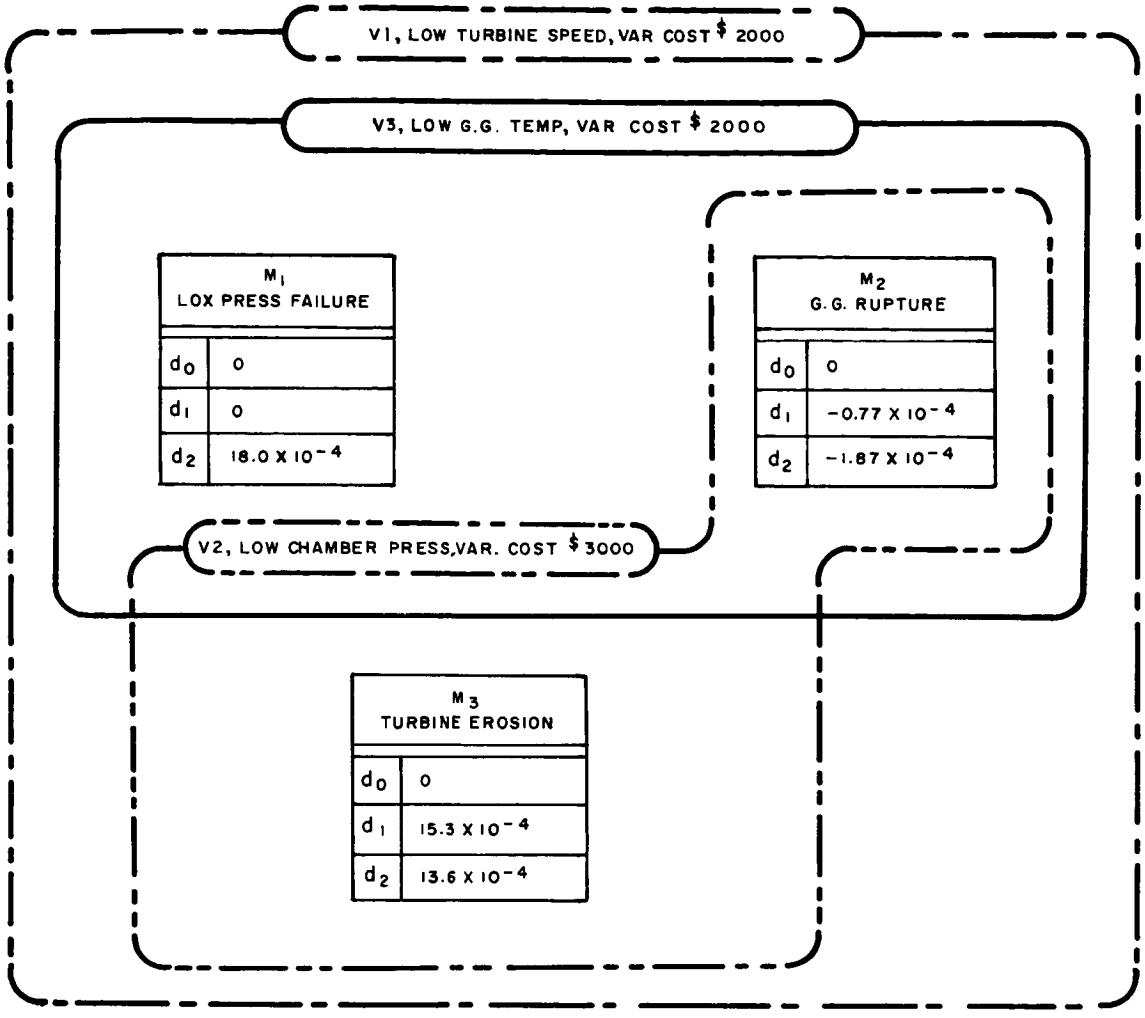
where d_o is the decision to continue, d_k is the kth decision, m_i is the malfunction represented, and $P(m_i)$ is the probability of m_i, for each value of k. The values in this list represent the difference between the risk for no READI and for a READI which always makes decision d_k when malfunction m_i occurs, attributable to m_i. Then a plot is made of the coverage of each malfunction detector by enclosing the malfunctions detected with a labeled closed curve. This representation of the design problem is called a Venn diagram representation.

The Venn diagram representation of the present example is shown in figure 3-3. There are eight possible combinations of malfunction detectors which may be made from the set of three malfunction detectors treated here. Thus there are eight possible READI systems. Using the Venn diagram the ability of each READI system to separate the malfunctions into different groups may be determined. For example, consider first the system employing only malfunction detector V1. Such a system can not tell the difference between malfunctions m_1, m_2, and m_3, since any one of them will cause V1 to appear. Such a set of malfunctions is called an inseparable set of malfunctions, and only one decision may be assigned to an inseparable set of malfunctions. Consider next the system employing only malfunction detector V2. In this case m_2 and m_3 form an inseparable set of malfunctions. Further, this system can not detect the occurrence of m_3. Thus m_3 and "no propulsion system malfunction" form an inseparable set of malfunctions. Malfunctions which are not separable from "no propulsion system malfunction" are called not monitored malfunctions. Finally, consider the system employing malfunction detectors V1, V2, and V3. In this case there are no sets of inseparable malfunctions, i.e., the system can tell the difference between m_1, m_2, and m_3 as shown in the following tabulation.

Malfunction	Malfunction Detector Term
m_1	$V1 \cdot V3 \cdot \overline{V2}$
m_2	$V1 \cdot V2 \cdot V3$
m_3	$V1 \cdot V2 \cdot \overline{V3}$

In this tabulation the combinations of the V's are in the Boolian sense and $\overline{V}n$ indicates the complement of Vn.

Next it must be determined which decision to assign to each set of inseparable malfunctions. Neglecting, for the moment, READI transducer unreliability, it is possible to assign these decisions on the basis of the list of risk differences associated with each malfunction. It must be kept in mind that each entry in this list represents the difference between the risk for no READI and for a READI which always makes the indicated decision when the indicated malfunction occurs, and is attributable to that malfunction. Thus, this difference should be maximized. Remembering that at most only one decision can be assigned to each inseparable set of malfunctions, it is seen that the decision for which the sum of the risk



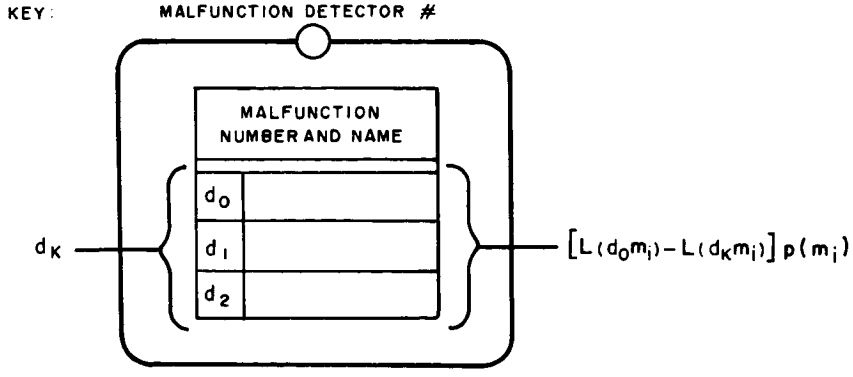


FIGURE 3-3

VENN DIAGRAM REPRESENTATION OF DESIGN PROBLEM

differences over the inseparable set of malfunctions is a maximum must be chosen. Consider again the system employing only V1 in the example. Here m_1, m_2, and m_3 form an inseparable set of malfunctions. Thus each entry in the list must be summed for each decision over m_1, m_2, and m_3. The results of this calculation are shown below:

Decision	Sum Over m_1, m_2, m_3
d_0	0
d_1	14.53×10^{-4}
d_2	29.73×10^{-4}

Thus in this system decision two, i.e. abort, is chosen when V1 indicates the presence of a malfunction. In contrast to this, consider again the system employing V1, V2, and V3. In this system m_1, m_2 and m_3 are separable. Therefore, if so desired, a different decision may be assigned to each. Again applying the above maximization principle, the decision corresponding to the maximum entry in its list was chosen for each malfunction. Therefore, d_2 was chosen for m_1 and d_1 for m_3. Inspection of the list for m_2 shows that d_o, i.e. no action, is the correct decision. This is because, within the set of possible corrective actions available in this example, there is no corrective action which, on the average, yields better results than no action. It was chosen, therefore, to deliberately not monitor m_1, and the definition of "not monitored malfunctions" was generalized to include those malfunctions which should not be separated from "no malfunction."

Having chosen the decisions for each inseparable set of malfunctions, it is now possible to assess the difference in risk between the system employing only V1 and the system employing V1, V2, and V3, again neglecting the unreliability of the READI transducers. To perform this comparison it should first be noted that the $L(d_o m_i)\ P(m_i)$ term in the risk difference serves as a common reference level from malfunction to malfunction. Thus by summing the entries in each list corresponding to the chosen decision over the set of malfunctions one obtains the difference in risk between no READI and the particular READI under consideration. This quantity may be considered to be the system value in that it represents the reduction in risk compared to no READI obtained by employing the system. The system value may be directly compared to the READI system cost, and the system

having the largest system value will result in the minimum risk. The system value of each of the above two systems is shown below.

System	System Value
Using V1	29.73×10^{-4}
Using V1, V2, V3	33.30×10^{-4}

The above process of decision assignment and system value computation may be carried out for each possible combination of malfunction detectors arising out of V1, V2, and V3. The results of such a computation are shown in table 3-7. Now, in order to be able to choose the best system, i.e., the system with minimum risk plus cost, the READI system cost must be taken into consideration. Since the system value represents the risk reduction over a no READI system, it is necessary to subtract the adjusted READI system cost, in risk units, from the READI system value. To do this the adjusted cost of each transducer is added to a basic READI system cost. This basic cost represents the central system cost plus the development costs shared over a number of vehicles. It is taken here as $20,000. This value is then converted to risk units by dividing by the mission plus vehicle replacement value, taken here as 50 million dollars. The results of these computations are shown in table 3-7.

Inspection of table 3-7 shows that the system employing V2 and V3 is the best system since it has the maximum system value less adjusted cost.

Up to this point READI transducer unreliability has been neglected. The effect of this factor on the above choice of optimum system will now be investigated briefly by considering the effects of false alarms on the chosen system. This investigation is being restricted to false alarms since their probability is higher than missed alarms; however, in a detailed evaluation of a system this restriction would not be made. It is assumed that the false alarm probability for each transducer is 1×10^{-4}. The decision rules for the chosen system were obtained using the Venn diagram of figure 3-3 and table 3-7. The rules obtained were

$$d_1 = V2 \cdot \overline{V3}$$

$$d_2 = \overline{V2} \cdot V3$$

Table 3-7. Summary of Example Design Problem

Malfunction Detector Content			Assigned Decisions			System Value	Adjusted System Cost *	System Value Less Adjusted System Cost	
V1	V2	V3	m_1	m_2	m_3				
			d_o	d_o	d_o	0	0	0	No READI
X			d_2	d_2	d_2	29.73×10^{-4}	4.40×10^{-4}	25.33×10^{-4}	
	X		d_o	d_1	d_1	14.53×10^{-4}	4.60×10^{-4}	9.93×10^{-4}	
		X	d_2	d_2	d_o	16.13×10^{-4}	4.40×10^{-4}	11.73×10^{-4}	
X	X		d_2	d_1	d_1	32.53×10^{-4}	5.00×10^{-4}	27.53×10^{-4}	
X		X	d_2	d_2	d_1	31.43×10^{-4}	4.80×10^{-4}	26.63×10^{-4}	
	X	X	d_2	d_o	d_1	33.30×10^{-4}	5.00×10^{-4}	28.30×10^{-4}	Best System**
X	X	X	d_2	d_o	d_1	33.30×10^{-4}	5.40×10^{-4}	27.90×10^{-4}	

*Assumes

1. A mission replacement cost of 5×10^7 dollars.
2. A basic system cost of 2×10^4 dollars.
3. Units are those of risk.

**With no failures in the READI equipment.

where the equations are to be taken in the Boolian sense: d_k is indicated if $d_k = 1$, and if $d_1 = d_2 = 0$, then $d_0 = 1$. The effects of transducer failures which cause false alarms will now be examined. Since this discussion concerns false alarms, it is known, a priori, that no propulsion system malfunction is taking place. Then the unfailed values of the terms in the above decision rules are

$$V2 = 0 \qquad \overline{V2} = 1$$
$$V3 = 0 \qquad \overline{V3} = 1$$

Now suppose V2's transducer fails so that V2 = 1. Then the values of the terms in the decision rules are

$$V2 = 1 \qquad \overline{V2} = 0$$
$$V3 = 0 \qquad \overline{V3} = 1$$

and we have

$$d_1 = 1 \cdot 1 = 1$$
$$d_2 = 0 \cdot 0 = 0$$

and decision one is indicated. Also, if V3's transducer fails so that V3 = 1, it is seen that d_2 is indicated.

Now when the system value is computed neglecting transducer failures, the term $\left[L(d_0\ m_0) - L(d_0\ m_0)\right] P(m_0)$ was dropped, since it is zero. Here m_0 indicates no propulsion system malfunction. In the presence of false alarms it is necessary to include a similar term for each false alarm. This term is of the form $\left[L(d_0\ m_0) - L(d_k\ m_0)\right] P(d_k)$, where $P(d_k)$ is the probability of the false alarms leading to d_k and use has been made of the fact that $P(m_0) \doteq 1$. Now $L(d_0\ m_0) = 0$, so that $-L(d_k\ m_0)\ P(d_k)$ is obtained, and is to be added to the system value for each false alarm. In the present example:

Transducer Failed	Decision	$P(d_k)$	$L(d_k\ m_0)$	$L(d_k\ m_0)\ P(d_k)$
V2	d_1	1×10^{-4}	1.0	1×10^{-4}
V3	d_2	1×10^{-4}	2.0	2×10^{-4}
				3×10^{-4}

Thus the system value, less adjusted cost corrected for false alarms of the system employing V2 and V3, is $(28.30 \times 10^{-4}) - (3.00 \times 10^{-4})$, or 25.30×10^{-4}.

Since the decrease in system value due to false alarms is a large percentage (11.5 percent), of the corrected system value, it is worthwhile to determine if there is a system more resistant to the effects of false alarms; that is, a system for which the corrected system value less adjusted cost is in excess of 25.30×10^{-4}. It should be noted that in the above calculations the effect of the simultaneous failure of V2 and V3 has been neglected. This is because the probability of such a failure is on the order of 10^{-8}. Thus it may be assumed, for purposes of design and evaluation, that only one transducer is failed at a time. Now consider the system employing V1, V2, and V3. The decision rules for this system are

$$d_1 = V1 \cdot V2 \cdot \overline{V3}$$

$$d_2 = V1 \cdot \overline{V2} \cdot V3$$

Consider, for example, the values of the V's in the presence of no malfunction when V1 is failed. These are

$$V1 = 1$$

$$V2 = 0; \ \overline{V2} = 1$$

$$V3 = 0; \ \overline{V3} = 1$$

Thus in this case

$$d_1 = 1 \cdot 0 \cdot 1 = 0$$

$$d_2 = 1 \cdot 1 \cdot 0 = 0$$

so that d_0 is indicated and no false alarm takes place. The results for V2 and V3 failed are the same. Thus this system has no subtracted term due to false alarms, and its system value less adjusted system cost remains at 27.90×10^{-4}. Therefore, when false alarms are considered, the system employing V1, V2, and V3 is the best system.

The above example has shown several additional features of the READI design problem. These are:

- In order to select the optimum system from among a set of possible systems, it is necessary to perform a trade-off involving risk and cost.

- That malfunction indicators perform three functions, which are
  - Separation of propulsion system malfunctions from no malfunction
  - Separation of one propulsion system malfunction from another
  - Information redundancy to mitigate the effects of READI transducer failures
- That the selection of the optimum system may be influenced by transducer failure characteristics
- That even in a small example the process of selecting the optimum system is time consuming and therefore a better method of system synthesis is required. Such a system synthesis procedure has been developed. It is described in paragraph 3-2 and developed in detail in Section IV.

3-2. OUTLINE OF THE DESIGN PROCEDURE

The previous examples demonstrated that to design a READI system it is necessary to identify a diversity of input data concerning the mission; the vehicle, including the propulsion system; and the READI system itself. In addition it is necessary to devise a procedure which will locate the optimum system in terms of transducer and signal processing content. The optimum system, it may be recalled from figure 2-6, is the system which minimizes the total cost, C_T, of the mission, where C_T is the sum of the fixed vehicle and launch costs and the risk to mission and crew.

Again referring to the first design problem, two design steps are suggested. These are:

Step 1 - Identification of malfunctions, m_i, and estimation of the probability of occurrence of each, $P(m_i)$.

- Design of malfunction detection techniques, V_i, and estimation of the probability of false alarms, missed alarms, and wrong alarms, P(FA), P(MA) and P(WA), respectively.

Step 2 - Identification of remedial actions available and computation of losses for each decision (d_k) executed from each malfunction (m_i) in the vehicle. (These will be referred to as m/d pairs.)

In the second design problem it became apparent that a variety of combinations of V's could be utilized. A third step is therefore suggested:

Step 3 - Synthesis of the subset of malfunction detection elements, V_i (i.e., transducers and processing circuitry), which yield the optimum system in terms of minimization of total cost, C_T.

In subsequent discussions the three steps will be identified as:

1. Malfunction Identification
2. Loss Computation
3. System Synthesis.

These main steps may be broken down into a number of substeps which require the services of three technical-skill groups:

- Propulsion System Analysis
- Mission Analysis
- Equipment and System Analysis.

The distribution of tasks among these skill groups is shown in figure 3-4. In order to obtain a better appreciation of the system synthesis procedure, the three main steps will be discussed in more detail in the following paragraphs.

A. MALFUNCTION IDENTIFICATION - STEP 1

Malfunction identification is of necessity the starting point in the design. In this step a statistical picture of the malfunction characteristics of the propulsion system is drawn. The two main areas of activity in step 1 are

- Statistical analysis of the propulsion system data to determine what malfunctions occur, estimate their likelihood of occurrence and construct cause and effect relationships
- Analysis of the cause and effect relationships and study of static test procedures to develop techniques for detecting malfunctions.

The results of the cause and effect analysis will also be used in Step 2, the computation of propulsion system losses.

A malfunction effect tree is a graphical method of presenting the results of the cause and effect analysis*. Part of such a tree is shown in figure 3-5. Malfunctions are defined at the upper level. This level has the characteristic that the malfunction areas must be statistically independent.

This model is helpful in finding techniques for malfunction detection. For instance, loss of fuel pump pressure is an indication of three different malfunctions. If better malfunction separation is required, the indication of loss of tank pressure may be used. The reason for this finer separation would be that the optimum decision may be different for the malfunction subgroups, tank rupture-vent valve open and high pressure fuel line rupture. It is also apparent that measurements made further down the tree may not be satisfactory, since the undesirable final effects are close at hand. In this simple case, for instance, if the malfunction had been fuel line rupture, thrust would be lost regardless of whether the engine was shut down or not. However, shutdown would prevent engine destruction by immediately cutting off lox flow. This part of the problem will be brought up in more detail in Step 2, Loss Computation.

The other main source of clues for malfunction detection techniques is the study of emergency shutdown procedures used in static testing. For instance, the following procedures are used in F-1 testing:

- Automatic "Red Line" Monitoring
- Chart Observers
- Special Devices
  - Combustion Instability Monitors
  - Structural Vibration Detectors
- Visual Observation of Engine.

The special significance of these procedures is that they reflect directly the malfunctions which, based on current experience, are anticipated during the test.

- - - - - - -

*Analysis of this kind is now accepted practice for large launch vehicles.

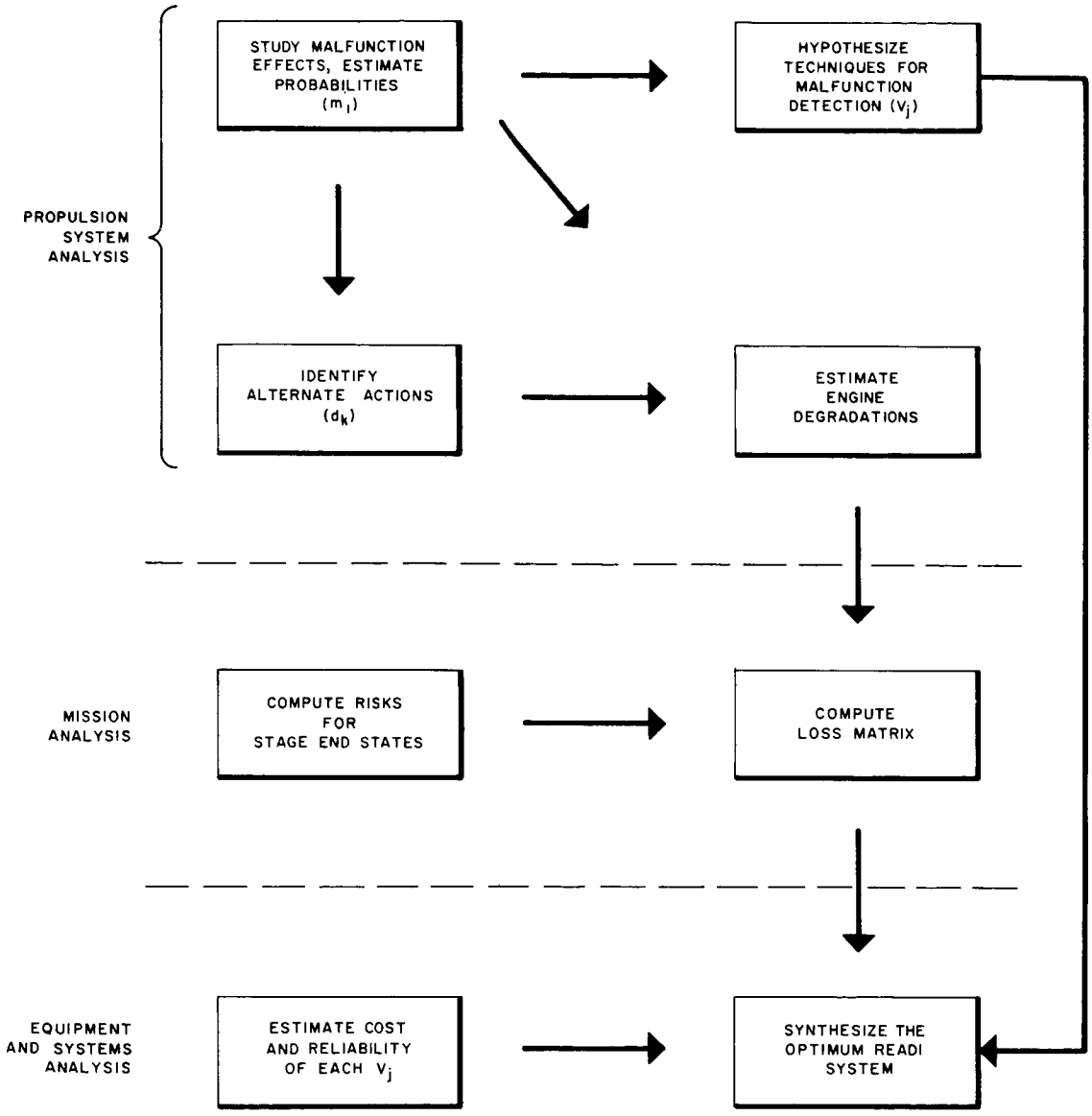


FIGURE 3-4
READI DESIGN PROCEDURE

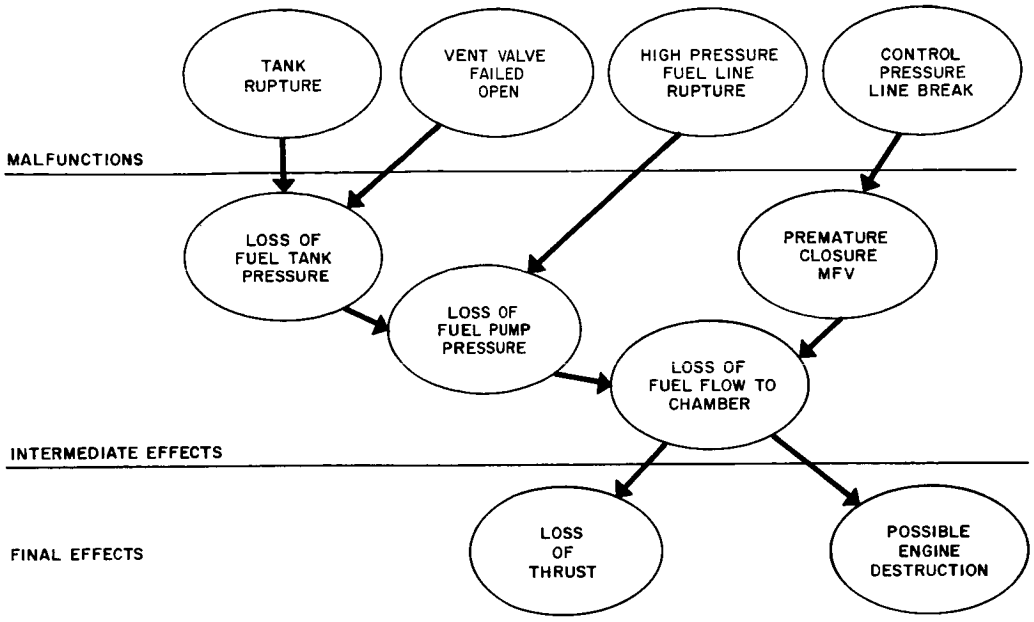


FIGURE 3-5
PART OF FAILURE EFFECT TREE FOR F-1

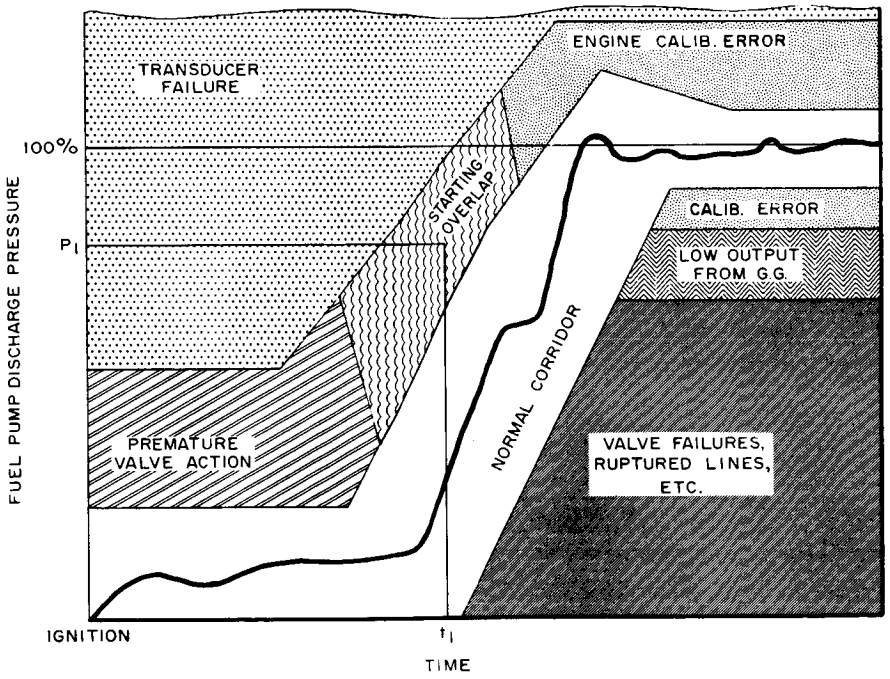


FIGURE 3-6
FUEL PUMP DISCHARGE PRESSURE FOR VARIOUS MALFUNCTIONS

Analysis of groups of related variables indicates to the designer the required formulation. For instance, fuel pump discharge pressure is an indicator of a variety of malfunctions when the signal is suitably processed and compared to other signals. Some of these malfunctions are shown in figure 3-6.

Suppose, for example, that it is desired to detect the "starting overlap" condition. This condition is caused by early opening of the gas generator propellant valve and/or prolonged operation of the turbine spinner. The spinner, which takes the form of a solid propellant gas generator in the H-1 engine, is designed to get the engine above the bootstrap level rapidly and repeatedly. Obviously, measurements of gas generator valve position and the temperature of the gas stream exiting from the spinner would be considered in the formulation. But if no abnormally high pump pressure were noted, the position and temperature measurements would be meaningless. One candidate formulation to be considered would involve the following operations:

n is Boolian 1	When
n_1	time = t_1 (See figure 3-6.)
n_2	fuel pump discharge pressure > P_1
n_3	gas generator valve opens early (for time t_1)
n_4	spinner temperature high (for time t_1).

A formulation which brings together all of the above limit conditions is the Boolian expression

$$(n_1)(n_2)(n_3 + n_4)$$

In general, the signal processing involves more than simply the comparison of a variable to a limit*. A typical catalog of malfunction detection techniques (V_i's) will involve operations of arithmetic (addition, subtraction, etc.), frequency filtering, differentiation and integration, and function generation. The selection of the best combination of techniques in the catalog is left to Step 3, System Synthesis.

- - - - - - -

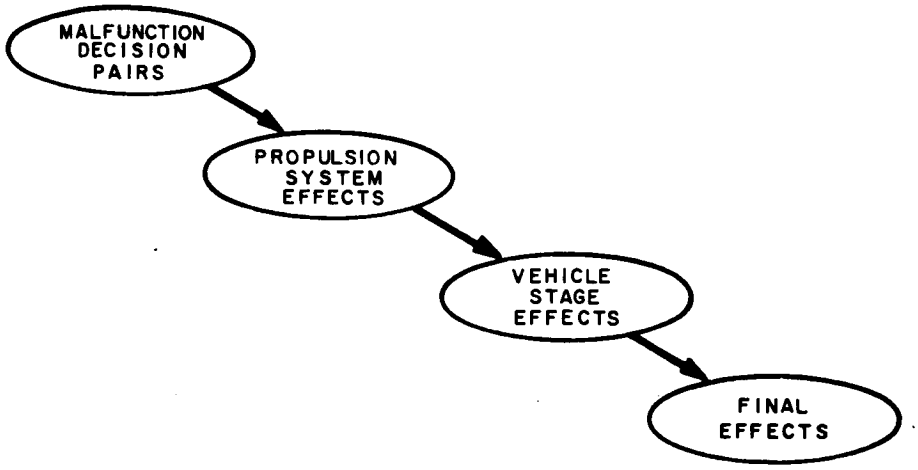
*The n_1, n_2 combination is an example of a time-varying limit.

B. LOSS COMPUTATION - STEP 2

The loss computation operation is composed of four substeps.

- Identification of alternate actions and formulation of decisions
- Computation of subsystem degradations and direct hazardous effects resulting from malfunction/decision pairs
- Computation of vehicle and stage effects resulting from the above step
- Computation of final effects on mission accomplishment, crew survival, recoverability of boosters, etc.

These substeps are summarized in the following sketch.



Alternative corrective actions may be fairly limited in large launch vehicles. In the first design problem (explosion detection) it will be recalled that there were only two alternatives: to continue (i.e., do nothing), or to abort. In the second example the possibility of shutting down a single engine was considered. Many unorthodox alternative actions should be considered in the initial study, even though associated with them are undesirable performance or reliability penalties which would make it undesirable to initiate the action as a matter of standard practice. However, once a severe malfunction has occurred and a considerable performance degradation or catastrophic loss is a certainty, the alternative may be attractive. For instance, consider a five-engine stage with 98-percent reliable engines. An alternative is available which, when executed, degrades the engine reliability to 90 percent, but permits the mission to continue on four engines. As shown in figure 3-7, the alternative would never be

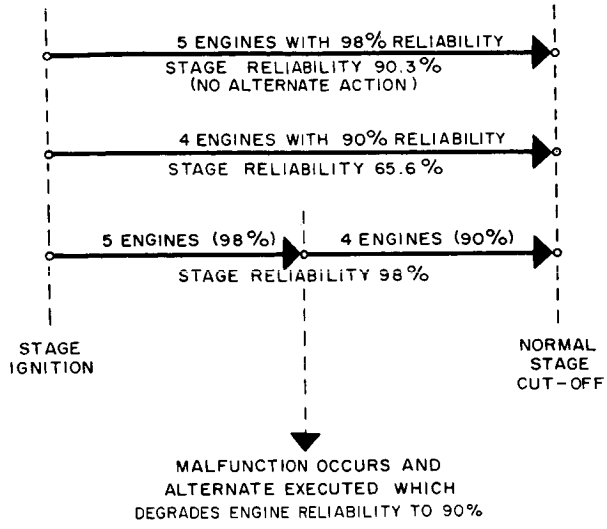


FIGURE 3-7

EMERGENCY MODE ANALYSIS (5-ENGINE STAGE)

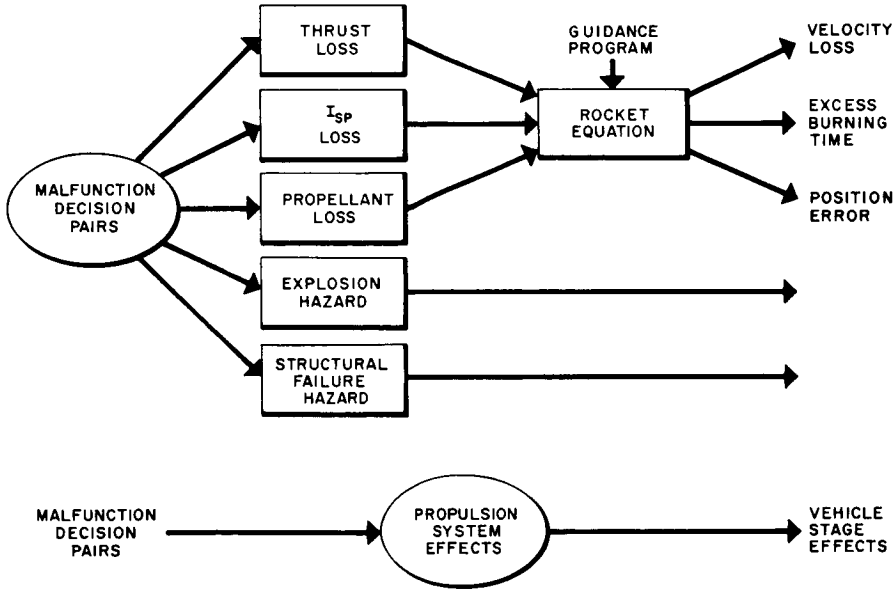


FIGURE 3-8

COMPUTATION OF LOSSES

programmed arbitrarily, but when a malfunction occurs a stage reliability of 98 percent can be maintained by executing the alternative.

The second substep in loss computation involves the detailed computation of the propulsion system losses resulting from all malfunction/decision pairs. The parameters used to describe the loss depend upon the subsystem in which the malfunction has taken place. For liquid rocket engine systems it has been found convenient to use percent losses of thrust, specific impulse and overboard propellant flow. At this juncture the vehicle and guidance scheme must be considered in order to predict the stage losses in terms of velocity increment, excess burning time, etc. This substep is summarized in figure 3-8.

It is then necessary to determine the effect of the propulsion system malfunction on the attainment of the mission objectives. The status of the vehicle can be defined during the burning time in terms of a velocity vector, a position in space and an attitude reference angle. Malfunctions in the propulsion system are most strongly reflected in loss of stage velocity increment. Since there are fairly well defined limits on the allowable velocity loss for a specific mission, these limits are used to define stage end states, description of the overall status of the mission, i.e., normal, alternate mission attainable, etc. A malfunction requiring engine shutdown at stage ignition may (for a first stage) be tantamount to abort while at a time close to normal stage cutoff. The same malfunction and decision may be satisfactory even for achievement of the prime mission. This requires that the stage burns for a somewhat longer time and some or all of the corrective capability of subsequent stages is expended. This idea is illustrated in figure 3-9. The loss vector computation is shown in figure 3-10.

C. SYSTEM SYNTHESIS - STEP 3

1. Input Data

The final step in the design process is the synthesis of the optimum system from among all of the possible systems. It is in the system optimization step that the diversity of input data has its full impact on the system designer. The designer is presented with the following information:

- A catalog of malfunction identification techniques - This catalog will include information on the transducers required, the signal processing, and the coverage in terms of malfunctions detected

- A tabulation of the losses for all malfunction/decision pairs - This information evolves from the last step in the loss computation process.

In addition, the designer supplies data on:

- The cost of implementing each malfunction technique - Cost will include prorated contributions to cost of developing, validating, and maintaining the system up to launch time, penalties due to weight, and the direct cost of equipment. Typical costs range from $2,000 to $15,000 per transducer, plus $100,000 fixed cost per stage prorated over 20 launch vehicles.
- The reliability of the READI system expressed in terms of probability of failure, in various modes, of the system components - The transducers and associated cabling are the dominant factors in READI unreliability. Typical failure rates are 10^{-4} per mission.

2. Appraisal of the Synthesis Problem

The size of the system is undefined at the outset. There could be two or 200 transducers per engine in the optimum system. Also, as shown in the second design problem, typical detection techniques have a considerable amount of overlapping coverage of malfunctions. This means that information redundancy will play a prominant roll in the design. Component redundancy can also be used to advantage, though failure rates must be adjusted to account for the lack of independence in failures of like transducers in a common environment.

It was possible in the second design example to converge rapidly on the optimum configuration because, for illustrating purposes, a small problem was extracted from a large one. The second design problem had three malfunctions, three detection means and three decisions, all of which were carefully selected. Analysis of the propulsion system for a real launch vehicle stage will uncover at least 20 important malfunctions per engine and an equal number in the stage. At least 30 candidate malfunction detection techniques and up to five decisions should be considered at the outset. Mission phase (i.e., engine ignition to vehicle lift-off, etc) has the effect of adding a completely new dimension to the problem. Typical stages will have five or more phases in which decisions, losses and detection techniques may change.

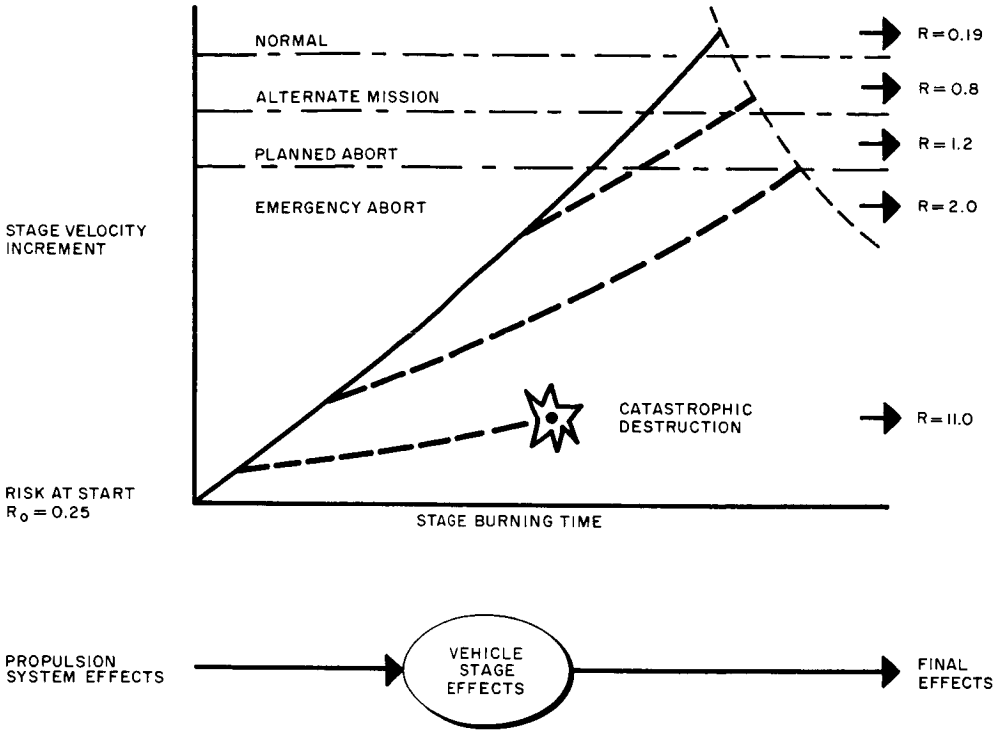


FIGURE 3-9
FINAL EFFECTS COMPUTATION

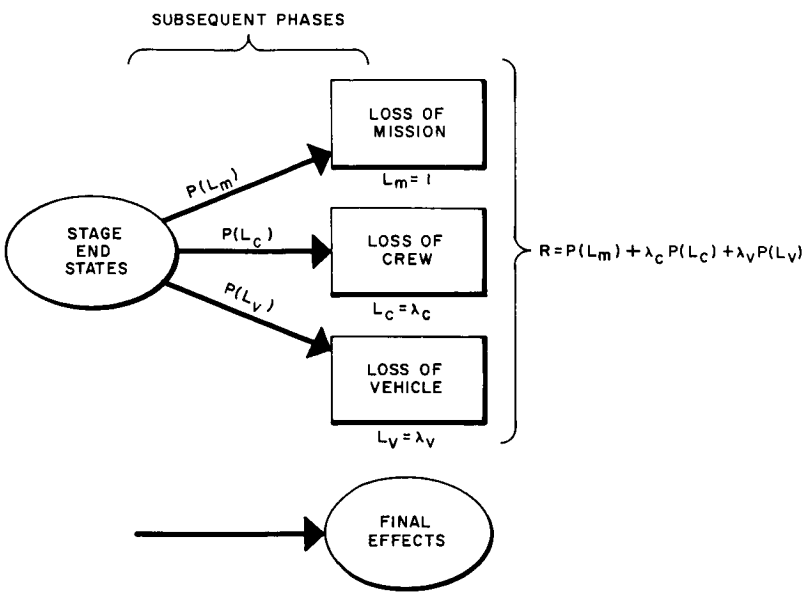


FIGURE 3-10
LOSS VECTOR COMPUTATION

3. Solution of the READI Synthesis Problem

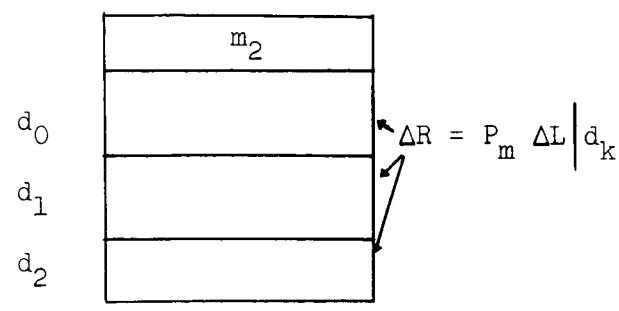
There are three essential steps to finding the optimum configuration. These are:

- Presentation of risk data in a manner suitable for system synthesis
- System reduction using testing criteria to establish that the optimum system will contain certain groups of malfunction detection techniques and that others will not be contained. In this step READI failures are neglected.
- Detailed evaluation of the reduced set of possible systems to find the optimum. A digital computer program is utilized in this final step where READI failures are considered.

These three steps will be considered in more detail in the following paragraphs.

a. Presentation of Risk Data

It is not always clear at the outset what decision is best for a given malfunction because of the complex interplay of malfunctions, stage and mission effects, and weighting factors placed on mission, launch vehicle and crew. A method of presenting risk data was shown in the second design problem which is helpful in pinpointing the best decision. It will be recalled that in figure 3-3 a list of risk differences, ΔR, for each possible decision is associated with each malfunction. The ΔR's are computed from the probability of malfunction factored by the difference between the loss for the decision in question and the no action decision. For instance, from the example,



An array of malfunctions can now be developed which covers a whole engine or stage, where each entry includes the above items of data.

b. System Reduction

The system reduction step serves as a coarse strainer which eliminates some malfunction detection channels and shows that others are definitely worthwhile and should appear in the optimum system. Testing criteria for the inclusion or exclusion of malfunction detection techniques are the tools used in system reduction. These testing criteria must meet three requirements:

- The criteria must be sufficiently effective to reduce the number of systems which must be fully evaluated to a reasonable number
- The criteria must be easy to apply. Any process approaching the full evaluation procedure in complexity is of no value
- The criteria must be true, i.e., the execution of the reduction operation must never result in the exclusion of malfunction detection channels which are in the optimum system, or in the definite inclusion of channels which are not in the optimum system.

For the purposes of system reduction, the malfunction detection techniques in the catalog are identified by the transducers which are required for each. The reason for this is that the variable part of the system cost is predominantly vested in transducers and cabling, rather than in the processing circuitry. Therefore, if, for instance, the measurement of fuel pressure against a high limit is under consideration and a cost has been assigned, then the measurement of the fuel pressure against a low limit is also available at no cost. At any stage of the reduction process, the system is described in terms of the transducer sets, or T-sets contained therein.

Two systems are defined at the outset in terms of transducer content: one is the maximum transducer set (max T-set) which uses all of the available transducers, and the other is the minimum transducer set (min T-set) which at the start contains no transducers. The optimum T-set is somewhere in between the minimum and maximum sets. The objective is to add transducers to the min T-set and remove transducers from the max T-set and converge on the optimum set. If the testing criteria are effective enough, or if the problem is simple enough, the optimum system can be found by the system reduction procedure. Then the complete evaluation is unnecessary, except to account for READI equipment failures.

The testing criteria are stated briefly in the following paragraphs.

INCLUDE CRITERIA

A transducer (or group of transducers), T, will be contained in the optimum system (i.e., added to the minimum transducer set) if, over any subset of malfunctions, the value of the minimum transducer set plus T, minus the value of the maximum transducer set minus T, exceeds the cost of T.

Stated mathematically, the include criteria are

$$\text{VALUE}_{I}\,(\min + T) - \text{VALUE}_{I}\,(\max - T) > \text{COST}\,(T)$$

where

VALUE_{I} ≡ the value over some I

min + T ≡ the minimum transducer set including T

max - T ≡ the maximum transducer set excluding T

COST (T) ≡ the cost of transducer T.

EXCLUDE CRITERIA

A transducer (or group of transducers), T, will not be contained in the optimum system (i.e., deleted from the maximum transducer set) if, over the region of influence of that T, the cost exceeds the value of some possible transducer set, P, plus T, minus the value of that transducer set minus T. By "some possible transducer set" is meant a transducer set which includes the minimum transducer set and is included in the maximum transducer set.

Stated mathematically, the exclude criteria are

$$\text{COST}\,(T) \quad \max_{P} \sum_{I \in I^*} \left[\text{VALUE}_{I}\,(P + T) - \text{VALUE}_{I}\,(P - T) \right]$$

where

COST (T) ≡ the cost of transducers T

$\underset{I}{\text{VALUE}}$ ≡ the value over some I

P + T ≡ some possible transducer set including T

P - T ≡ some possible transducer set excluding T

I* ≡ those malfunction subsets contained in the region of influence of transducer T

The include and exclude criteria are restated and proved in Section IV. However, before proceeding to the details, the criteria will be demonstrated on the numerical example in Design Problem 2.

In order to apply the criteria to the second design problem it is first necessary to present the malfunctions in the array format shown in figure 3-3. Recall that each numerical entry for the malfunctions in the array is the risk reduction achieved by making a particular decision, compared to no decision, when the malfunction occurs:

$$\Delta R = Pm\ \Delta L | d_k$$

This malfunction array can be subdivided by malfunction detectors (V's), which are referred to a T-set. When considering a particular V, it is necessary to study only the region of m's within the influence of the V, i.e., in figure 3-3 only the m's enclosed in the loop for the subject V.

Refer now to table 3-1 and consider V1. Applying the include criteria we have

$$(29.7 - 33.3)10^{-4} = -3.6 \times 10^{-4}$$

where

29.7 = min system plus T, i.e. no system plus T

33.3 = max system minus T, i.e. V2 and V3.

Since we get a negative value there is no point in proceeding further. The include criteria have failed and we proceed to try the exclude criteria:

$$(33.3 - 33.3) \times 10^{-4} = 0 < 4.4 \times 10^{-4}$$

where

$$33.3 = \text{value } (P + T), \text{ i.e. } (\underbrace{V2 + V3}_{P}) + \underbrace{V3}_{T}$$

$$33.3 \text{ (the subtrahend)} = \text{value } (P - T), \text{ i.e. } V2 + V3$$

$$4.4 \times 10^{-4} = \text{cost of } T$$

This indicates the V1 will definitely not be in the optimum system. It will be recalled that the optimum system, neglecting transducer failures, contained V2 and V3; this point may be verified by application of the include criteria to V2 and V3.

The question might reasonably be raised, "Why bother with the system reduction step? Simply proceed to the final evaluation of all systems on the digital computer." The answer is that it takes too long. The somewhat simplified example, which is cited in Section II, covering a whole engine started out with 10 candidate transducers. There are 1024 systems which would require full evaluation if no preliminary reduction were accomplished. This would require 178 hours ($10,000) in computer time and about one-half man-year of engineering time to prepare the input data. After the system reduction step there were only 10 systems remaining which required complete evaluation. Since the number of systems increases exponentially (a 20-transducer set yields 1,048,576 systems) the reduction step is essential.

SECTION IV

DEVELOPMENT OF SYSTEM DESIGN TECHNIQUE

4-1. INTRODUCTION

The system design technique, including both the detailed system evaluation procedure and the system synthesis technique, is developed in this section. It should be recalled from Section III that this procedure is based on relating malfunction/decision pairs to risk. As illustrated by the two examples presented in paragraph 3-1, there are eight basic sets of input information required for the evaluation and synthesis of READI systems. These are

- The set of propulsion system malfunctions and their probabilities of occurrence
- The set of malfunction detectors available and their coverage
- The set of alternative actions available
- The losses associated with each malfunction/decision pair
- The basic system cost and the adjusted cost of each transducer employed by the malfunction detectors
- The mission plus vehicle replacement value
- The failure characteristics and probabilities for each transducer
- Loss weighting factors.

This information is obtained from basic data and analyses concerning the mission, vehicle, and READI system with the aid of several mathematical models. The purpose of these mathematical models is to set up a well-defined and orderly method of obtaining the above information from the more basic information. This approach is necessary because of the large amount of input data required in any real design problem. This approach

also facilitates the preparation of standard digital computer programs to conduct the majority of numerical computations necessary.

The mathematical models interact to some extent. However, it is possible to classify them, for purposes of discussion, into three more or less distinct groups. These groups are

- The Mission Model
- The Propulsion System and Vehicle Model
- The READI Model.

These models are discussed in paragraph 4-2. In paragraph 4-3, the models are brought together and the equations for computing risk are obtained. The computer programs which have been written for the determination of risk are briefly described in paragraph 4-4. Finally, paragraph 4-5 describes, in detail, the system synthesis scheme.

The material presented in this section is quite detailed. The level of detail is that which would be employed in the design of a system for a real mission/vehicle complex after considerable data had been collected. However, it is important to note that it is possible to employ the design and evaluation procedures in levels of detail less than those given here. In general, this is accomplished by neglecting certain detailed features of the READI system, the vehicle, and the mission. For example, in considering the general value of READI for a particular stage, it can be assumed that there are ideal READI systems in the other stages. Some additional points where simplification can be introduced early in the study of a particular application are indicated in the text; however, the actual simplification will be dependent upon the particular application.

4-2. MATHEMATICAL MODELS

A. MISSION MODEL

The first step in the construction of the mission model is the division of the mission into operationally meaningful periods. This division is summarized in figure 4-1.

The first division of the mission is into boost and post-boost periods. The boost period is further divided into stages corresponding to the physical operation of the stages of the booster. Finally, each stage is divided into several operationally meaningful phases. During the

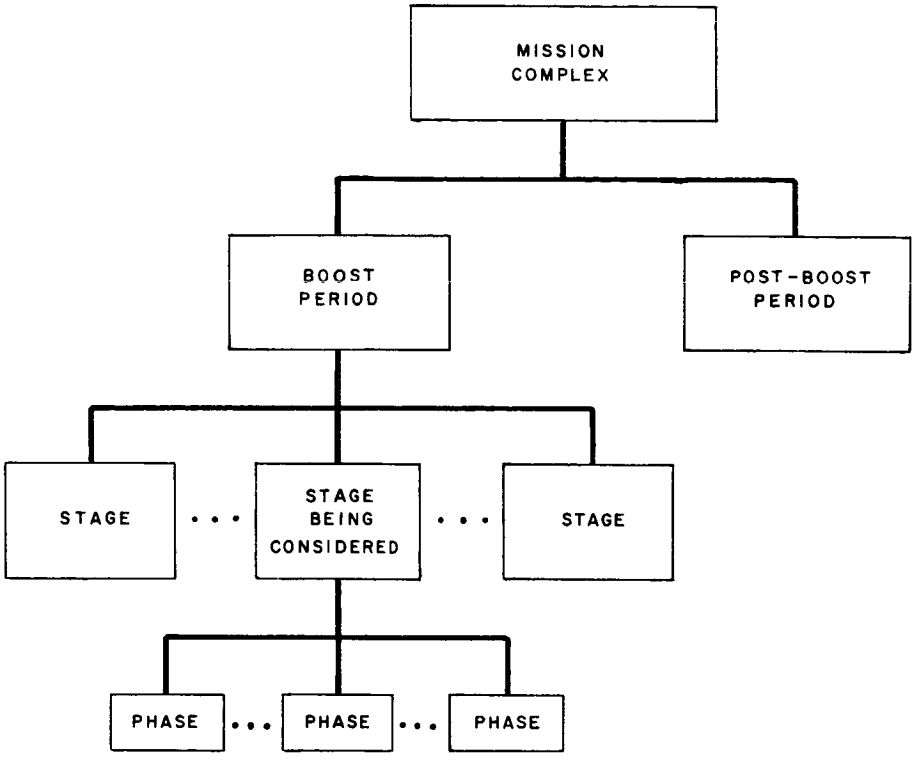


FIGURE 4-1
STRUCTURE OF MISSION MODEL

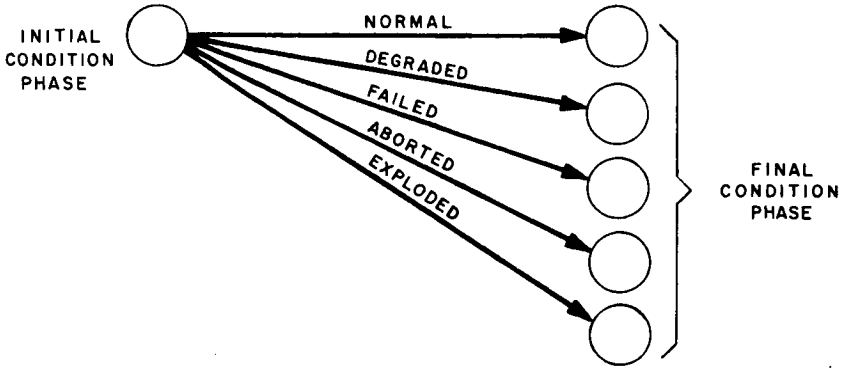


FIGURE 4-2
TYPICAL PHASE MODEL

earlier portions of the program, these phases for a second-stage propulsion system were prestart, start, operate and shutdown. However, further examination of the over-all evaluation problem showed that, for the second stage, the following phases are more useful for the example considered here: prestart, start to mainstage, mainstage, except for the last 10 seconds, and the last 10 seconds of mainstage plus stage cutoff. During prestart and start to mainstage, an alternate mission single engine-out capability exists. During mainstage, a prime mission single engine-out capability exists.

The phase is then the basis of the mission model. Therefore, the structure of the phase model will be considered first. Each phase model consists of an initial condition node, called the normal initial condition node, and several final condition nodes. These nodes are taken to represent the operational condition of the vehicle with respect to its assigned mission. For the mission studied here, these final condition nodes, for each phase in the second stage, are taken as normal, degraded, failed, aborted, and exploded. The phase model is then made up of the probabilities of transition from the normal, initial condition node to each of the final condition nodes.

The transition from the normal initial condition node to the jth final condition node of the pth phase of the qth stage is denoted by $t_{j,q,p}$ and its probability by $P(t_{j,q,p})$. A list of all symbols employed in Section IV is given under paragraph 4-7, List of Symbols. The convention on the numbering of the final condition nodes is as follows:

Node	Value of j
Normal	0
Degraded	1
Failed	2
Aborted	3
Exploded	4

The convention on the numbering of the phases in the second stage is as follows:

Phase	Value of p
Prestart	1
Start to mainstage	2
Mainstage less last 10 sec	3
Last 10 sec of mainstage plus stage cutoff	4

Thus, $P(t_2;\ _3,\ _2)$ is the probability of the transition from the normal, initial condition node to the failed final condition node of the mainstage phase of stage two. A schematic representation of a typical phase model is shown in figure 4-2.

The stage models are similar in structure to the phase models. Both consist of several initial condition nodes and several final condition nodes. The final condition nodes of the stage models are the same as the final condition nodes of the phase models. Again, the stage model is made up of the probabilities of transition from each of the initial condition nodes to each of the final condition nodes.

The stage model is built up from the phase models on the basis of two assumptions. The first of these is that, at most, one phase transition other than the transition from the normal initial condition node to the normal final condition node can take place in each stage. This assumption is reasonable on the basis of the propulsion system malfunction probabilities being quite low. On the basis of this assumption the stage transition probabilities from the stage normal initial condition node to each of the stage final condition nodes can be computed. This operation is shown schematically in figure 4-3. Denoting the transition from the stage normal initial condition node of stage q to the jth stage final condition node of stage q by $t'_j;\ _q$, and denoting its probability of occurrence by $P(t'_j;\ _q)$, then, on the basis of this assumption, for stage two

$$P(t'_o;\ _q) = \prod_{P=1}^{4} P(t_o;\ _q,\ _p)$$

and for j greater than zero

$$P(t'_j;\ _q) = P(t_j;\ _q,_1) + \sum_{P=2}^{4} \left[P(t_j;\ _q,\ _p) \prod_{i=1}^{P-1} P(t_o;\ _q,\ _i) \right]$$

Here the convention on j is taken to be the same as in the phase model, and is made of the fact that there are four phases in stage two.

The second assumption enables one to compute the transition probabilities from the other stage initial condition nodes. But first the convention that the stage initial condition nodes are the same as some of the previous stages final condition nodes is established. In the case of

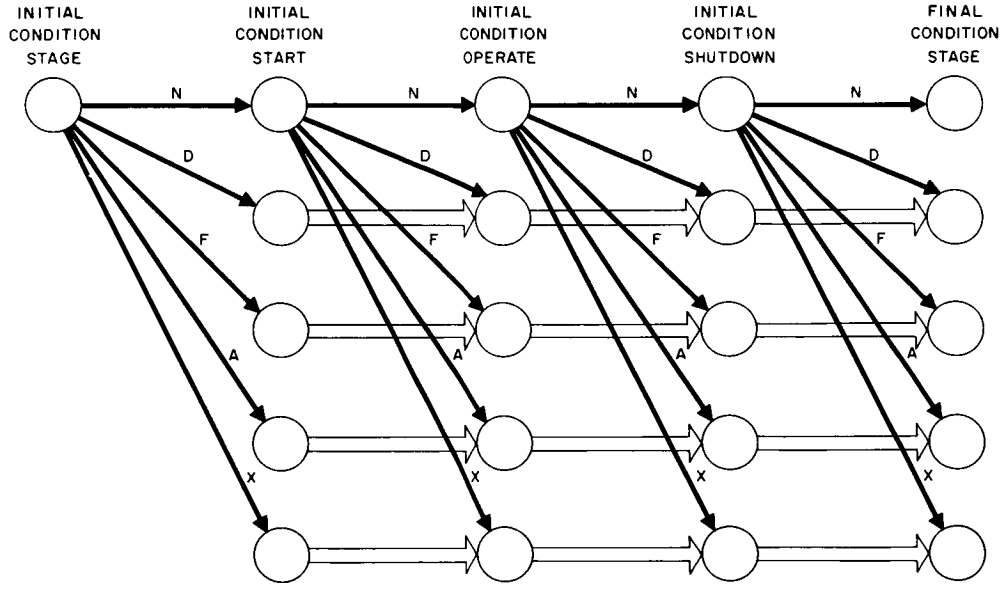


FIGURE 4-3
CONSTRUCTION OF STAGE MODEL

the first stage, only a single, normal initial condition node is employed. In particular, the normal, degraded and failed conditions are common from stage to stage. The aborted and exploded conditions are not included since the mission is terminated if these conditions occur. Then, for the degraded and failed initial condition nodes the conventions indicated in table 4-1, in terms of the phase transition taking place, are established. This procedure is also summarized in figure 4-4.

Table 4-1

Phase Transitions

Stage Initial Condition	Transition	Stage Final Condition
Degraded	Normal	Degraded
	Degraded	Failed
	Failed	Aborted
	Aborted	Aborted
	Exploded	Exploded
Failed	Normal	Failed
	Degraded	Aborted
	Failed	Aborted
	Aborted	Aborted
	Exploded	Exploded

The probabilities of a transition from stage initial condition nodes, other than the normal, to each of the stage final condition nodes now follow directly. Let $t'_{1,\ j;\ q}$ denote the transition from the 1th stage initial condition node of stage q to the jth stage final condition node of stage q and let $P(t'_{1,\ j,\ q})$ denote its probability. Then, using figure 4-4, one has, for example,

$$P(t'_{1,\ 3;\ 2}) = P(t'_{3;\ 2}) + P(t'_{4;\ 2})$$

and

$$P(t'_{2,3;2}) = P(t'_{1;2}) + P(t'_{2;2}) + P(t'_{3;2})$$

The other values of $P(t'_{1,j;q})$ are similarly constructed.

The boost period model is then obtained by joining the various stage models, making use of the commonality of the stage initial and final condition nodes. The mission terminating nodes lead to mission final end states as shown in figure 4-5.

The structure of the post-boost period model is again similar to that of the stage models, which consist of a set of initial condition nodes, a set of final condition nodes, and transition probabilities between the initial condition and final condition nodes. The initial condition nodes are the same as the final condition nodes of the last stage of the boost period less the mission terminating nodes. The final condition nodes are the end-states of the mission and are taken in the present example as

- Successful Prime Mission
- Successful Alternate Mission
- Mission and Vehicle Loss, and Safe Return of the Crew
- Mission Vehicle, and Crew Loss.

The boost and post-boost period models are then joined, making use of the commonality of the initial condition nodes to obtain the total mission model. The resulting model is shown schematically in figure 4-6.

Losses are now assigned to each mission end state. The reference level, i.e. zero, for these losses is taken as a successful prime mission and the unit of loss is taken as the mission replacement value. In the assignment of losses to the mission end states, the fact that the loss is a vector quantity must be taken into account. Usually it has two or more components which are normally measured in different units. This point is discussed in more detail in Appendix A. The design criterion chosen for READI is the minimization of the total expected loss. Since the minimization can be performed only on a scaler quantity, the loss vector is converted to a scaler quantity by the application of weighting factors to each of the components of loss.

In the current evaluations the loss vector has two components, mission loss and crew loss. These have been combined to a scaler by the crew-to-mission value ratio λ_c. For example, a crew-to-mission value ratio of zero is typical of an unmanned mission, while a crew-to-mission value ratio of one indicates a willingness to sacrifice the mission to save the crew. The ratio, λ_c, makes it possible to vary the emphasis placed on the

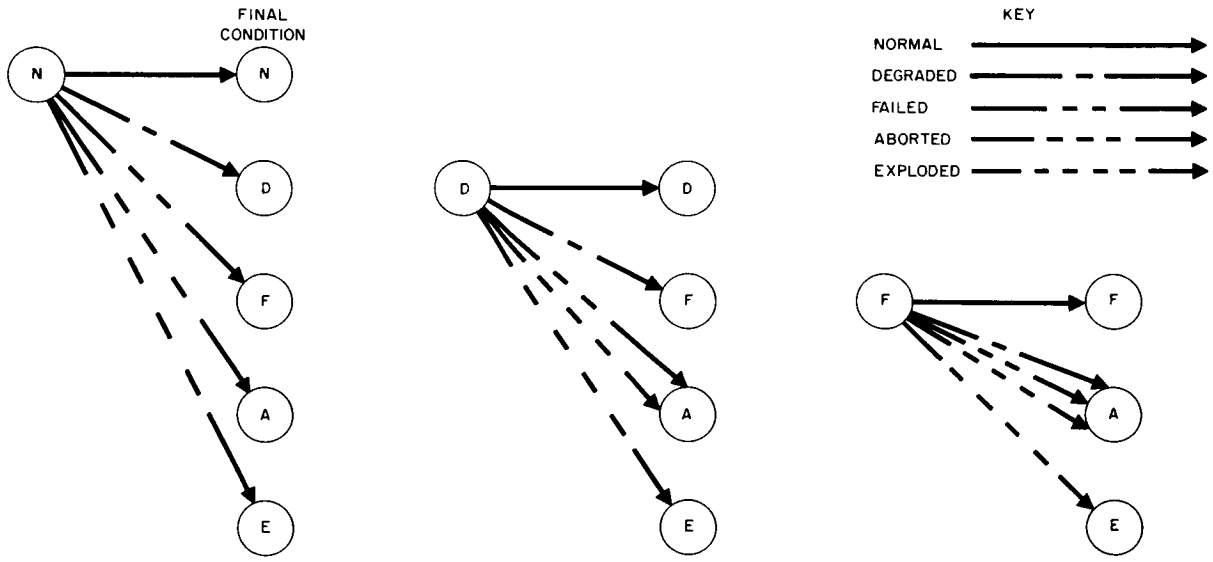


FIGURE 4-4
CONSTRUCTION OF STAGE MODEL(NON - NORMAL INITIAL CONDITION)

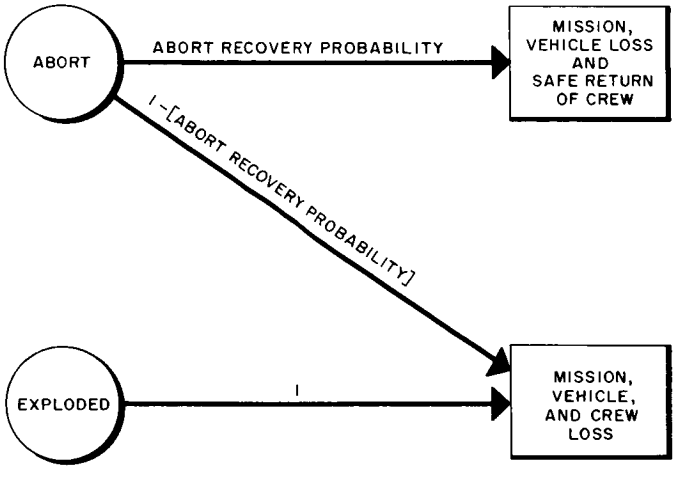


FIGURE 4-5
TREATMENT OF MISSION TERMINATING NODES

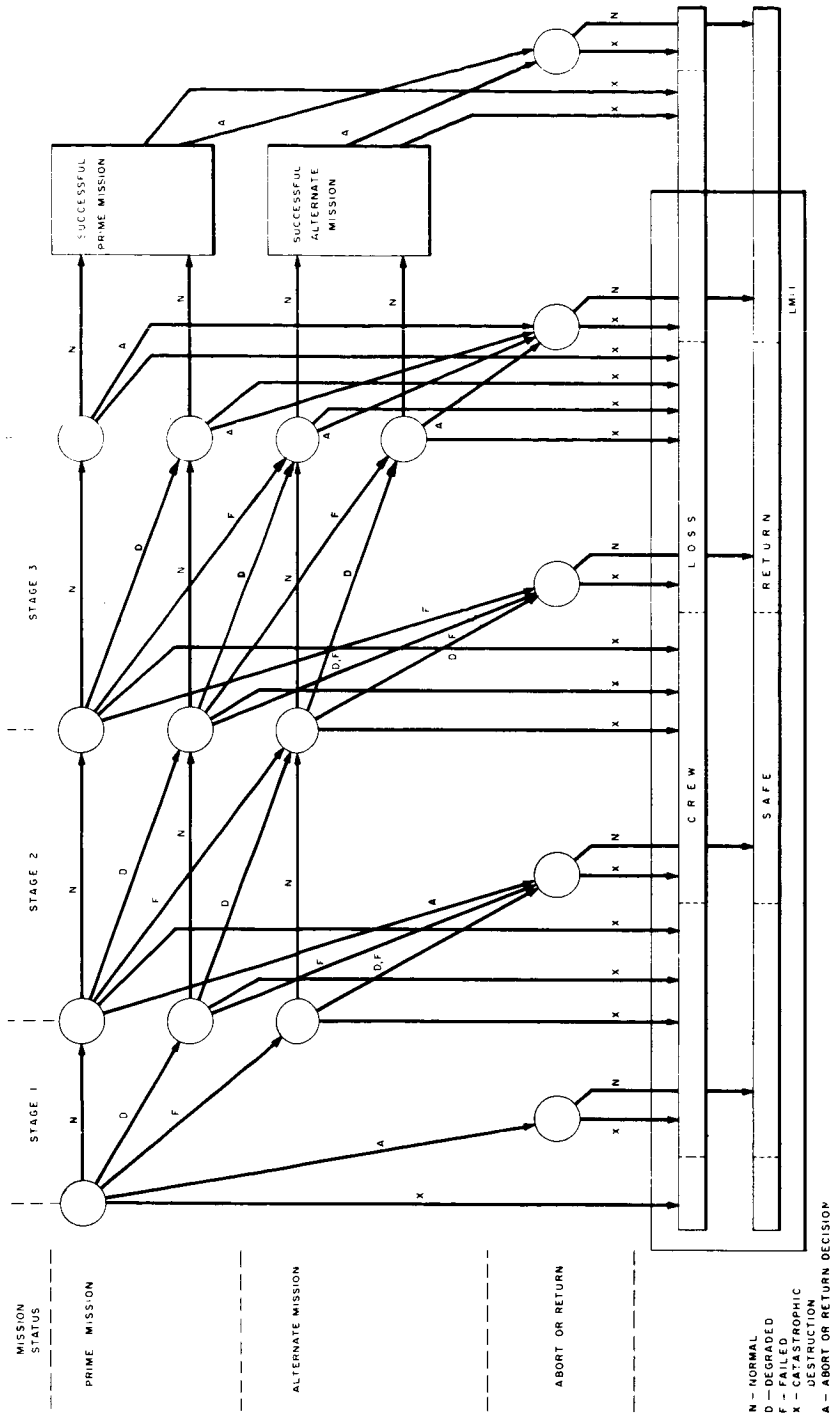


FIGURE 4-6
OVERALL MISSION MODEL

safe return of the crew in relation to the accomplishment of the prime mission in a systematic manner. A crew-to-mission value ratio of 10 is used as a basic value here. The assignment of losses involving both the state of the mission and the crew as a single number is based on the assumption that the basic required mission accomplishment and crew survival probabilities are separately met by the vehicle. In the present mission model, the following losses were assigned to the mission end states:

End State	Loss
Successful Prime Mission	0.0
Successful Alternate Mission	0.8
Mission Vehicle Loss and Safe Return of Crew	1.0
Mission, Vehicle, and Crew Loss	11.0

Now, by knowing the various transition probabilities and the abort recovery probability, the risk at any phase or stage condition node may be computed. An example of this procedure is shown in figure 4-7.

In order to be able to apply to the computation of risk the framework built up using the mission model, it is necessary to be able to calculate the phase transition probabilities. To accomplish this, the other two models are required. These are described in the following paragraphs.

B. PROPULSION SYSTEM AND VEHICLE MODELS

The purpose of the propulsion system and vehicle models is to represent the malfunctions of the propulsion system and determine their consequences for each possible READI decision. This information is used in system evaluation and synthesis, and in the design of malfunction detectors. The generation of the information required in system evaluation and synthesis is discussed in subparagraphs 1 and 2 below. The representation of their malfunction detectors is discussed in subparagraph 3.

1. Definition of Propulsion System Malfunction

One of the basic sets of data required for the determination of the transition probabilities is the probability of each propulsion system malfunction. To obtain these data, it is first necessary to define clearly what is meant by a propulsion system malfunction. This definition is rooted in the malfunction effects tree, a portion of which was shown in figure 3-3. To describe the definition of malfunction, a different representation of

such a tree is shown in figure 4-8. In this figure, an elementary level of propulsion system malfunctions has been introduced. These are taken to represent such malfunctions as broken springs or ruptured pressure diaphragms, and may be considered to be the elementary cause of the propulsion system malfunctions. Intermediate and final effects are shown below them in figure 4-8.

Different levels of intermediate effects are labeled with different letters and a numeral. Final effects or losses are denoted with an L and a numeral. Losses are divided into categories (such as loss of thrust) which are defined to facilitate the computation of the effects of the malfunction on the stage and mission. For convenience, the loss categories are sometimes subdivided into intervals such as Δ thrust < 5 percent, Δ thrust = 5 to 20 percent, etc. The level of the malfunction effects chosen for the definition of propulsion system malfunctions for the purpose of further analysis is shown just below the level of the elementary malfunctions. The basic characteristic of this level is that those elementary malfunctions causing a particular malfunction cause no other malfunction.

It is assumed that the malfunctions so defined are useful in the design of malfunction detectors. Finally, on the basis of the definition of malfunctions, it is assumed that malfunctions are independent events.

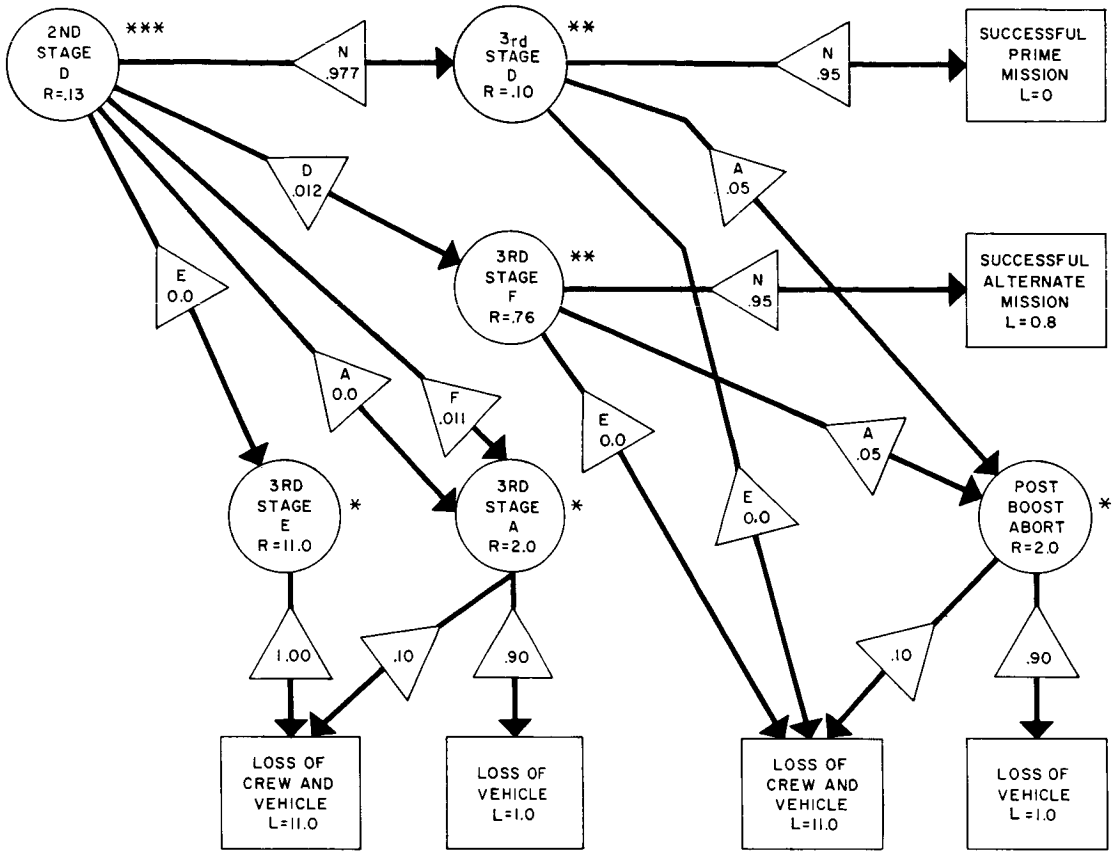
2. Computational Procedure

It is now necessary to compute a set of propulsion system losses for each propulsion system malfunction/READI decision pair. The set of decisions available is determined from an engineering analysis of the propulsion system, vehicle, and mission. The decisions are generally dependent upon the phase of the stage being considered. The set of propulsion system losses employed here is

- Percent loss of total stage thrust
- Ratio of lox flow overboard to total lox flow
- Ratio of fuel flow overboard to total fuel flow
- Percent Isp loss*
- Explosion probability.

- - - - - - -

*Isp losses were very small compared to the other loss components and were neglected.



STEP 1
COMPUTE RISK AT * NODES
STEP 2
COMPUTE RISK AT ** NODES
STEP 3
COMPUTE RISK AT *** NODE

KEY
N = NORMAL
D = DEGRADED
F = FAILED
A = ABORT
E = EXPLODED

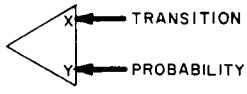


FIGURE 4-7
COMPUTATION OF RISK AT R (1,2)

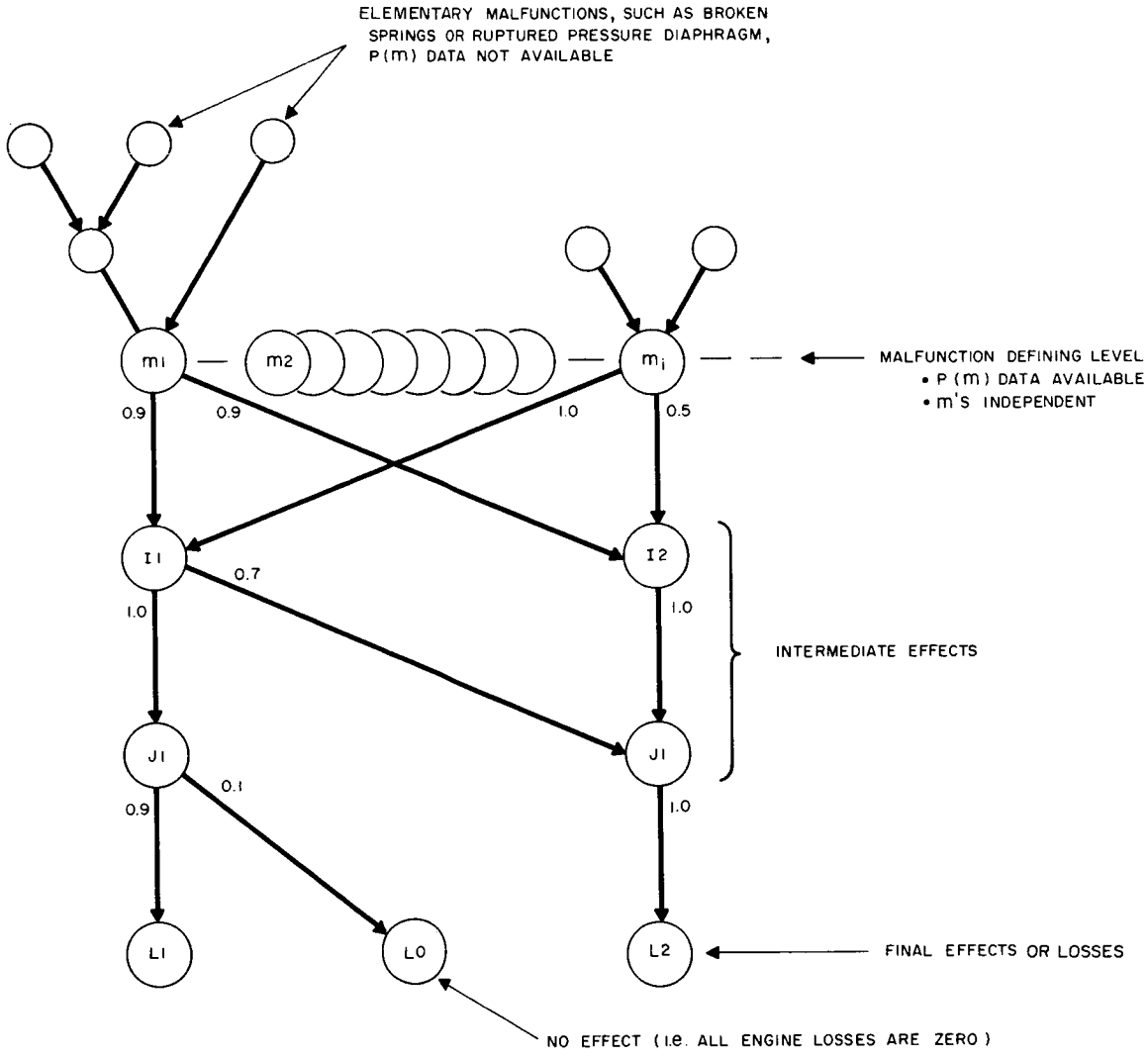


FIGURE 4-8
PORTION OF MALFUNCTION EFFECTS TREE

To see how this association is carried out, consider first the calculation of the above losses when no action is the READI decision. In figure 4-8, the probability of one node causing another node is shown on the lines connecting each node. First, it will be noted that there is no separation of causes in the intermediate effects and final effects region. Secondly, the probability of one node causing another is not unity in each case. There are two basic reasons for this fact. The first is the inability on the part of even the most experienced propulsion system analyst to determine with certainty the effect of each propulsion system malfunction; the second reason is that for certain malfunctions (in particular, continuous amplitude malfunctions), the effects are random from engine to engine and launch to launch. These two phenomena together are called stochastic malfunction effects.

If it were not for the fact that malfunction effects are stochastic in nature, the association of propulsion system losses with malfunctions with no READI action would be fairly straightforward. The final effects could be chosen to represent suitable numerical intervals of each propulsion system loss defined above. Thus, one might have a final effect of an explosion probability between 0.1 and 0.2. In order to associate a single number for each such loss, the arithmetic mean of the interval limits would be used for each node. Then, since the final effects representing intervals of the same engine loss parameter are disjoint, (that is, one could not have, for example, a thrust loss between 10 percent and 20 percent and at the same time have a thrust loss of 0 percent), one could associate a single such interval with each malfunction.

To account for the stochastic nature of malfunction effects, it is necessary to introduce some additional complications when considering the system in detail. It is desirable to accomplish this in a manner which least obscures the physical content of the basic malfunction effect. Thus, each malfunction is partitioned into submalfunctions such that

- Each submalfunction always leads to one and only one set of engine loss parameters (that is, it is not stochastic)
- The probability of each submalfunction is the conditional probability that the partitioned malfunction leads to the engine loss parameters of the submalfunction multiplied by the probability of the partitioned malfunction.

To see how this partitioning of malfunctions is carried out, consider malfunction m_1 in figure 4-8. Suppose L_1 and L_2 represent two intervals of different propulsion system loss parameters. Then, suppose m_1 occurs. To show this computational procedure clearly, the representation of the malfunctions effects tree shown in figure 4-9 is introduced. In this figure, the intermediate effects have been broken down into disjoint events. Further, "no intermediate effect" nodes I_o and J_o have been introduced for completeness. Revised probabilities of one node causing another are shown. These probabilities are based on the assumption that the transitions from one level to the next take place independently. Thus, for example

$$P(I_1 \text{ and } I_2) = (0.9) \cdot (0.9) = 0.81$$

$$P(I_2 \text{ and not } I_1) = (0.9) \cdot (1 - 0.9) = 0.09$$

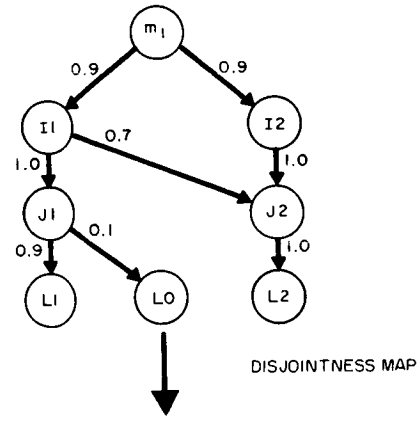
$$P(I_1 \text{ and not } I_2) = (0.9) \cdot (1 - 0.9) = 0.09$$

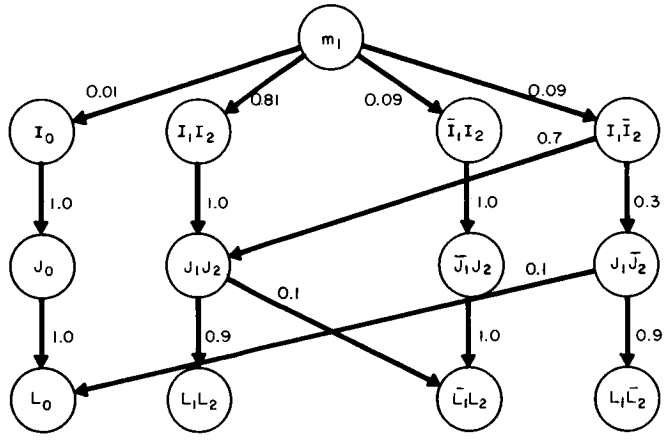
The sum of these three probabilities is 0.99. Since the intermediate effects on any level are now disjoint, the probability that a node on one level leads to some node on the next level must be one. Therefore, by subtraction, the probability that m_1 causes I_o is 0.01. The other probabilities shown in figure 4-9 are obtained in the same manner.

Now, assuming that m_1 has occurred, the transitions from one level to the next are independent of the transitions which took place at the higher levels. The conditional probabilities of each final effect node, as shown in the figure, can now be computed. Thus, in this example, m_1 is divided into four submalfunctions:

Submalfunction	Always Causes	Probability
$m_{1.0}$	L_0	$0.0127 \cdot P(m_1)$
$m_{1.1}$	L_1 and L_2	$0.7857 \cdot P(m_1)$
$m_{1.2}$	L_2 and not L_1	$0.1773 \cdot P(m_1)$
$m_{1.3}$	L_1 and not L_2	$0.0243 \cdot P(m_1)$

To consider decisions other than no action, the effect of the decision can be introduced by reconstructing the tree in the region "down stream" of the node or nodes where the executed decision modifies the cause and effect relationships which are used to construct the tree. Again, this detailed treatment is only required when working on a highly detailed level.





$P(L_0/m_1) = 1.0 \times 1.0 \times 0.01 + 0.1 \times 0.3 \times 0.09 = 0.0127$

$P(L_1L_2/m_1) = 0.9\,(1.0 \times 0.81 + 0.7 \times 0.09) = 0.7887$

$P(\bar{L}_1L_2/m_1) = 1.0 \times 1.0 \times 0.09 + 0.1\,(0.7 \times 0.09 + 1.0 \times 0.81) = 0.1773$

$P(L_1\bar{L}_2/m_1) = 0.9 \times 0.3 \times 0.09 = 0.0243$

1.0000

FIGURE 4-9
MALFUNCTION EFFECTS TREE

3. Representation of Malfunction Detectors

Three levels of detail in the representation of the malfunction detectors are employed in the design of a READI system. These are the levels associated with

- The first step in the synthesis procedure described in paragraphs 3-2 and 4-5
- The second step in the synthesis procedure; that is, the detailed evaluation of systems described in paragraphs 3-2 and 4-2
- The actual design of hardware.

In the first step of the synthesis procedure, it is necessary only to know which malfunctions or submalfunctions are detected by each malfunction detector. In the second step of the synthesis procedure, it is necessary to add information concerning the transducers employed by each malfunction detector and their failure characteristics as detailed in subparagraph 4-2,D. Finally, when carrying out the design of equipment, very detailed information is required. The following paragraphs discuss the basis of the representation used in the first step of the synthesis procedure. Subparagraph 4-2,D discusses the consideration of transducer failures, while equipment design is discussed in Section V.

The statistical malfunction effects tree is the major source of information used in synthesizing malfunction detection for a new system. Other main sources of design information are the engine test stand procedures and engine test data. The malfunction tree is used to define a variety of malfunction detectors, whereas analysis of test data and the use of other models of the propulsion system supply the comparator-stored reference or decision limit, information. The other models vary in complexity from simple mathematical representations of the operation of the engines when malfunctions occur to digital computer models which accomplish the same thing with greater accuracy and detail.

It is convenient to gather all of the available malfunction detectors together on one chart. This is shown in the sketch below and in detail in figure 4-10.

V / m		S_L			
		1	2	3	4
m_o					
m_i				1	

Many malfunction detectors are simply noted as a signal S_L with a subscript (1 to 4) for various processing limits. A 1 appearing in the body of the chart indicates that the malfunction detector (that is, S_L processed to a specified limit) will occur when the malfunction occurs. Care is used in selecting decision limits to match properly with variable amplitude malfunctions, such as propellant leaks. The objective here is to avoid the stochastic splitting of malfunctions in a manner analogous to the way intermediate effects are presented in the malfunction effects tree. The method described previously in subparagraph 2 is applicable to stochastic sensible effects; however, it leads to a representation of malfunctions and malfunction detectors which is too complex for the initial optimization step, where a very large number of malfunction detectors is under consideration. Further automation (that is, reduction of the procedure to computer operations) is required for the first step in the synthesis scheme and for the writing of decision rules (which are required in the second step) before the stochastic sensible effects can be included in the over-all synthesis procedure.

A 1 in figure 4-10 also implies that the malfunction indication occurs in time for an appropriate corrective action to be taken. This point is best illustrated by considering an entry in the chart. A 1 appears in column 3 under turbine speed for fuel pump cavitation, meaning that a "high turbine speed" indication will be noted when the pump cavitates. However, this is a transient overspeed condition followed by a rapid loss

	HIGH #2 VIB.		TURBINE SPEED				GG TEMP				CH. #2 PRESS				FUEL INJ ΔP				LOX INJ ΔP				ENGINE FUEL FLOW				ENGINE LOX FLOW				FLOW DISC. PRE-VALVE TO INJECTOR				PUMP INLET PRESS				GG S.O. VALVE OPEN, NO FIRE CKT. VOLTAGE	IGNITER VALVE OPEN, NO FIRE CKT. VOLTAGE	PREMOTOR CH 2 FLOW	NO FUEL PRIME	TURBOPUMP VIB.	TURBINE EXHAUST FAILURE	HELIUM PRESS		STAGE COMMON				ELEC PWR 28V DC
																															FUEL		LOX		FUEL		LOX												ULLAGE		PRESSURE		
																															>5%	>30%	>5%	>30%																				
MALFUNCTION	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	-	5.1	5.2	5.3	-	6.1	6.2	6.3	-	7.1	7.2	7.3	7.4	8.1	8.2	8.3	8.4	9.1	9.2	10.1	10.2	11.1	11.2	12.1	12.2	13.0	14.0	15.0	16.0	17.4	19.0	20.1	20.2	21.1	21.2	22.1	22.2	23.1
CLOGGED CH #2 FUEL INJECTOR (20%)	1											1																																										
ENGINE FUEL LEAK (5%)																									1						1																							
ENGINE FUEL LEAK (30%)																1									1	1					1	1																						
CLOGGED CH 2 LOX INJECTOR (20%)												1																1																										
ENGINE LOX LEAK (5%)																													1				1																					
ENGINE LOX LEAK (30%)																				1									1	1			1	1																				
FUEL PUMP CAVITATION	1				1																			1																														
LOX PUMP CAVITATION					1															1								1																										
GAS GENERATOR STRUCTURAL FAILURE			1	1				1																																														
TURBOPUMP GEAR BEARING FAILURE			1	1																																							1											
TURBOPUMP STRUCTURAL GAILURE			1	1																																																		
TURBINE, NOZZLE EROSION				1								1				1				1								1																										
GG INJECTORS, ERODED FUEL, CLOGGED LOX				1				1				1				1				1								1																										
GG VALVE OPEN (DURING PRESTART)																																							1															
PRE-VALVE CLOSED (FUEL AND LOX)					1						1	1			1	1			1	1			1	1			1	1							1	1	1	1																
IGNITER PROP VALVE OPEN (DURING PRESTART)																																								1														
MAIN PROP VALVE, CLOSED					1						1	1			1	1			1	1			1	1			1	1																										
MAIN PROP VALVE, OPEN																																										1											
PRIME VALVE, CLOSED																																																					
COMBUSTION INSTABILITY	1	1																																																				
CHAMBER BURNOUT																									1						1																							
INJECTOR EROSION, FUEL, CH #2																									1						1																							
INJECTOR EROSION, LOX, CH #2	1												1																1				1											1									
TURBINE EXHAUST FAILURE																																																					
GG INJECTOR CLOGGED FUEL, ERODED EX					1					1			1					1				1			1				1																										
GG FUEL LEAK (INCL. BOOTSTRAP LINES)									1	1																																												
GG OX LEAK (INCL. BOOTSTRAP LINES)			1	1			1	1			1	1			1	1			1	1			1	1			1	1																										
U12, U17 OR U18 CLOSED (LOSS HE PRESS)				1				1																																					1	1							
LOSS, LOW ELECTRIC POWER				1				1																																														
QD 2, U19 OR U21 OPEN, FUEL (60% OF ONE ENGINE)																																				1													1				
LINE OR TANK LEAK, FUEL (60% OF ONE ENGINE)																																				1													1				
LINE OR TANK LEAK, FUEL (180% OF ONE ENGINE)																1								1											1	1												1	1				
QD 1, U20, U22 OPEN, LOX (60% OF ONE ENGINE)																																						1														1		
LINE OR TANK LEAK, LOX (60% OF ONE ENGINE)																																						1														1		
LINE OR TANK LEAK, LOX (180% OF ONE ENGINE)				1				1				1								1								1									1	1														1	1	

UNLESS OTHERWISE NOTED THE FOLLOWING LIMITS ARE IMPLIED

X.1 - VERY LOW OR LOSS
X.2 - LOW
X.3 - HIGH
X.4 - VERY HIGH

FOR 1 THRU 10 THE LOW AND LOSS LIMITS ARE VALID ONLY DURING MAINSTAGE

FIGURE 4-10
COMPLETE SET OF SIGNAL SPACE SEPARATIONS FOR MODEL PROPULSION SYSTEM

of turbine speed. Note that a 1 is not found in the low or very low columns. The reason for this is twofold:

- Many malfunctions result in loss or low speed while relatively few result in high speed. Therefore, from the viewpoint of discrimination, the high limit is more useful.
- Since it is desirable to close the gas generator propellant valves as fast as possible to limit engine damage, the indication which appears first is used.

Finally, it should be noted that all of the malfunction indications are assumed to occur simultaneously. In effect this simplification compresses all of the lags and transport times in the engine to zero. If a valuable discrimination can be made by monitoring a variable at several limits as a function of time, these simply appear as additional entries in figure 4-10.

To summarize, the conditions implicit in the chart are

- Decision limits are selected for each variable
- Limits are selected to avoid stochastic occurrence of indications
- Indications appear in time for corrective action
- All indications occur at once.

C. DETERMINATION OF TRANSITION PROBABILITIES FOR MALFUNCTION DECISION PAIRS

Having discussed the manner in which engine losses are estimated, attention is now turned to the procedure used to relate these losses to the phase transition probabilities. This step provides the link between indicated engine performance and expected mission performance.

This process is considered in detail in Appendix B. Functional as well as explicite relationships are shown to demonstrate the principles involved, and a numerical example is also given.

The procedure used to calculate transition probabilities for the model mission-vehicle-engine used to demonstrate the value of READI and to illustrate the design procedure will be discussed in this section. The particular characteristics of the given mission phase (the time between prime mission engine-out capability and cut off) were used to circumvent the complexity inherent in solving the general problem.

The transition (j) probabilities employed in the example considered here are defined physically as shown in table 4-2.

Table 4-2

Definition of Transition Probabilities

$P(t_j/m_i\ d_k)$		
j	Name	Description
0	Normal	All prime mission objectives can be achieved if succeeding performance is degraded or normal
1	Degraded	All prime mission objectives can be achieved if succeeding performance is normal
2	Failed	All alternate mission objectives can be achieved if succeeding performance is degraded or normal
3	Aborted	Mission terminated by attempting abort
4	Exploded	Mission terminated by catastrophic destruction. Crew lost.

The breakdown of table 4-2 is detailed enough to provide accurate assessment of mission performance but not so sophisticated as to be inconsistent with confidence levels on data used in the probability estimation.

Transitions 3 and 4 are different from 0, 1, and 2 because the mission is terminated. The losses incurred when these transitions are obtained do not depend on the transitions in the stages which follow.

The probability of transition 4 is estimated directly by tracing through the malfunction effects analysis, as discussed previously. The other transitions are determined by first determining transition probabilities conditioned on no explosion occurrence and then multiplying by the probability of no explosion (1-probability of explosion). The conditional

probabilities of transitions are determined by the percent stage thrust lost and the percent total stage mass flow lost overboard. These two engine parameters were the only important performance measures for the model used in this study. Furthermore, examination of these parameters indicated that there were only three cases of interest: no losses, small losses, and large losses. Taking advantage of these properties, table 4-3 was prepared. An example is worked out in part (b) of this table. The specified conditional probabilities actually serve to define quantitatively the transitional modes for the phase and stage being treated. They are consistent with reasonable constraints on stage cut-off conditions.

Table 4-3

Development of Transition Probabilities

		Percent Stage Thrust Loss				
		0	≤ 0.20	> 0.20		j
	0	1	0	0	Normal	0
		0	1	0	Degraded	1
		0	0	0	Failed	2
		0	0	1	Aborted	3
Percent Stage Flow Leak	≤ 0.10	0.9	0	0	Normal	0
		0.1	0.9	0	Degraded	1
		0	0.1	0	Failed	2
		0	0	1	Aborted	3
	> 0.10	0	0	0	Normal	0
		1	0	0	Degraded	1
		0	1	0	Failed	2
		0	0	1	Aborted	3

(a) Transition probabilities conditioned on no explosion

$P(t_j/m_i\ d_k\ \overline{E})$

Malfunction 14 - Turbopump structural failure

Decision 0 - No action

Thrust Loss = 0.20

Leak = 0.04 (ox and fuel)

Explosion Probability = 0.5

Table 4-3 (Cont.)

Development of Transition Probabilities

j =	0	1	2	3	4
$P(t_j/m_i\ d_o)$ =	0	0.45	0.05	0	0.5

(b) Example of $P(t_j/m_i\ d_k)$ computation

Although great simplification has been introduced in the computation of transition probabilities, the results are quite realistic. Spot checks have been made in certain areas to show the reasonableness of the results.

D. THE READI MODEL

The READI model will be used to describe the READI system for the purposes of risk computation, cost computation, and system synthesis. Since each of these is a separate function, there are, in reality, three representations involved. These are

- The evaluation representation
- The cost representation
- The synthesis representation.

The synthesis representation is described in detail in paragraphs 3-2 and 4-5. The other two representations are discussed in the following paragraphs.

The evaluation representation has two purposes. The first of these is to obtain the probability of each READI transducer failure mode. The second is to determine the effect of each transducer failure mode on the decision indicated by READI.

The transducer failure probabilities take the following form. Consider first a simple transducer for which there are no corresponding redundant transducers and no self-check mode has been introduced. For such a transducer two failure modes are introduced. These are the very high failure mode and the very low failure mode. When a transducer is failed in the very high failure mode its output is taken to be such that it appears to be above the highest threshold employed with that transducer. Similarly, when a transducer is in the very low failure mode its output is taken to be such that it appears to be below the lowest threshold employed

with that transducer. Two failure modes rather than one are introduced for two reasons. First, the majority of transducer failures can be accommodated in these two modes. Second, the failure of a transducer in one mode may effect the output of READI in a different manner than failure in the other mode. Thus with each simple transducer there are associated two failure probabilities, i.e., the very high failure probability and the very low failure probability.

It is assumed that once a transducer fails in a given mode it remains failed in that mode. For this reason the transducer failure probabilities are taken to be mission phase dependent and are denoted by $P(S_{L;q,p})$, where L denotes the particular failure mode of the particular transducer, and, again, q and p denote the stage and phase. Then $P(S_{L;q,p})$ is defined to be the probability of transducer failure mode L occurring during or before phase p of stage q. Finally, for simple transducers, it is assumed that the totality of the transducer failure modes occur independently. The assumption of independence is based on the fact that simple transducers each perform different functions and will therefore be somewhat dissimilar and located in different areas of the propulsion system.

In order to discuss further the transducer failure model employed only in the case of a detailed design of a system, it is necessary to recall the types of redundancy employed in READI systems. There are three such types of redundancy: information redundancy, transducer redundancy, and transducer self-check, which is a special form of information redundancy. Each of these redundancy techniques affects the transducer failure model in a different manner, and they are considered separately in the following paragraphs.

First, consider information redundancy. Information redundancy occurs when two or more transducer channels detect the same malfunction. Information redundancy is handled directly in the portion of the READI model concerned with the effect of transducer failures on the READI decision, and no modification of the transducer failure model is required.

Next, consider transducer redundancy. Transducer redundancy occurs when two or more identical transducers are used to pick-up the same propulsion system malfunction. The modification to the failure model for doubly redundant transducers will be worked out here. The generalization of the modification to the case of higher order redundancy is straightforward. Let S and S' be two identical transducers employed for double transducer

redundancy. Let $\bar{S}$ denote the unfailed operation, S_H the very high failure, and S'_L the very low failure of transducer S. Now assuming that $P(S_H)$ and $P(S_L)$ are not zero and using

$$P(S_A \cdot S_B') = P(S_B'/S_A)\ P(S_A)$$
$$= P(S_A/S_B')\ P(S_B')$$

the probabilities, shown in table 4-4,a, are obtained. Here, for example, $P(S_B'/S_A)$ is the conditional probability of S'_B, given that S_A has occurred. It is the usual procedure in studying redundant systems to assume that the component failures occur independently, i.e., $P(S_B'/S_A) = P(S_B')$, etc. In this case, however, since the identical redundant transducers are mounted close to one another in the propulsion system, and are therefore continually exposed to the same environment, it is not possible to assume independent failures. Rather, it is only assumed that $P(S_B'/S_A) > P(S_B')$, etc. This has the effect of reducing the gain on reliability obtainable by the use of redundant transducers from that which would be obtained if it were possible to make the independence assumption. However, since the transducers are identical, and are exposed to the same environment, it may be assumed that

$$P(S_A/S_B') = P(S'_A')/S'_B)$$
$$P(S'_A') = P(S'_A).$$

It is further assumed that

$$P(S_L'/S_H) = P(S'_H'/S_L) = 0$$

That is, the probability that the two transducers fail in opposite modes is zero. Then making use of Bayes law and the fact that S, S_H, S'_L are disjoint events, the results in table 4-4,b are obtained. Inspection of this table shows that one may replace a pair of doubly redundant transducers with two equivalent simple transducers with the very high and very low failure probabilities shown in table 4-4,c. Transducer No. 1 is associated with the failure of both redundant transducers, while transducer No. 2 is associated with the failure of only one redundant transducer.

Table 4-4

Development of Doubly Redundant Sensors Representation

(a)

S \ S'	Not Failed	High Failure	Low Failure
Not Failed	$P(\bar{S}'\|\bar{S})\ P(\bar{S})$	$P(S_H'\|\bar{S})\ P(\bar{S})$	$P(S_L'\|\bar{S})\ P(\bar{S})$
High Failure	$P(S_H\|\bar{S}')\ P(\bar{S}')$	$P(S_H'\|S_H)\ P(S_H)$	$P(S_L'\|S_H)\ P(S_H)$
Low Failure	$P(S_L\|\bar{S}')\ P(\bar{S}')$	$P(S_L\|S_H')\ P(S_H')$	$P(S_L'\|S_L)\ P(S_L)$

(b)

S \ S'	Not Failed	High Failure	Low Failure
Not Failed	$P(\bar{S}'\|\bar{S})\ P(\bar{S})$	$[1-P(S_H'\|S_H)]\ P(S_H)$	$[1-P(S_L'\|S_L)]\ P(S_L)$
High Failure	$[1-P(S_H'\|S_H)]\ P(S_H)$	$P(S_H'\|S_H)\ P(S_H)$	0
Low Failure	$1-P(S_L'\|S_L)\ P(S_L)$	0	$P(S_L'\|S_L)\ P(S_L)$

(c)

<u>Transducer No. 1:</u>

$$P\ (\text{high failure}) = P(S_H'|S_H)\ P(S_H)$$

$$P\ (\text{low failure}) = P(S_L'|S_L)\ P(S_L)$$

<u>Transducer No. 2:</u>

$$P\ (\text{high failure}) = 2\ [1 - P(S_H'|S_H)]\ P(S_H)$$

$$P\ (\text{low failure}) = 2\ [1 - P(S_L'|S_L)]\ P(S_L)$$

Note: The conditioning event f^S or f^{SC} is also assumed in the above probabilities.

Finally, consider the effect of employing transducer self-check. Transducer self-check makes use of the fact that in many instances the failure of a transducer can be detected by means of its abnormal output. Transducer self-check is employed in READI as follows. When a malfunction indicator indicates the presence of a propulsion system malfunction (i.e., V = 1) this indication is not immediately gated through to the decision logic. Rather, the outputs of the transducers involved in the malfunction detector are examined by the self-check circuitry. If one or more of these transducers is found to be failed, the malfunction detectors which employ the failed transducers are permanently set to indicate "no malfunction". If no involved transducer is found to be failed, the output of the malfunction detector is gated through to the decision circuitry.

In order to account for self-check, each transducer so checked is replaced by a simple transducer with three failure modes rather than two. These failure modes are the self-check failure mode, which is taken to be the transducer failed in a manner such that this failure can be detected, the very high failure mode, and the very low failure mode. These failure modes are taken to be disjoint, and suitable probabilities, defined as above, are assigned.

The problem of determining the effect of each transducer failure mode on the decision made by READI will now be considered. This will be dependent upon the condition of the propulsion system, in addition to the particular failure mode of the particular transducer being considered. In order to determine the effect of transducer failures, a specific value is assigned to the output of each unfailed transducer in the presence of each propulsion system malfunction. These values are based on the propulsion system being treated. Thus a two-dimensional array of values of transducer outputs is obtained, one dimension of which is transducers and the other dimension of which is propulsion system malfunctions. In addition, a value of transducer output is assigned for each transducer failure mode. Now, using these two items of information (plus the definition of each malfunction detector in terms of the values of the outputs, the transducers employed, the form of each decision rule, and the priority of the decisions), the decision indicated for each propulsion system malfunction transducer failure mode pair may be obtained determinately. In carrying out this process it is assumed that, at most, one transducer is failed at any given time. This assumption will introduce only negligible errors into the final calculations, since the probability of two or more simple transducers

failing is much smaller than the probability of one simple transducer being failed. If $P(d_{k;q,p}\ m_{i;q,p}\ S_{L;q,p})$ denotes the probability of decision d_k, given that propulsion system malfunction m_i and transducer failure mode S_L have occurred in phase p of stage q, then $P(d_{k;q,p}\ m_{i;q,p}\ S_{L;q,p})$ is 1 for some single d_k and 0 for the others.

Consider now the computation of adjusted system cost. The use of READI system cost as part of the optimization criterion not only enables one to carry out realistic system trade-offs, but also tends to favor simple systems over complex systems. Thus, the term adjusted system cost is all-inclusive; that is, it includes both direct and indirect costs. The method of computing this factor is summarized in figure 4-11. The cost of the development and testing of READI by Sperry, the cost of the design and testing of the necessary vehicle modifications by the appropriate contractor, and the NASA administrative costs are estimated. These costs are then amortized over a number of vehicles to yield the development cost of READI per vehicle. This cost is taken as fixed for any READI chosen.

READI production fixed costs are taken to include the costs of the stage logic unit, displays, and decision actuators. In computing this cost the following items are considered:

- Production cost
- Test cost
- Installation cost
- Weight penalty.

Those displays and actuators present on the vehicle prior to the addition of READI are favored by assigning them a total cost of zero. The READI production fixed cost is also taken as fixed for any READI chosen.

The READI transducer cost is taken to include the cost of the transducers and their associated special signal conditioning circuits. In computing the costs of this item the above listed costs are considered for each transducer employed. Again, those transducers and signal conditioning circuits on the vehicle prior to the addition of READI are favored by assigning them a total cost of zero. Since various READI systems employ different transducers, the READI transducer cost is dependent upon the trial system under consideration. The sum of the READI fixed production costs, development costs per vehicle, and transducer costs is taken to be the adjusted system cost.

4-3. COMPUTATION OF RISK

As shown in subparagraph 4-2, A in order to be able to compute the risk at any stage mode of the mission model it is necessary to know the phase transition probabilities, $P(t_{j;\ q,p})$, for all phases in that stage and subsequent stages and in the post-boost period. These probabilities are computed as follows. The definition of conditional probability results in

$$P(t_{j;\ q,p}\ m_{i;\ q,p}\ d_{k;\ q,p}\ S_{L;\ q,p}) = P(t_{j;\ q,p}\ m_{i;\ q,p}\ d_{k;\ q,p}\ S_{L;\ q,p})$$

$$P(d_{k;\ q,p}\ m_{i;\ q,p}\ S_{L;\ q,p})\ P(m_{i;\ q,p}\ S_{L;\ q,p})$$

Where $P(A|B)$ is the conditional; probability of A given B. Now assuming that

$$P(t_{j;q,p}|m_{i;q,p}\ d_{k;q,p}\ S_{L;q,p}) = P(t_{j;q,p}|m_{i;q,p}\ d_{k;q,p})$$

and that the set of engine malfunctions, the set of transducer failure modes, and the set of decisions are, separately, sets of mutually exclusive events, results in

$$P(t_{j;q,p}) = \sum_k \sum_i \sum_L P(t_{j;q,p}|m_{i;q,p}\ d_{k;q,p})$$

$$P(d_{k;q,p}|m_{i;q,p}\ S_{L;q,p}).$$

$$P(m_{i;q,p}\ S_{L;q,p})$$

This is the basic expression for $P(t_{j;q,p})$

Now $P(t_{j;q,p}\ m_{i;q,p}\ d_{k;q,p})$ is calculated on the basis of the propulsion system and vehicle model as described in subparagraph 4-2,C, and $P(d_{k;q,p}\ m_{i;q,p} S_{L\ q,p})$ is calculated on the basis of the READI model as described in subparagraph 4-2 D. The probability $P(m_{i;q,p}\ S_{L;q,p})$ is computed from the propulsion system and READI models as follows. It is first noted that engine malfunctions and transducer failure modes fall into two distinct categories: those which are associated with a single engine in the cluster, and those which are associated with the portions of the propulsion system and READI common to all engines in the cluster. Making use of the definitions shown in table 4-5 and assuming that:

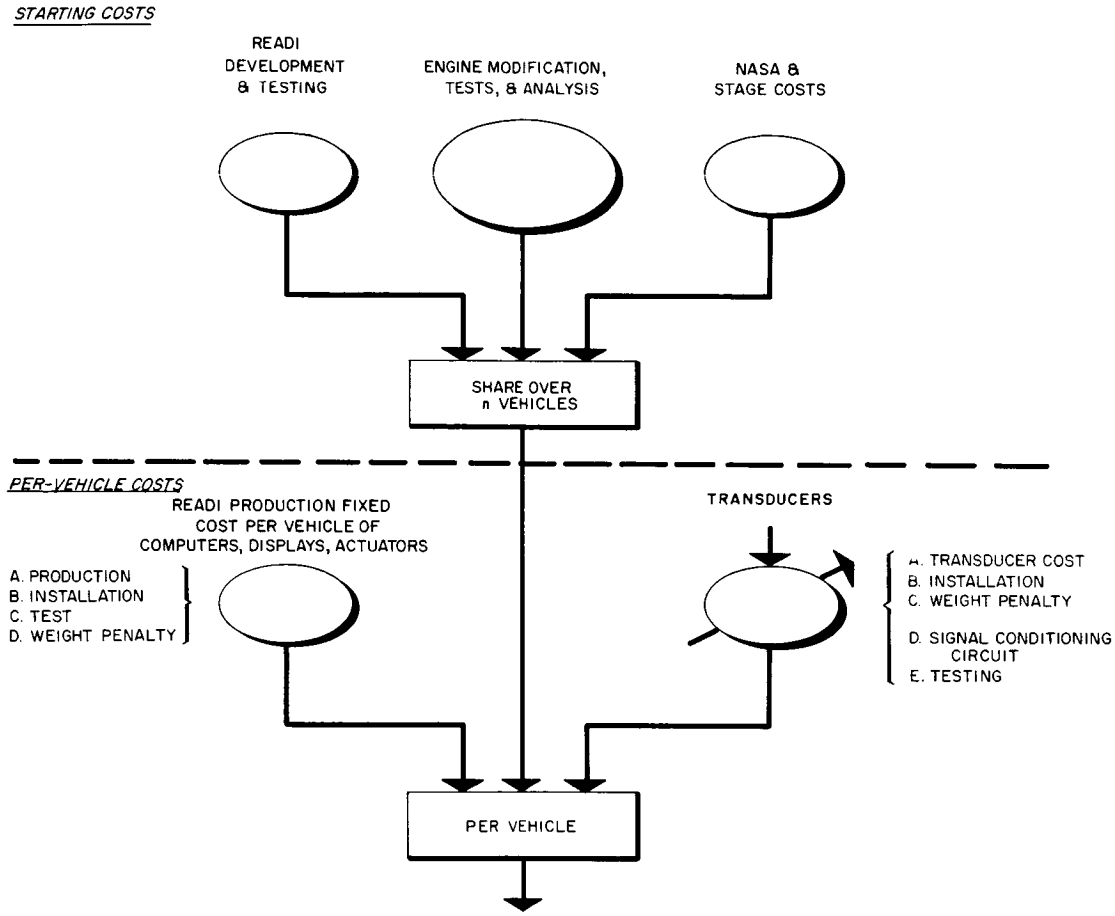


FIGURE 4-11
COST MODEL

- Engine malfunctions occur independently from engine to engine, but on a mutually exclusive basis within the engine
- Transducer failures occur independently from transducer package to transducer package, but on a mutually exclusive basis within the transducer package. (A transducer package is the set of transducers associated with a single engine or the stage common part of the propulsion system).
- The probability of failure of more than one engine is negligible for the purpose of risk computation
- The probability of failure of more than one transducer package is negligible
- The failure of an engine and of a transducer package not attached to that engine is an event of negligible probability.

the results shown in table 4-6 are obtained. In table 4-6 all transducers are taken to be simple transducers and redundant transducers are replaced by their simple transducer equivalents. Further, malfunctions are taken to be defined on the level of propulsion system malfunctions discussed in subparagraph 4-2, B.

Thus $P(t_{j;q,p})$ may be computed. From these computations follow the stage transition probabilities as described on subparagraph 4-2, A.

Table 4-5
Definition of Terms
$P(m_{i;q,p}\ S_{L;q,p})$

Term	Definition
$P^E_{q,p}$	The probability that a single engine operates successfully (i.e. without malfunction) during phase p of stage q.
$PEC_{q,p}$	The probability that the stage common propulsion systems components operate successfully during phase p of stage q.
$PS_{q,p}$	The probability that a single engine transducer package operates successfully during phase p of stage q.
$PSC_{q,p}$	The probability that the stage common READI components operate successfully during phase p of stage q.

Table 4-5 (Cont.)

Definition of Terms

$P(m_{i;q,p}\ S_{L;q,p})$

Term	Definition
f^E	The event of an engine failure.
f^{EC}	The event of a stage common propulsion system component failure.
f^S	The event of a single engine transducer package failure.
f^{SC}	The event of a stage common READI component failure.
n_q	The number of engines in stage q.

Table 4-6

Probability of Propulsion System Malfunction and System Failure Events

$P(m_{i;q,p}\ S_{L;q,p})$

Transducer Failure (L)	Engine Malfunction (i)	$P(m_{i;q,p}\ S_{l;q,p})$
No failure	No malfunction	$\left[(P^E{}_{q,p})^{n_q}\ P^{EC}{}_{q,p}\right] \cdot \left[(P^S{}_{q,p})^{n_q}\ P^{SC}{}_{q,p}\right]$
No failure	Single engine	$\left[(P^S{}_{q,p})^{n_q}\ P^{SC}{}_{q,p}\right] \cdot \left[P(m_i \mid f^E)\ n_q\ (1-P^E{}_{q,p})(P^E{}_{q,p})^{n_q-1}\right]$
No failure	Stage common	$\left[(P^S{}_{q,p})^{n_q}\ P^{SC}{}_{q,p}\right] \cdot \left[P(m_i \mid f^{EC})\ (1-P^{EC}{}_{q,p})\right]$
Engine transducer package	No malfunction	$\left[(P^E{}_{q,p})^{n_q}\ P^{EC}{}_{q,p}\right] \cdot \left[P(S_L \mid f^S)\ n_q\ (1-P^S{}_{q,p})(P^S{}_{q,p})^{n_q-1}\right]$
Stage common transducer package	No malfunction	$\left[(P^E{}_{q,p})^{n_q}\ P^{EC}{}_{q,p}\right] \cdot \left[P(S_L \mid f^{SC})\ (1-P^{SC}{}_{q,p})\right]$
Engine transducer package	Single engine	$\left[P(m_i \mid f^E)\ n_q\ (1-P^E{}_{q,p})(P^E{}_{q,p})^{n_q-1}\right] \cdot \left[P(S_L \mid f^S)(1-P^S{}_{q,p})\right]$

Table 4-6 (Cont.)

Probability of Propulsion System Malfunction and System Failure Events

Transducer Failure (L)	Engine Malfunction (i)	$P(m_{i;q,p}\ S_{L;q,p})$
Stage common transducer package	Stage common	$\left[P(m_i \mid f^{EC})\ (1-P^{EC}_{q,p})\right] \cdot \left[P(S_L \mid f^{SC})\ (1-P^{SC}_{q,p})\right]$

In order to go further, it is simpler to now specify a particular stage within the mission model for further study. In line with Phase I work, the second stage is chosen. In this case the risks at the stage final condition nodes were computed assuming an ideal READI on the third stage. An ideal READI is a READI which monitors all propulsion system malfunctions and always makes the best decision when a malfunction occurs.

$$R(0,1) = P(t'_{o,2})\ R(0,2) + P(t'_{1,2})\ R(1,2) + P(t'_{2,2})\ R(2,2) + P(t'_{3,2})\ R(3,2) + P(t'_{4,2})\ R(4,2)$$

$$R(1.1) = P(t'_{o,2})\ R(1,2) + P(t'_{1,2})\ R(2,2) + \left[P(t'_{2,2}) + P(t'_{3,2})\right]\ R(3,2) + P(t'_{4,2})\ R(4,2)$$

and

$$R(2,1) = P(t'_{o,2})\ R(2,2) + \left[P(t'_{1,2}) + P(t'_{2,2}) + P(t'_{3,2})\right] R(3,2) + P(t'_{4,2})\ R(4,2).$$

Then the total mission risk is given by

$$R = P(t'_{o,1})\ R(0,1) + P(t'_{1,1})\ R(1,1) + P(t'_{2,1})\ R(2,1) + k$$

where k is the risk due to possible abort or explosion in the first stage.

The above expression for R may be simplified if the engine/vehicle/READI combination is reliable. First of all, it is possible to neglect the last three terms on the right-hand side of the expression for R, so that

$$R \doteq P(t'_{o,1})\, R(0,1)$$

$$\doteq P(t'_{o,1}) \left[\sum_{j=o}^{4} P(t'_{j,2})\, R(j,2) \right]$$

Second, for j greater than zero, one may assume

$$P(t'_{j,2}) \doteq \sum_{P=1}^{P_2} P(t_{j;q,p}).$$

Also, it may be assumed that

$$\prod_{P=1}^{P_2} P(t_{o;2,p}) = 1$$

and

$$P(t'_{o,1}) = 1$$

so that

$$R \doteq R(0,2) + \sum_{P=1}^{P_2} \sum_{j=1}^{4} P(t_{j;2,p})\, R(j,2).$$

It should be emphasized that the above expression for risk holds only if the assumption of a reliable system holds, including vehicle, engines, and READI. Otherwise, a more complicated expression for risk must be used.

Now replacing $P(t_{j;2,p})$ in the above expression one has

$$R \doteq R(0,2) + \sum_{P=1}^{P_2} \sum_{j=1}^{4} \sum_{k} \sum_{i} \sum_{L} \Big[P(t_{j;2,p} | m_{1;2,p}\, d_{k;2,p})$$

$$P(d_k\, m_{i;2,p} | S_{L;2,p})\, P(m_{i;2,p}\, S_{L;2,p}) \cdot R(j,2) \Big]$$

One may define a loss attached to decision k, malfunction i, engine phase p, stage 2, as

$$L(d_k\, m_{i,j,p,2}) = \sum_{j=1}^{4} P(t_{j;2,p} | m_{i;2,p}\, d_{k;2,p})\, R(j,2).$$

Then

$$R \doteq R(0,2) + \sum_p \sum_k \sum_i \sum_L \Big[P(d_k | m_{i;2,p}\ S_{L;2,p})\ P(S_{L;2,p}\ m_{i;2,p}) \cdot L(d_k, m_{i;p,2}) \Big]$$

This is the final form of the total risk equation with a real READI system in the second stage.

For the purpose of using the evaluation procedure as a design aid, it is desirable to partition the total risk, R, into several meaningful components. To this end the risk components defined in table 4-7 are introduced. The ideal READI risk is the risk obtainable with a READI which monitors all propulsion system malfunctions and indicates the optimum decision if a malfunction occurs. The not monitored risk increment is the increase in risk due to the fact that not all propulsion system malfunctions are monitored. The discrimination risk increment is the increase in risk due to the fact that READI cannot separate all malfunctions. The false alarm risk increment is the increase in risk due to false alarms caused by transducer failures. The missed and wrong alarm risk increments are similarly defined. The sum of the ideal READI risk and the risk increments is the total risk, R, as obtained above.

4-4. DIGITAL COMPUTER COMPUTATION OF RISK

The theoretical basis of the computation of the total risk and risk components for any given READI system, vehicle, and mission complex are presented in paragraphs 4-2 and 4-3. Brief examination of this material shows that the actual numerical computations involved in calculating the risk in a single case are quite extensive. Experience has shown that for the large examples considered in this report roughly one man-month of computation is required for each READI system considered. Since the detailed evaluation of risk is required for a number of READI systems during the system synthesis, several digital computer programs have been prepared to carry out the more time-consuming portions of the computation. This section describes briefly these computer programs. Detailed information concerning the computer programs is contained in Appendix A.

Table 4-7

Definition of Risk Components

Malfunction Component	Definition
Ideal READI Risk	$R(0,2) + \sum_{P} \sum_{i=0} P(m_{i;2,p})\ L(d'_{k_{1;2,p}}\ m_{i;2,p})$
Not Monitored Risk Increment	$\sum_{P} \sum_{L=0} (1-I_{i;2,p})\ P(m_{i;2,p}) \left[L(d_{k_{i;2,p}}\ m_{i;2,p}) - L(d'_{k_{i;2,p}}\ m_{i;2,p})\right]$
Discrimination Risk Increment	$\sum_{P} \sum_{L=0} I_{i;2,p}\ P(m_{i;2,p}) \left[L(d_{k_{i;2,p}}\ m_{i;2,p}) - L(d'_{k_{i;2,p}}\ m_{i;2,p})\right]$
False Alarm Risk Increment	$\sum_{P} \sum_{k=1} \sum_{L=0} P(d_{k;2,p} \mid m_{o;2,p}\ S_{h;2,p})\ P(m_{o;2,p}\ S_{L;2,p}) \left[L(d_{k;2,p}\ m_{o;2,p}) - L(d_{o;2,p}\ m_{o;2,p})\right]$
Missed Alarm Risk Increment	$\sum_{P} \sum_{i=1} \sum_{L=0} P(d_{o;2,p} \mid m_{i;2,p}\ S_{L;2,p})\ P(m_{i;2,p}\ S_{L;2,p}) \left[L(d_{o;2,p}\ m_{i;2,p}) - L(d_{k_{i;2,p}}\ m_{i;2,p})\right]$
Wrong Alarm Risk Increment	$\sum_{P} \sum_{k=1} \sum_{L=0} P(d_{k;2,p} \mid m_{i;2,p}\ S_{L;2,p})\ P(m_{i;2,p}\ S_{L;2,p}) \left[L(d_{k;2,p}\ m_{i;2,p}) - L(d_{k_{i;2,p}}\ m_{i;2,p})\right]$

Notation:

$d_{k_{i;q,p}}$ - the optimum decision for $m_{i;q,p}$

$d_{k_{i;q,p}}$ - the programmed decision for $m_{i;q,p}$

$$I_{i;q,p} = \begin{cases} 1 \text{ if } d_{k_{i;p,q}} = d_o \\ 0 \text{ if } d_{k_{i;q,p}} = d_o \end{cases}$$

d_o - no action m_o - no malfunction

A general flow diagram of the risk computation is shown in figure 4-12. There are three main groups of inputs: the READI system information, the propulsion system information, and the mission information. The contents of each of the input groups is detailed in figure 4-12. In order to compute risk it is first necessary to obtain for each combination of transducer failure mode, propulsion system malfunction, and READI decision, the particular probability:

- $P(d_{k;q,p} | m_{i;q,p} S_{L;q,p})$
- $L(d_k m_{i;q,p})$
- $P(m_{i;q,p} S_{L;q,p})$

After this has been accomplished it is necessary to perform the summations indicated in paragraph 4-3 to obtain the total risk and the risk components.

Two separate programs have been written to carry out the above steps. These are

- READI failure enumeration routine
- Risk computation routine.

Each of these programs is summarized in the following paragraphs.

Consider first the computation of $P(d_{k;q,p} | m_{i;q,p} S_{L;q,p})$. As pointed out in subparagraph 4-2,D for any fixed $(m_{i;q,p} S_{L;q,p})$, this probability is for one and only one $d_{k;q,p}$ and 0 for all other decisions. Thus a list containing the value of k for which the probability is 1 contains all the necessary information concerning $P(d_k | m_i S_L)$. Such a list is quite long; however, such a list containing entries for those $(m_{i;q,p} S_{L;q,p})$ for which the associated $d_{k;q,p}$ is other than the programmed decision for $m_{i;q,p}$, combined with a list of programmed decisions for each $m_{i;q,p}$, is of reasonable length and contains the required information. The READI failure enumeration routine generates these two lists for each phase of the stage under consideration on the basis of the following input information:

- Definition of READI system decision rules in terms of the Boolian outputs of the malfunction detectors
- Definition of Boolian 1 for each malfunction detector in terms of the outputs of the transducers employed
- The normal value of the output of each transducer in the presence of each propulsion system malfunction including no malfunction
- The output of each transducer in each failure mode
- The programmed decision for each malfunction.

Each of the above items is required for each phase of the stage under consideration.

Consider next the computation of the total risk and the risk components. These computations are carried out in the risk computation routine. This routine takes the propulsion system malfunction probabilities and the READI system malfunction probabilities and computes each $P(m_{i;p,q}S_{L;p,q})$. Then using the $P(t_{j;q,p}\ m_{i;q,p}d_{k;q,p})$ from the transition probability routine, the probability of explosion for each $(m_{i;q,p}d_{k;q,p})$, and the risks at each stage final conditions mode, the required $L(m_i d_{k;p,q})$ is computed. Finally, using these two items plus the lists generated by the READI failure enumeration routine, the total risks and risk components are computed.

4-5. SYSTEM SYNTHESIS PROCEDURE

A. INTRODUCTION

The purpose of the READI system synthesis procedure is to identify the combination of READI transducers and associated signal processing, in the set of all possible combinations of READI transducers, that can be employed on the vehicle under consideration and yields the optimum system. The number of such combinations is finite, and there exists a well-defined evaluation procedure. Thus it is possible, in theory at least, to proceed as follows. Taking as the input a catalog of all the malfunction detectors (in terms of the transducers employed), the propulsion system malfunctions detected by each malfunction detector, and the loss data for each malfunction decision pair synthesize a READI system corresponding to each combination of

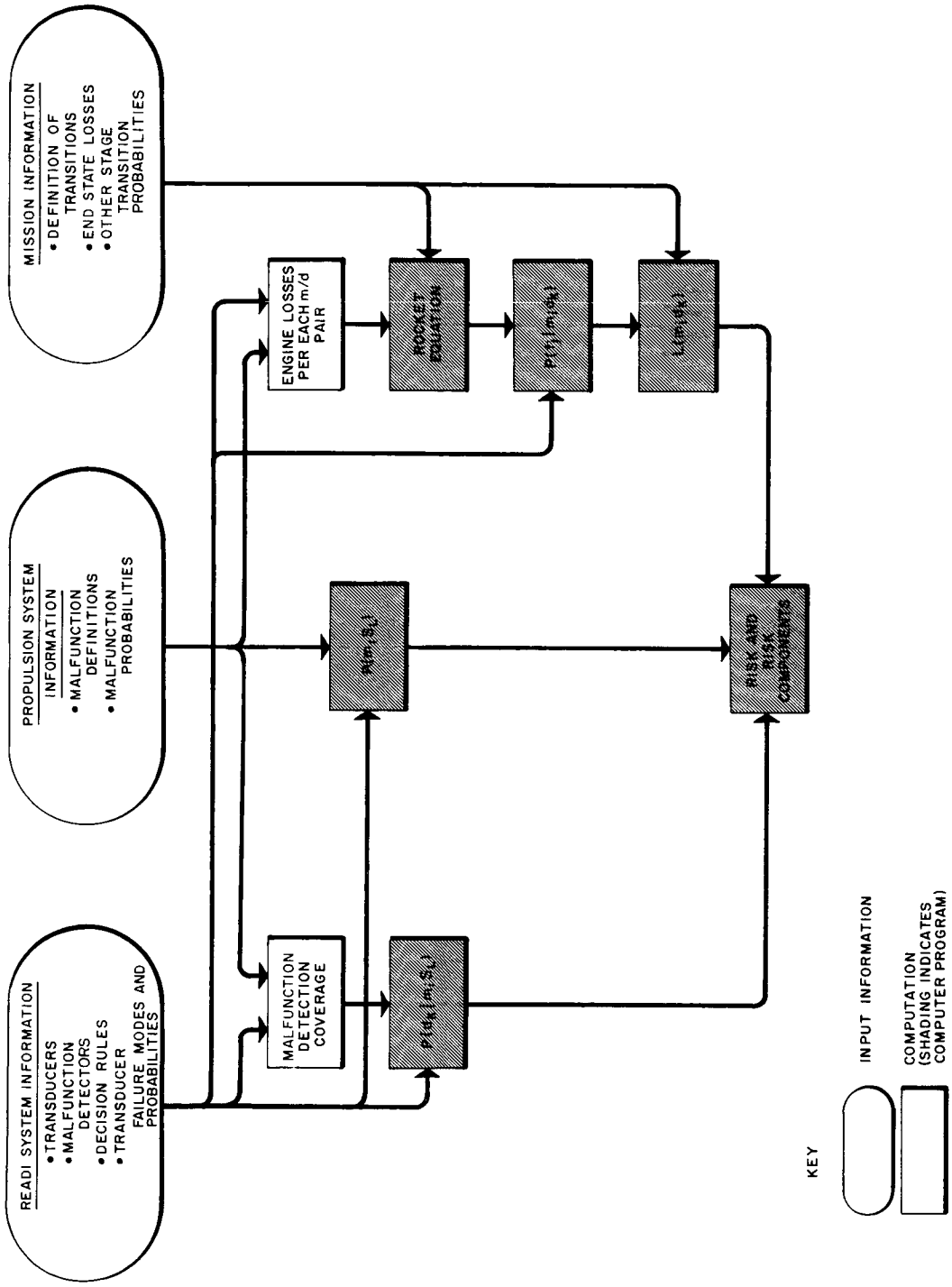


FIGURE 4-12
GENERAL FLOW CHART-RISK COMPUTATION

transducers. Then, using the evaluation procedure, evaluate each such system. However, as indicated in paragraph 3-2, the number of possible combinations of READI transducers is equal to 2^n, where n is the number of such transducers. Thus the number of systems to be evaluated grows exponentially with the number of READI transducers available. In any synthesis problem for a real vehicle-mission complex this exponential growth results in a very large number of systems to be evaluated.

The basic ideas of the synthesis procedure developed are illustrated in figure 4-13. As may be seen, the procedure is a two-step process. The basic purpose of the first part is to reduce the number of combinations of transducers which must be examined by performing a detailed evaluation of the corresponding systems. Briefly, this is accomplished as follows. Each of the available transducers is examined in turn. First it is decided if sufficient reason exists to include it in the optimum system, and if this is the case, it is placed in the set of included transducers and deleted from the transducer list. Sufficient reason to include the transducer in the optimum system means that the transducer satisfies a condition which implies that the transducer is in the optimum system. It is important to note that the condition is not necessarily satisfied by all the transducers in the optimum systems, i.e., it is not a necessary condition. If there is not sufficient reason to include the transducer in the optimum system, then it is examined to see if there is sufficient reason to exclude it from the optimum system. If this is the case it is placed in the excluded transducer set and deleted from the transducer list. Again, the exclude condition is not a necessary condition. Thus it is possible that some transducers will not be placed in either the included transducer set or the excluded transducer set. Such transducers are placed in the undetermined transducer set. This process is continued until testing of transducers is no longer fruitful. Thus it may be seen that the heart of the first part of the synthesis procedure is the criteria used for placing the transducers in the included transducer set and the excluded transducer set. The construction of these criteria, which are recursive in nature, is the major topic of subparagraphs 4-5, B, C and D.

However, before proceeding to lay the necessary preliminary groundwork for the criteria, consider the second part of the synthesis scheme. This part is initiated after the application of the first part no longer places any transducers in the included or excluded transducer sets. It

is the purpose of the second part of the synthesis procedure to select the optimum system from the remaining possible systems using the detailed evaluation scheme. At this point all the transducers in the catalog are in one and only one of three sets. Those in the excluded transducer set are not considered any further. Those transducers in the included transducer set are definitely in the optimum system, and any system considered in the second part must contain all of these transducers. The transducers in the undetermined transducer set, however,may or may not be in the optimum system. Thus the systems corresponding to each combination of transducers containing all the transducer in the included set plus none, some, or all of the transducers in the undetermined set are evaluated and the optimum system is selected.

B. PRELIMINARY DEVELOPMENT

Before proceeding to develop the include and exclude criteria, it is first necessary to state certain assumptions and definitions and to discuss certain preliminary results.

In addition to the assumptions made in paragraph 4-3 for the purpose of system evaluation, it is also assumed that the effect of READI transducer unreliability is negligible for the purposes of the first part of the synthesis scheme. There is little danger in this assumption since transducer unreliability is considered in the second step of the scheme. Thus any particular transducer unreliability problem will be detected during the second part and mitigated by the application of the appropriate redundancy technique.

The first part of the synthesis procedure will be discussed as if a single phase only was being treated and the stage and phase subscripts and summations employed in paragraph 4-3 will be dropped. However, the synthesis of the procedure may be applied to the design of READI systems for an entire stage by merely renumbering the malfunctions in each phase so as to form a single sequence of malfunction numbers and proceeding in the manner described below as if a single phase were being treated.

The value of READI lies in its ability to reduce mission risk. Thus, the system value of a READI system, S, which is denoted by SV(S), will be introduced:

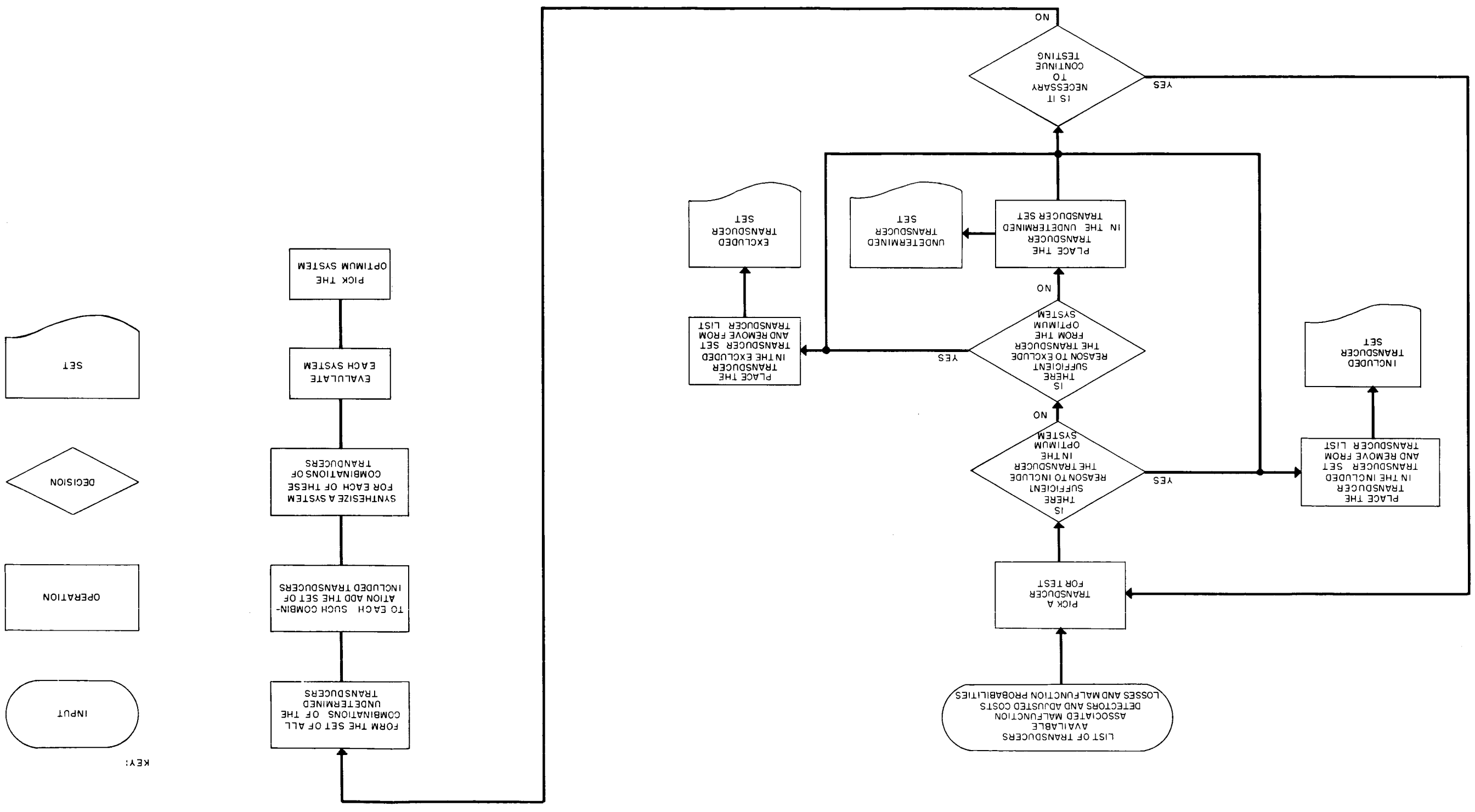


FIGURE 4-13
SIMPLIFIED FLOW
DIAGRAM, SYSTEM SYNTHESIS PROCEDURE

$$SV(S) = \text{Risk (No READI)} - \text{Risk (S)}$$

Now denoting the decision programmed for propulsion system malfunction m_i by d_{k_i} (making use of the expression obtained for risk in paragraph 4-3), and remembering that transducer unreliability is being neglected, one obtains for the system value

$$SV(S) = \sum_{i=1} P(m_i)\left[L(d_o, m_i) - L(d_{k_i}, m_i)\right]$$

where $P(m_i)$ is the probability of propulsion system malfunction m_i. It will be remembered that this is the factor introduced in the second example of paragraph 3-1.

We now denote the set of propulsion system malfunctions by $\mathfrak{m}$ and introduce the idea of a partition of the set $\mathfrak{m}$. A partition of $\mathfrak{m}$ is a class of subsets of $\mathfrak{m}$, say $\{\mathfrak{m}'_1, \mathfrak{m}'_2, \ldots, \mathfrak{m}'_n\}$, such that the logical union of the sets $\{\mathfrak{m}'_1, \ldots, \mathfrak{m}'_n$ is $\mathfrak{m}$ and no two sets contain a common malfunction. That is, in set notation,

$$\bigcup_{i=1}^{n} \mathfrak{m}'_i = \mathfrak{m}$$

$$\mathfrak{m}_i \cap \mathfrak{m}'_j = \phi \text{ for } i \neq j$$

It may be seen that, in general, there is more than one partition of $\mathfrak{m}$. To each possible combination of READI transducers there corresponds a particular partition of the set $\mathfrak{m}$. The construction of this partition is such that each subset contains a single set of inseparable malfunctions, where the set of malfunctions which are not monitored, i.e., are inseparable from no propulsion system malfunction, is considered to be an inseparable set of malfunctions containing m_o. The inseparable set of malfunctions detected by malfunction detectors V1, V2 ..., and Vn only is denoted by $\mathfrak{m}'_{V1, \ldots, Vn}$, and the set inseparable from no malfunction is denoted by $\mathfrak{m}'_o$. The construction of this partition is most easily accomplished on the basis of the Venn diagram representation of the malfunction detectors arising from the set of transducers under consideration.

Consider again the second example of paragraph 3-1, the Venn diagram of which is shown in figure 3-3. Suppose that only V2 is being employed. Then the partition of $\mathfrak{m}$ corresponding to this system is

$$\mathfrak{m}'_{V2} = \{m_2, m_3\}$$

and

$$\mathfrak{m}'_o = \{m_o, m_1\}$$

In contrast to this partition, consider the partition corresponding to the system employing V1, V2, and V3. This partition is

$$\mathfrak{m}_{V1,\ V3} = \{m_1\}$$

$$\mathfrak{m}_{V1,\ V2} = \{m_3\}$$

$$\mathfrak{m}_{V1,\ V2,\ V3} = \{m_2\}$$

$$\mathfrak{m}_o = \{m_o\}$$

Finally, the partition corresponding to no READI is

$$\mathfrak{m}'_o = \mathfrak{m} = \{m_o, m_1, m_2, m_3\}$$

In general, the first equality of the above holds.

As pointed out in paragraph 3-1, only one decision, including the no action decision, may be programmed for all the malfunctions in a set of inseparable malfunctions. Further, for the malfunctions contained in $\mathfrak{m}_o$, the programmed decision must be no action since the probability of $\mathfrak{m}_o$ is far greater than the probability of all the other malfunctions, i.e., since the propulsion system is quite reliable. The decision programmed for the set of inseparable malfunctions $\mathfrak{m}'_{V1,\ldots,}\mathfrak{m}_{Vn}$ is denoted by $d_{k_{m'V1,\ \ldots,Vn}}$.

Now a method for choosing $d_{k_{m'V1,\ldots,\ Vn}}$ for any $\mathfrak{m}'_{V1,\ldots Vn}$ must be found. To do this first note that out of all the possible ways of assigning these decision rules those rules which result in the maximum system value will also result in minimum risk. It is assumed that there is no difference in cost between any of the ways of assigning the decision rules once the set of available decision rules has been specified. Thus, the assignment of decision rules should be such that the system value is a maximum. Now letting $\mathfrak{m}'$ be the class of sets of inseparable malfunctions and making use of the fact that this class is a partition of $\mathfrak{m}$, the set of malfunctions, results in

$$SV(S) = \sum_{\mathfrak{m}'_{V1,\cdots,Vn} \in \{\mathfrak{m}'-\mathfrak{m}_o\}} \left[\sum_{\mathfrak{m}_i \in \mathfrak{m}_{V1,\cdots,Vn}} \left[L(d_o\ m_i) - L\left(d_{k_{m'_{V1,\cdots Vn}}}\ m_i\right) \right] P(m_i) \right]$$

Thus SV(S) will be a maximum if each of the inner sums is a maximum. Therefore, $d_{k\ 'V1,\cdots,\ V2}$ should be chosen from the set of available decisions so that

$$\sum_{\mathfrak{m}_i\ \mathfrak{m}_{V1,\cdots,Vn}} \left[L(d_o\ m_i) - L\left(d_{k_{m'_{V1,\cdots,Vn}}}\ m_i\right) \right] P(m_i)$$

is rendered a maximum. From this point on it will be assumed that the decision for each inseparable set of malfunctions is assigned in this manner, and system values of the corresponding system will be denoted by max S'V(-).

It is now possible to understand a basic result upon which much of the synthesis scheme is based. Consider two systems, S_o and S_1. Let S_o employ malfunction detectors V1, ..., Vn and S_1 employ the same set of malfunction detectors V1, ..., Vn plus one more malfunction detector Vn + 1. Then

$$\max SV(S_1) \geq \max SV(S_o)$$

This is most easily seen by considering again the various functions of a malfunction detector. As stated in paragraph 3-1 these are:

- o Separation of propulsion system malfunctions from no malfunction
- o Separation of propulsion system malfunctions one from another
- o Information redundancy to mitigate the effects of READI transducer failures.

Since transducer unreliability is not considered in this part of the synthesis procedure, function (C) is of no interest at present. Therefore, any malfunction detector, and thus Vn + 1, can perform any one of four possible functions when added to a nonempty set of malfunctions. These sets are

i. Function (a) only
ii. Function (b) only
iii. Functions (a) and (b)
iv. No additional function.

Each of these functions is illustrated for Vn + 1 in figure 4-14. Using this figure, the effect by adding Vn + 1 to V1 and V2 may be investigated. In (i) the programmed decision for malfunction one may be different from no action. If the preferred decision for malfunction one is no action, then $SV(S_1) = SV(S_o)$ if not, then $SV(S_1) > SV(S_o)$. In (ii) the decisions for malfunctions two and four may differ. If malfunctions two and four have the same preferred decision then $SV(S_1) = SV(S_o)$ if not, then $SV(S_1) > SV(S_o)$. In (iii) the decision for malfunction one may be different from no action and the decisions for malfunctions two and four may differ. If the preferred decision for malfunction one is no action, and if the preferred decision for malfunction two is the same as for malfunction four, then $SV(S_1) = SV(S_o)$. If either one or both of these conditions on the preferred decision is not the case, then $SV(S_1) > SV(S_o)$. In (iv), since there are no possible changes in the decisions, $SV(S_1) = SV(S_o)$. Thus it is seen that in each case $SV(S_1) \geq SV(S_o)$. The above procedure may be extended to the general case.

Consider further case (iii) of figure 4-14. Suppose for the moment that the preferred decision for malfunction one is other than no action and that the preferred decision for malfunction two differs from that for malfunction one. Then the terms in $SV(S_1)$ due to these malfunctions are greater than the corresponding terms in $SV(S_o)$. However, the term in $SV(S_1)$ due to malfunction three is the same as the corresponding term in $SV(S_o)$. Thus, in this case, only those terms in the $SV(S_1)$ due to malfunctions contained in partition sets changed by the addition of Vn + 1 are different from the corresponding terms in $SV(S_o)$. A similar result may be obtained for the other cases shown in figure 4-14. Indeed, this result may also be extended to the general case, except that the terms need not necessarily differ since the preferred decisions for the newly separated malfunction need not necessarily differ.

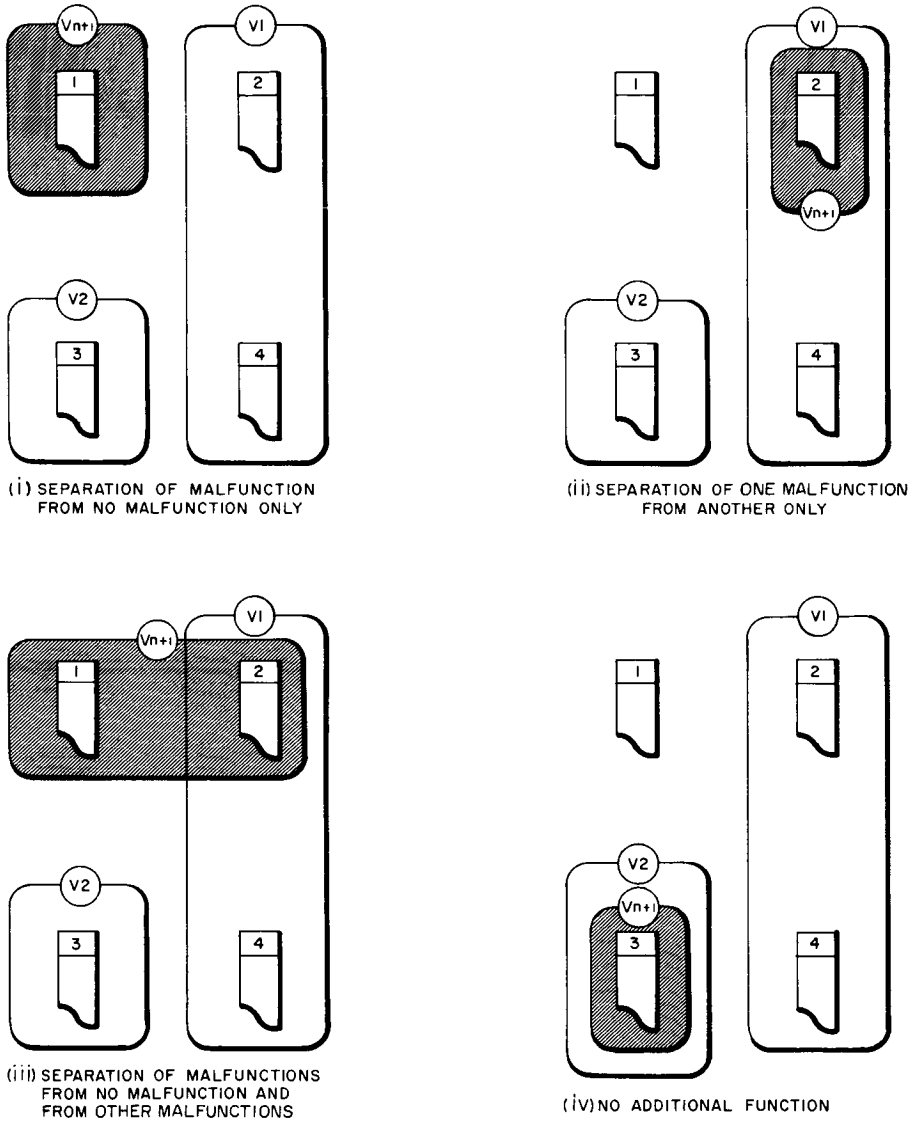


FIGURE 4-14
POSSIBLE EFFECTS OF ADDING Vn + 1 TO V1 + V2

C. DEVELOPMENT OF THE INITIAL INCLUDE AND EXCLUDE CRITERIA

It is now possible to obtain criteria for the inclusion and exclusion of transducers. These criteria are used in the initial step of system optimization to test transducers (and associated processing) for transfer to the "included set" or the "excluded set" of transducers. These criteria are easily generalized for use in the iterative scheme depicted in figure 4-13. This generalization is discussed in subparagraph 4-6,D.

It is first necessary to introduce some additional notations. A set of transducers is denoted by $\{T\}$. In particular, $\{T\}_u$ is used to denote the set of all available transducers, and $\{T\}_o$ is used to denote the set of transducers employed by the optimum system. In general, $\mathfrak{m}$ shall be used to denote a set of propulsion system malfunctions. In particular, $\mathfrak{m}_u$ is used to denote the set of all propulsion system malfunctions. Also, the system value of a READI system, S, over a set of malfunctions $\mathfrak{m}_o$, $SV_{\mathfrak{m}_o}(S)$ is defined to be

$$SV_{\mathfrak{m}_o}(S) = \sum_{m_i \; \mathfrak{m}_o} P(m_i) \quad L(d_o, m_i) - L(d_{k_i}, m_i)$$

where the summation notation means that the sum extends over only those m_i terms contained in the set of malfunctions $\mathfrak{m}_o$. Thus, for example the system value employed in subparagraph 4-5,B is $SV_{\mathfrak{m}_u}(S')$. The term $S_{\{T\}}$ denotes the system employing all of the malfunction detectors which use only the transducers contained in the set of transducers $\{T\}$ and where the decisions are assigned such that $SV_{\mathfrak{m}_u} S_{\{T\}} = \text{maximum } SV_{\mathfrak{m}_u} S_{\{T\}}$. Finally, the adjusted cost of transducer T is denoted by C(T)

It is now possible to state and discuss the include criterion.

> If there exists at least one set of malfunctions, $\mathfrak{m}_o$ contained in or equal to $\mathfrak{m}_u$, such that
> $\max SV_{\mathfrak{m}_o}(S_7) - \max SV_{\mathfrak{m}_o}(S_{\{\{T\}_u - T\}}) \geq C(T)$, <
>
> where $\{\{T\}_u - T\}$ is the set of all possible transducers less T, then T is in the optimum system.

To see why this is the case it is assumed that T is not in $\{T\}_o$ and a contradiction is obtained. The fact that T is assumed not to be in the optimum system is obtained from the definition of the optimum system, and from the definition of $SV_{\mathfrak{m}_u}(S)$, one obtains, after a little manipulation, that

$$\max SV_{\mathfrak{m}_u}(S_{\{T\}_o} + T) - \max SV_{\mathfrak{m}_u}(S_{\{T\}_o}) < C(T)$$

That is, if the transducer T is not in the optimum system, the gain in system value realized by employing the set of transducer $\{T\}_o + T$, rather than just $\{T\}_o$, is less than the cost of T. Now employing the definition of $SV_{\mathfrak{m}_u}(S)$ and $SV_{\mathfrak{m}_u}(S)$, and noting that the set of malfunctions $\{\mathfrak{m}_u - \mathfrak{m}_o\}$ plus the set of malfunctions $\mathfrak{m}_o$ is $\mathfrak{m}_u$, the sum on the left-hand side of the above inequality may be broken up as system sums of system values over $\mathfrak{m}_o$ and $\mathfrak{m}_u - \mathfrak{m}_o$ and may be written as

$$\left[\max SV_{\mathfrak{m}_o}(S_{\{T\}_o} + T) - \max SV_{\mathfrak{m}_o}(S_{\{T\}_o})\right] +$$

$$\left[\max SV_{\mathfrak{m}_u - \mathfrak{m}_o}(S_{\{T\}_o} + T) - \max SV_{\mathfrak{m}_u - \mathfrak{m}_o}(S_{\{T\}_o})\right] < C(T)$$

It is now possible to employ the result concerning the addition of malfunction detectors obtained in subparagraph 4-5,B. Since T is not contained in $\{T\}_o$, and since there is at least one malfunction detector associated with T this results in

$$\max SV_{\mathfrak{m}_u - \mathfrak{m}_o}(S_{\{T\}_o} + T) - \max SV_{\mathfrak{m}_u - \mathfrak{m}_o}(S_{\{T\}_o}) \geq 0$$

Further,

$$\max SV_{\mathfrak{m}_o}(S_{\{T\}_o} + T) \geq \max (S_{\{T\}_o})$$

and

$$\max SV_{\mathfrak{m}_o}(S_{\{\{T\}_u - T\}}) \geq \max SV_{\mathfrak{m}_o}(S_{\{T\}_o})$$

Thus,

$$\max SV_{\mathfrak{m}_o}(S_T) - \max SV_{\mathfrak{m}_o}(S_{\{\{T\}_u - T\}}) < C(T)$$

and the contradiction has been obtained.

Finally it is noted that the inequality obtained is most powerful if $\mathfrak{m}_o$ is such that

$$\max SV_{\mathfrak{m}_u - \mathfrak{m}_o}(S_{\{T\}_o + T}) - \max SV_{\mathfrak{m}_u - \mathfrak{m}_i}(S_{\{T\}_o}) = 0$$

If this is the case, then $\mathfrak{m}_o$ is just the set of malfunctions contained in the partitions changed by the addition of the malfunction detectors associated with transducer T. But it was shown in subparagraph 4-2,B that the only terms which change the system value are due to the malfunctions in $\mathfrak{m} - \mathfrak{m}_o$ also. Thus, if there is some set of malfunctions, m, for which the inequality of the include criterion is satisfied, it will also be satisfied for $\mathfrak{m}_o$ chosen on the basis of the partitions which change due to the additional T. Therefore, $\mathfrak{m}_o$ can be chosen in the include criterion on this basis so that the most powerful inequality is obtained.

The exclude criterion will now be considered.

> If for every possible combination of transducers, {T}, drawn from the set of all possible transducers less T, one has
> $\max SV_{\mathfrak{m}_u}(S_{\{\{T\}_1 + T\}}) - \max SV_{\mathfrak{m}_u}(S_{\{T\}_1}) < C(T)$
> then T is not in the optimum system.

That is, if the difference between the system value for every possible system employing T and the corresponding system not employing T is less than the cost of T, then T will not be in the optimum system. Unfortunately, it does not appear possible to obtain a specific set of transducers, {T} , to use in this test. Thus this test is more difficult to apply than the include criteria. This disadvantage may be omitigated somewhat by a slight modification of the iterative procedure, which will now be considered.

D. ITERATION PROCEDURE

The iteration procedure is described in subparagraph 4-5,A and is shown schematically in figure 4-13. The include and exclude criteria developed in subparagraph 4-5,C do not take advantage of the fact that at any step in the iterative procedure, beyond the testing of the first transducer for the first time, there may be transducers in the included and excluded transducer sets. By taking advantage of this information, the include and exclude criteria may be made more powerful as the iteration process proceeds.

Consider first the include criterion. Let $\{T\}_E$ be the set of excluded transducers. Then the transducers in $\{T\}_E$ will not be used in any reasonable system and one may replace the set $\{\{T\}_u - T\}$ by the set $\{\{T\}_u - \{T\}_E - T\}$ and the include criterion inequality becomes

$$\max SV_{\mathfrak{m}_o}(S_T) - \max SV_{\mathfrak{m}_o}(S\{\{T\}_u - \{T\}_E - T\}) \geq C(T)$$

Consider next the exclude criterion. Let $\{T\}_I$ be the set of included transducers. Then the set of transducers which are not in either the excluded or included sets is $\{T\}_u - \{T\}_E - \{T\}_I$. Now in this case it is known that each combination of transducers to be investigated must represent a possible system. Thus $\{T\}_1$ must contain all of the transducers in $\{T\}_I$ and none of the transducers in $\{T\}_E$. Thus the following generalized exclude criterion is obtained.

If for every possible combination of transducers, $\{T\}_1$, such that

1. $\{T\}_1$ does not contain T.
2. $\{T\}_1$ does not contain $\{T\}_E$
3. $\{T\}_1$ does include $\{T\}_I$

One has

$$\max SV_{\{\mathfrak{m}\}_u} S_{\{T\}_1 + T} - \max SV_{\{\mathfrak{m}\}_u}(S_{\{T\}_1}) < C(T)$$

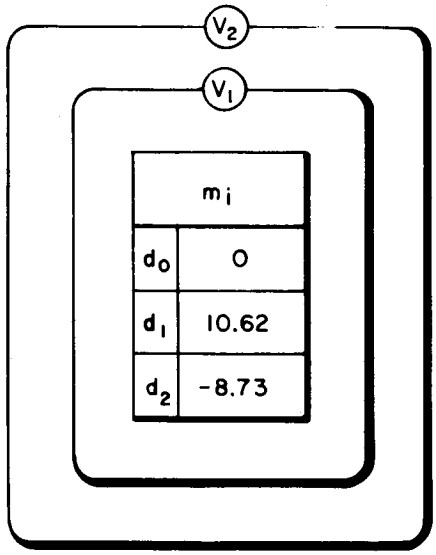
Then T is not in the optimum system.

Therefore as more and more transducers are placed in $\{T\}_I$ and $\{T\}_E$, the exclude criterion becomes more powerful and easier to apply, since the number of possible $\{T\}_1$'s is reduced exponentially. To take advantage of this effect, the iteration procedure is revised so that the include criterion is applied

to the entire list of transducers before the exclude criterion is applied. This order of testing is employed until testing is no longer fruitful, and the synthesis procedure goes on to part two.

In order to determine when testing is no longer fruitful, one proceeds as follows. A record is made of the contents of the undecided transducer set at the beginning of each iteration through the transducer list. When this iteration is completed the contents of the undecided transducer set are compared to this record, and if they are the same, testing is terminated. If the contents are not the same, the process is repeated and at least one more entire iteration is completed.

Finally, after testing the transducers one at a time, the situation illustrated in figure 4-15 may arise.



T1 YIELDS V1 ONLY
T2 YIELDS V2 ONLY

T1, T2 IN UNDECIDED TRANSDUCER SET AT END OF TESTING OF SINGLE TRANSDUCERS

FIGURE 4-15
EXAMPLE OF TRANSDUCER OR GROUP

In the case illustrated, T1 and T2 remained in the undecided transducers set, since when one was being tested the other was present in $T_u - T_E - T$ in the include criterion and some of the T_1 set of the risk difference list shows that at least one of the two transducers must be present in optimum list. To take this into account the so-called OR group of T1 and T2 is formed and subjected to the testing procedure of part one.

The OR group consists of synthetic transducers corresponding to each combination of the transducers containing at least one transducers. In this case, the combinations are (T1), (T2) and (T1 and T2). If the testing procedure of part one cannot place one of the combinations of the OR group in the included transducer set, then care is taken in part two of the synthesis procedure to be sure that each system considered contains at least one of each transducer in each OR group.

The detailed application of the first and second parts of the synthesis procedure to the problem for which the results are given in paragraph 2-2 is given in Appendix D.

4-6. SYMBOL LIST FOR SECTION IV

Symbol	Definition
$P(A)$	Probability of event A
$P(A\|B)$	Conditional probability of event A given event B
$t_{j;q,p}$	Phase transition from normal initial condition node to yth final condition node of phase p of stage q
$t'_{j;q}$	Stage transition from normal initial condition node to yth final condition node of stage q.
$t_{\ell,y;q}$	Stage transition from ℓ^{th} initial condition node to y^{th} final condition node of stage q
λ_c	Crew to mission value ratio
$S_{L;q,p}$	Lth simple transducer failure mode in phase of stage q. (L=0 denotes no transducer failure)
$M_{i;q,p}$	ith propulsion system malfunction in phase p of stage q (i=0 denotes no malfunction)
$d_{k;q,p}$	Decision k in phase p of stage q (k=0 denotes no action decision)
$R(j,q)$	Risk at final condition node j of stage q
$L(d_k m_i;q,p)$	Loss for malfunction-decision pair (d_k, m_i) in phase p of stage q.
$d_{k'_i;q,p}$	Optimum decision for $m_{i;p,q}$
$d_{k_i;q,p}$	Programmed decision for $m_{i;p,q}$
R	Total risk
$I_{i;q,p}$	$= \begin{cases} 1 \text{ if } d_{k_{i;p,q}} = d_o \\ 0 \text{ if } d_{k_{i;p,q}} \neq d_o \end{cases}$
V	General symbol for malfunction detector

Symbol	Definition
S'	General symbol for READI system
SV(S)	System value of S
$\mathfrak{m}$	Set of all propulsion system malfunctions
$\mathfrak{m}'_i$	Partition set of $\mathfrak{m}$
$\mathfrak{m}_{V1...Vn}$	Inseparable set of malfunctions detected by V1,..., Vn only
$a_1,...,a_n$	Set whose elements are $a_1,...,a_n$
$\mathfrak{m}_o^1$	Set of not monitored malfunctions
$d_{k'V1...Vn}$	Programmed decision for inseparable set of malfunctions $\mathfrak{m}'_{V1,...,Vn}$
{T}	A set of transducers
$\{T\}_u$	The set of all transducers
$\{T\}_o$	The optimum set of transducers
$\mathfrak{m}_u$	The set of all propulsion system malfunctions
$S_{\{T\}}$	READI system using transducer set {T}
C(T)	Adjusted cost of transducer T
A-B	The set consisting of all the elements of A less the elements of B
A+B	For disjoint sets, the logical union of A and B
$\{T\}_E$	The set of excluded transducers
$\{T\}_I$	The set of included transducers

SECTION V

DEVELOPMENT OF EQUIPMENT

5-1. OBJECTIVES

The Phase II equipment development program had two major objectives. These were:

- Develop techniques and equipment capable of meeting the functional, reliability, and flexibility requirements of a READI system
- Fabricate an experimental system suitable for test on a presently available rocket engine.

The results obtained in fulfilment of the first objective are discussed in paragraph 5-2 and those of the second objective are discussed in paragraph 5-3.

5-2. SYSTEM COMPONENTS

A. INTRODUCTION

One of the prime objectives of the equipment development phase is to develop the special techniques and equipment required for the fabrication of a READI system as it would be implemented for a launch vehicle. These special techniques and equipments will first be described in this section in terms of the general requirements placed on the components which constitute a typical READI system.

From an equipment viewpoint it is convenient to picture the READI equipment as a multichannel system. Each channel consists of one or more transducers, intermediate linear and two-state circuitry, and output buffer circuits leading to control elements in the vehicle. A

simplified block diagram of the READI system is shown in figure 5-1. All the transducer output signals are first normalized to the same signal form and magnitude (1-volt dc). These conditioned signals are then processed into a binary state (0, 1) by comparators in accordance with the transducer threshold levels specified in the catalog of malfunction detection techniques. The transducer self-check thresholds are also applied to other comparators to indicate transducer failures. The self-check comparator output (0, 1) and the malfunction detection comparator output (0, 1) are both applied to the V-logic circuits. The V-logic circuits perform the Boolian functions specified by the various catalogued malfunction detection techniques, and produce an output when the Boolian requirements are met and no transducer failure has occurred. The V-logic outputs are now processed by the decision logic circuits which initiate the desired remedial action in accordance with the engine malfunction indicated, the decision priority specified, and the mission phase of the launch vehicle.

The functional design requirements of a READI system may be completely defined in the following forms:

- A catalog of techniques, V's, for identifying the condition of the engine and associated subsystems
- Indication of necessary self-check provisions and channels where information and transducer redundancy are required to effect the otpimum trade-off between complexity and risk due to READI equipment failures
- A set of programmed decision rules (d's) in terms of the malfunction indication, V, as a function of phase of the mission.

In the remainder of this section, the various system component functional requirements are discussed in detail, but without reference to any specific propulsion system or vehicle.

B. TRANSDUCER REQUIREMENTS

Based on the experience gained through static testing of engines and subsystems, the input parameters to READI and the types of transducers needed are familiar, although the general requirements for READI transducers contrast somewhat with the requirements for static ground

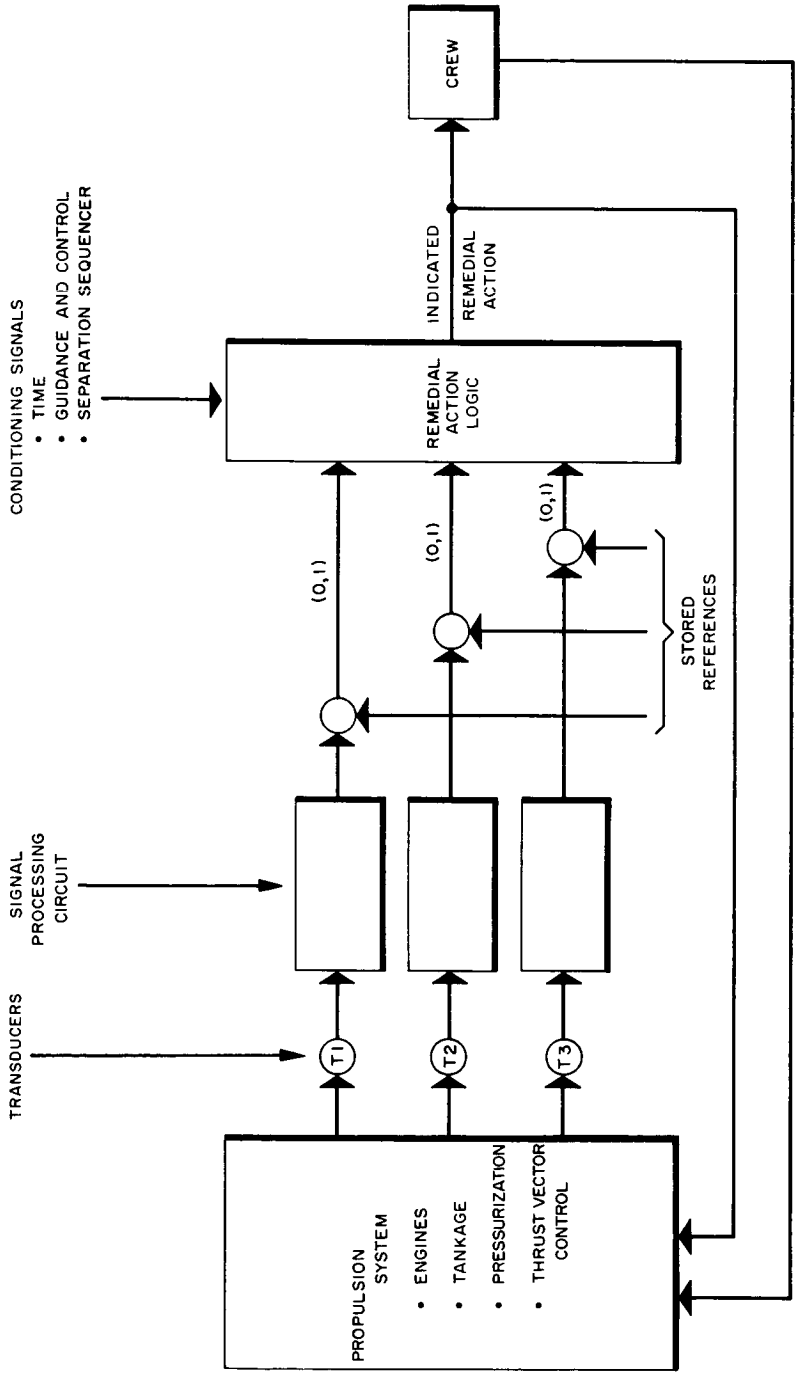


FIGURE 5-1. READI SIMPLIFIED BLOCK DIAGRAM

tests. Table 5-1 illustrates the contrasting requirements of READI and static ground testing applications for transducers monitoring such engine parameters as pressure, flow and temperature.

Table 5-1

Comparison of Transducer Requirements for Ground Test and Telemetry and READI Applications

	Ground Test and Telemetry	Airborne READI
Typical Accuracy Requirements (% full scale)	±1% including environmental effects	±2 to ±5% including environmental effects
Reliability	Loss of measurement seldom considered critical	Transducer failure can cause false, missed or wrong alarm; protection is required
Weight and Size	Seldom a consideration on the ground but becomes a vital problem in upper stages	Fewer transducers required, and still a problem in upper stages
Range	Wide range measurement required	Transducer can be tailored to critical decision range
Cost	Since large numbers of transducers are used, purchase cost is a consideration	Fewer transducers are used; cost of development, installation, calibration, etc, far exceed hardware cost
Dynamic Response	Generally high response output is required for detailed analyses	Typical fast response requirement is 10 milliseconds for 63% response to step. Temperature sensors are sometimes a problem. Response requirements generally less stringent than for ground test and telemetry
Processing Circuitry	Circuitry integrally packaged with transducers is sometimes advantageous	No advantage to integrally packaged circuitry. Better environmental control in central location yields higher reliability; processing circuits are quite specialized for READI

It was not one of the READI program objectives to attempt to improve transducers performance or reliability. Information gained from current evaluation programs being conducted by major rocket manufacturers,

together with other data and analyses, are used to select the best transducer configuration. In some READI applications it is expedient, or even mandatory, to use previously installed transducers. Therefore, the READI processing circuitry is designed to: (1) cope with a variety of transducer types, and (2) compensate for the more likely failures in transducers and cabling.

Typical transducers are shown in table 5-2, grouped according to output form and full scale indications.

1. Transducer Reliability

Previous analyses* have identified transducers and associated cabling as the major source of READI system unreliability. Techniques are demonstrated in Section IV to identify the optimum configuration for a READI system, including the use of information redundancy. Estimates of transducer failure rates range from 10^{-2} to 10^{-6} failures per mission, most being about 10^{-4}. This value is comparable to failure rates experienced by rocket engine components of similar complexity. A study of the effects of transducer and cable failures on the output signals indicates that over 90 percent of the failures result in either very high or very low (in many cases zero) outputs. This fact is used in tracing through systems to determine the effect of transducer failures in the synthesis procedure. This also suggests that techniques may be found to self-check transducer signals.

Reasonable limits on transducer outputs, and reasonable limits for the rate of change of transducer outputs, may be found. These limits may then be imposed as self-check criteria on the transducer signal.

- - - - - - -

*Details of Phase 1 are in Final Report, Sperry Report No. CA-4251-0160, Rocket Engine Analyzer and Decision Instrumentation (READI) Investigation, Vol. I and II, furnished by Sperry Gyroscope Company to National Aeronautics and Space Administration under contract NAS-8-4003.

Table 5-2

Transducer Signal Groups

Signal and/or Magnitude Variable	Frequency	Frequency Amplitude	D-C Volts		A-C Volts	
			≤250 mv	>250 mv	≤0.5 volt	>0.5 volt
RPM	Pulse pickup					
Flow	Pulse pickup					
Vibration		Velocity pickup				
Pressure				Potentio-metric	Wire strain gage; semi-conductor strain gage	Variable reluctance
Temperature			Thermocouple			
Position				Mechanical magnetic, or photo-electric switch		
Fire Detector				Continuous element		

2. Self-check Criteria on the Transducer Signal

a. Rate Positive and Negative Limits

Limits are imposed on rates by physical constraints. For example, the maximum positive rate of turbine rpm occurs with no load (propellant valves closed) and is limited by the short term torque-to-inertia ratio of the turbopump assembly. Rates in excess of reasonable limits therefore indicate failure of a transducer. Much rate of change limit data can be obtained from the study of analog recordings of the subject variable over normal and abnormal engine runs.

b. Maximum Positive and Maximum Negative Limits on Variables

Limits on the variable itself are more difficult to establish. For example, many READI decision limits are set for a variable below a given limit, and it is generally impossible to distinguish between legitimate malfunction indications and transducer failures in the low direction. As indicated in figure 3-6, it is possible to recognize some failed-high indications, especially if the determination is made before start or during the starting transient.

C. FUNCTIONAL REQUIREMENTS OF PROCESSING CIRCUITS

The electronic circuitry in a typical airborne READI system will accept a variety of inputs, as indicated in table 5-2, and will produce as an output electrical signals capable of altering the control of the vehicle. Typical output actions would involve:

- Actuation or deactuation of pilot stages of propellent valves
- Firing of explosively operated components
- Introduction of alternate signals to control servos.

The nature of processing which takes place between the input transducer signals and the output actions is specified by:

- Malfunction detection techniques*

- - - - - - -

*Phase 1 Final Report, Sperry Report No. CA-4251-0160, Vol. 1, p. 4-3 and 5-3; and Vol. 2, Appendix K.

- Requirements for redundancy and self-check
- Decision rules
- Output interface requirements.

The first three items of information are obtained from the output of Step 3, Optimization, described in the design procedure in Section III. It will be recalled that an optimum system is selected from the results of a complete evaluation of a subset of candidate systems, where the evaluation includes the effects of READI system failures. Output interface requirements are obtained from a study of the propulsion systems and the remedial actions programmed.

The presentation of malfunction detectors is in the form of a catalog in which input signals, signal processing and self-check requirements are specified. A catalog of signal space separations (malfunction detectors) for the H-1 vehicle is given in Appendix E.

The presentation of decision rules is in the form of tables of Boolian expressions for decisions in terms of malfunction detectors and mission phases. A typical decision rule would appear as

$$D2 = (p1 + p2) \quad (V1 \cdot V6 + V13 + V9 \cdot V9 + V12 : V10 + ---)$$

where

D2 = Decision No. 2
(p1+p2) = Phase 1 OR Phase 2
V1·V6 = V1 AND V6
V13 = OR V13
V9·V9 = OR V9 AND V9 (component redundancy)
V12·V10= OR V12 AND not V10

The presentation of the output interface requirements is in the form of electrical currents which must be supplied within specified voltage ranges for minimum periods of time in order to execute the desired decision.

1. Processing Circuitry Reliability Requirements

In any selected channel of the READI system, the transducers, cabling, processing circuit, comparators, and logic form a chain of

electrical elements. Therefore, failures of the processing and logic are equally as important as failures of transducers and cabling. In either area the reliability of components will be a deciding factor in the selection of component basic types and suppliers. Single chip integrated electronic microcircuitry has potentially an order of magnitude higher reliability than conventional semiconductor circuitry, and, therefore, is favored for use whenever suitable circuits are available or can be produced. The predicted trends for various types of electronic circuitry are shown in figure 5-2.

Using integrated circuits, the computed reliability of typical processing circuits is 10 to 20 times higher than the associated transducers. Therefore, in the evaluation of systems, the entire failure probability is assigned to the transducers. The predicted failure rate per mission of each channel of a READI system must be computed and predicted circuit failure rates in excess of 10^{-6} per mission are indicative of a possible trouble area. Further attention is required in this case to consider the nature of the resulting false, missed, or wrong alarms and the failure rates that have been used in system design for the associated transducers.

2. Processing Circuitry Flexibility Requirements

The overall design of a READI system for a launch vehicle will be an iterative process, even after the optimum configuration is found. This is the case because the initial design will use a great deal of estimated input data, which will change as the development and test of subsystems progresses. Also, any future launch vehicle will be used for a variety of missions, some manned and others unmanned, and mission profiles, alternate missions, storage burning time, and payload weights will vary. For these reasons it is essential that the READI system be quite flexible. Specifically, the following should be easily changeable.

- Malfunction detection and self-check limits
- Logic to accommodate changes in information and component redundancy
- Logic to permit changes in decision rules.

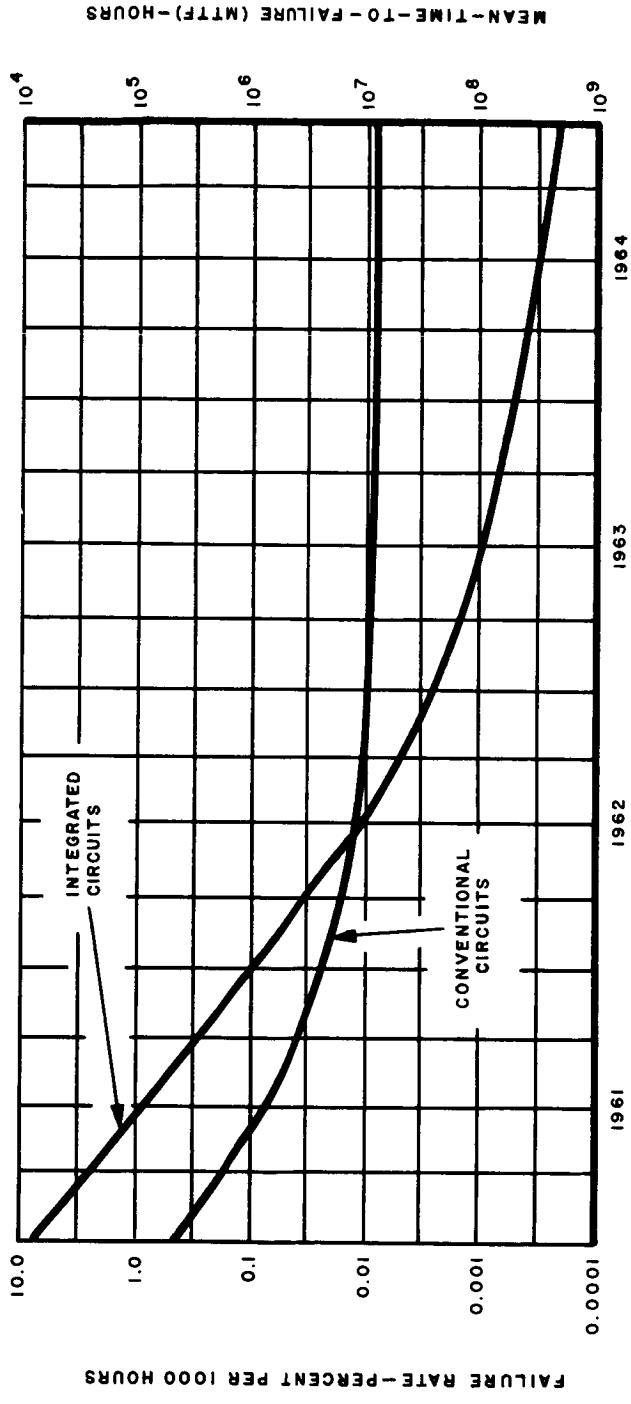


FIGURE 5-2 RELIABILITY TRENDS FOR INTEGRATED AND CONVENTIONAL CIRCUITS

Changes of the type noted above require varification test procedures which are most conveniently accomplished away from the vehicle in a subassembly test. One approach to solving this problem is to use a modular build-up of units which can be easily replaced in the main electronic assembly when a change is required. This method of construction also has other obvious advantages of flexibility in the development and manufacture of the equipment.

3. READI Signal Processing from Transducer to Decision

In the preceding paragraphs the READI equipment requirements have been developed in terms of functional, reliability, flexibility and packaging requirements. Now the circuit design approaches which have been developed to meet these general requirements will be described.

Two basic approaches were considered in the first phase of the READI investigation to accomplish the required processing. These approaches used parallel processing and a serial digital computer. A trade-off study* indicated that, for a five-engine second stage, a combination of the parallel and serial techniques was attractive. The parallel technique was favored for simple processing requirements and the serial computer was favored for the more complex requirements, especially those involving high accuracy.

System trade-off studies, conducted during Phase 2, have indicated that the optimum READI configuration for a typical large launch vehicle will contain fewer transducers per engine and, therefore, have reduced signal processing requirements than was predicted in the Phase 1 investigation. Specifically, the number of transducers per engine has been reduced from 22-28 to 8-10. This reduction makes the strictly parallel approach appear much more attractive. It should be noted that the processing circuitry developed for the H-1 READI system completely meets all of the functional requirements which were initially spelled out at the beginning of Phase 2. It was not necessary to compromise the desired performance of any channel of the system to stay within the constraints of parallel processing techniques.

- - - - - - -

*Phase 1 Final Report, Sperry Report No. CA-4251-0160, Vol. 2, Appendix C.

In the parallel approach three basic operations are performed. In order, these are:

- Analog processing of transducer signals
- Comparison of processed signals to references or to other processed signals
- Logical (i.e., two-state) processing to produce a decision.

4. Signal Processing Channels

The output signals of the various transducers (rpm, flow, temperature, etc.) differ in their form and magnitude, as shown in table 5-2. Standard processing circuits have therefore been developed to normalize the different transducer signals to a nominal 1-volt dc level, providing a common signal form and magnitude for further processing (level detection, multiplexing, converting, etc.) To facilitate the design of these signal processing circuits, the transducers were fitted into one of six categories, based upon the transducer output signal. The transducers are listed in table 5-2 according to their respective group and the monitored variable.

To illustrate the processing circuits used in implementing the analog signal processing, the circuits used to process the following transducer signal groups will be discussed:

- Low level d-c volts (temperature)
- High level d-c volts (pressure)
- Frequency (rpm)
- Frequency-amplitude (vibration)
- A-c volts (pressure).

a. Low Level D-C Volts (Temperature)

The processing circuit developed for low level d-c input signals is shown in figure 5-3. This circuit performs the following operations on the input signal:

- Modulation
- Amplification

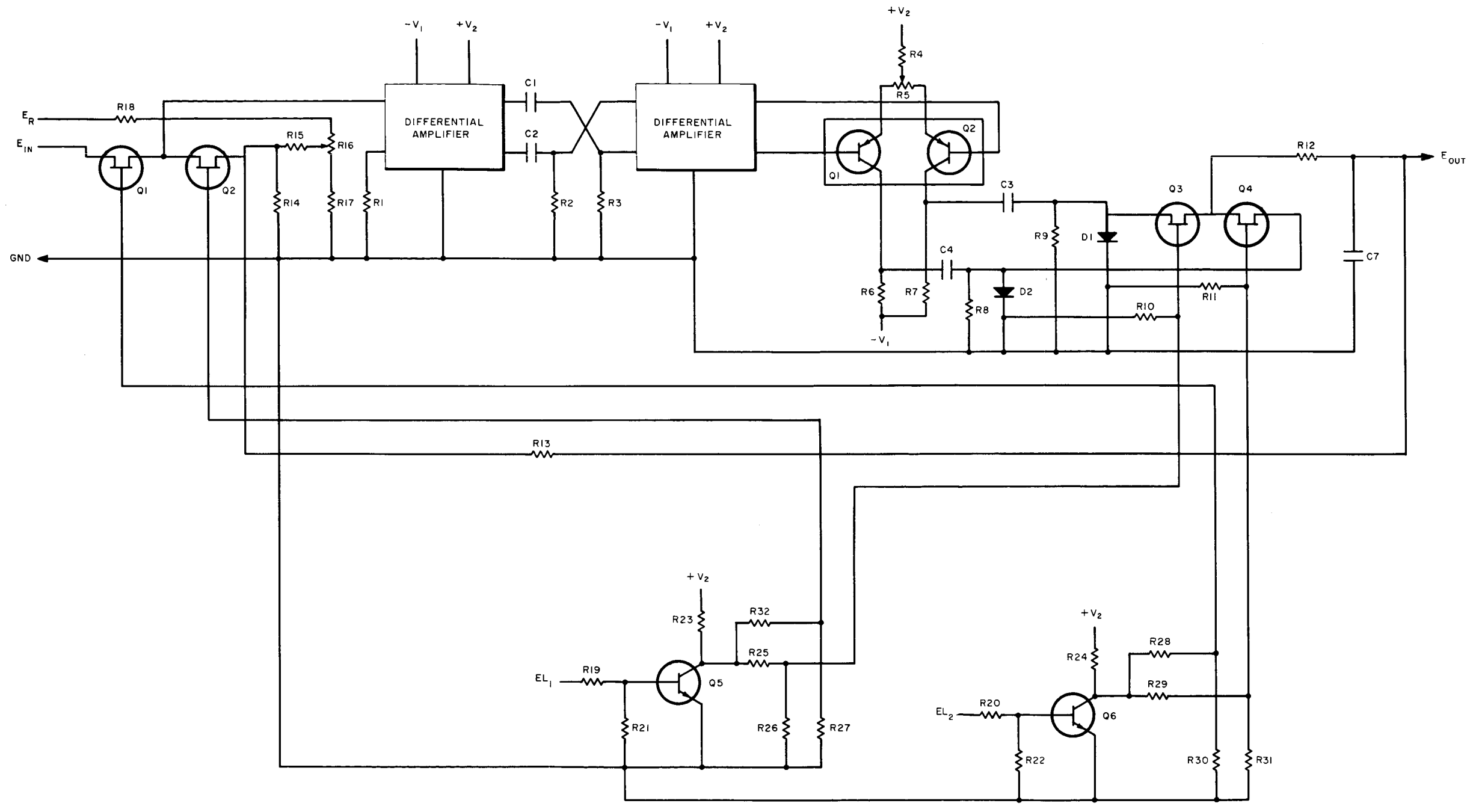


FIGURE 5-3
PROCESSING CIRCUIT LOW
LEVEL D-C INPUT (TEMPERATURE)

- Demodulation
- Filtering.

The low level d-c signal is first modulated at a selected frequency by field effect transistors. To provide a greater output signal accuracy over a restricted input signal range, a reference voltage (E_R) is provided. The difference between the input signal (E_{IN}) and this reference signal (E_R) is modulated and provides an output signal (E_{OUT}) equal to $G(E_{IN} - E_R)$ with increased accuracy over the restricted range. The modulated signal is amplified and then demodulated by field effect transistors. The demodulated output signal ripple is then attenuated by a low-pass filter, providing a d-c signal compatible with the requirements of the circuits performing subsequent operations.

b. High Level D-C Volts (Pressure)

The processing circuit developed for high level d-c output transducers is a low gain differential amplifier or, as in the case of the potentiometer pressure transducer, a simple resistive attenuator. Since the transducer output signal form is compatible with the requirement of the processing circuit output signal, only the magnitude of signal must be modified. Therefore, a d-c gain equal to or less than four is the required processing circuit characteristic.

c. Frequency (RPM)

Figures 5-4 and 5-5 illustrate the processing circuit developed for processing frequency signals from pulse pickup transducers. Figure 5-4 shows the analog portion of the processing circuit, while figure 5-5 shows the logical design and operation of the frequency-to-analog converter. The following operations are performed by the processing circuit:

- Transducer output signal shaping
- Frequency-to-analog conversion
- Modulation
- Filtering.

The transducer output signal frequency is initially reshaped into a square wave for use by the frequency-to-analog converter. The frequency-to-analog converter accepts these square waves and generates a constant time interval on the output at the same rate as the applied signal

from the transducer. This constant time interval is applied to a modulator as the reference modulating frequency. The reference voltage to the modulator is modulated at a rate equivalent to the incoming transducer frequency and for an interval equivalent to the constant time base generated. The output signal of the modulator is, therefore, a series of constant volt-second areas occurring at the same rate as the transducer output pulse rate. This volt-second area is now averaged by a low-pass filter which results in a d-c output that is proportional to the output frequency of the transducer.

d. Frequency-Amplitude (Vibration)

The processing circuit developed to condition frequency-amplitude signals is illustrated in figure 5-6. This circuit performs the following functions:

- Differentiation
- Band-pass filtering
- Amplification
- Rectifying
- Filtering of ripple.

The frequency-amplitude signal to be processed is received from a velocity-type vibration pickup. The required output of the conditioning circuit is to be meaured of the acceleration. The transducer output signal is therefore differentiated to provide the required acceleration information. Furthermore, the acceleration signal is to be limited in its frequency spectrum to a specified bandwidth. A band-pass filter, which is composed of two second order active filters, one low pass and the other a high pass, is therefore employed. The resulting signal is amplified, rectified and filtered, and provides a signal of approximately 1-volt dc for further processing.

e. A-C Volts (Pressure)

Figure 5-7 illustrates a typical signal processing channel developed to condition a-c input signals from transducers. The conditioning functions performed by this processing channel are:

- Amplification
- Rectification
- Filtering.

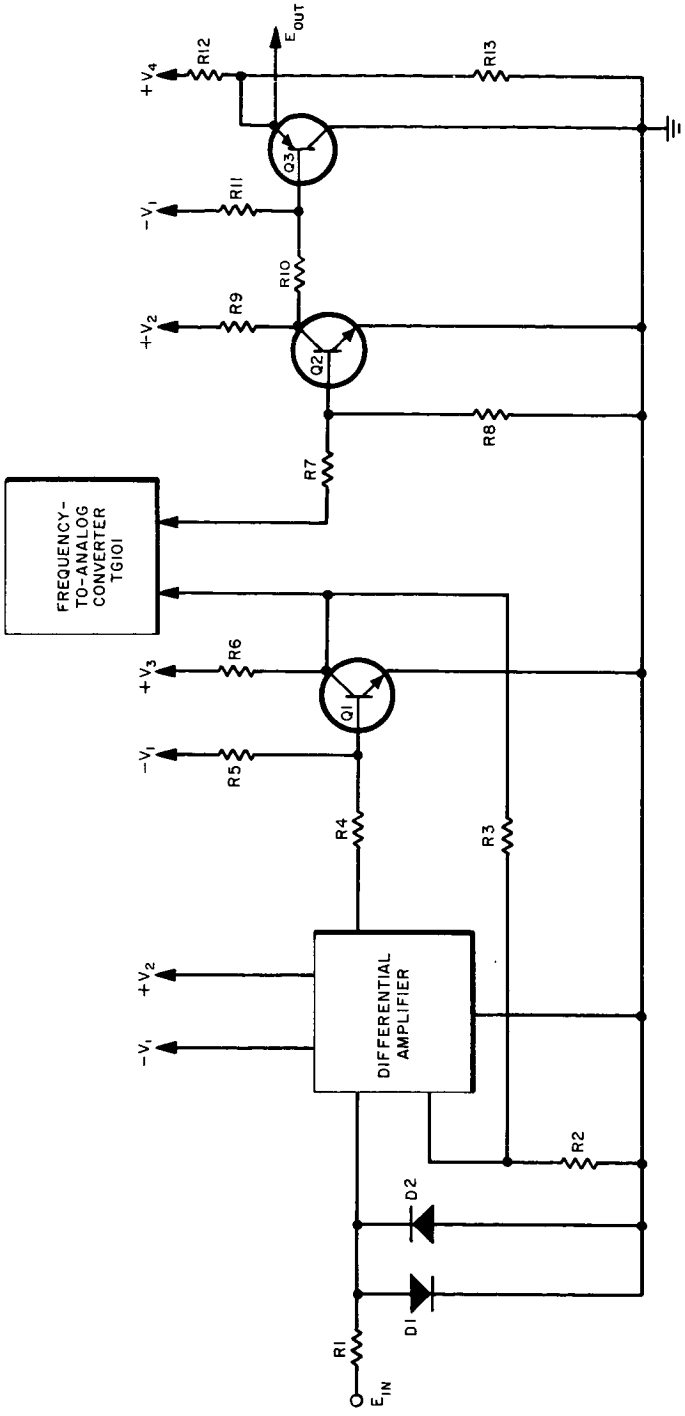
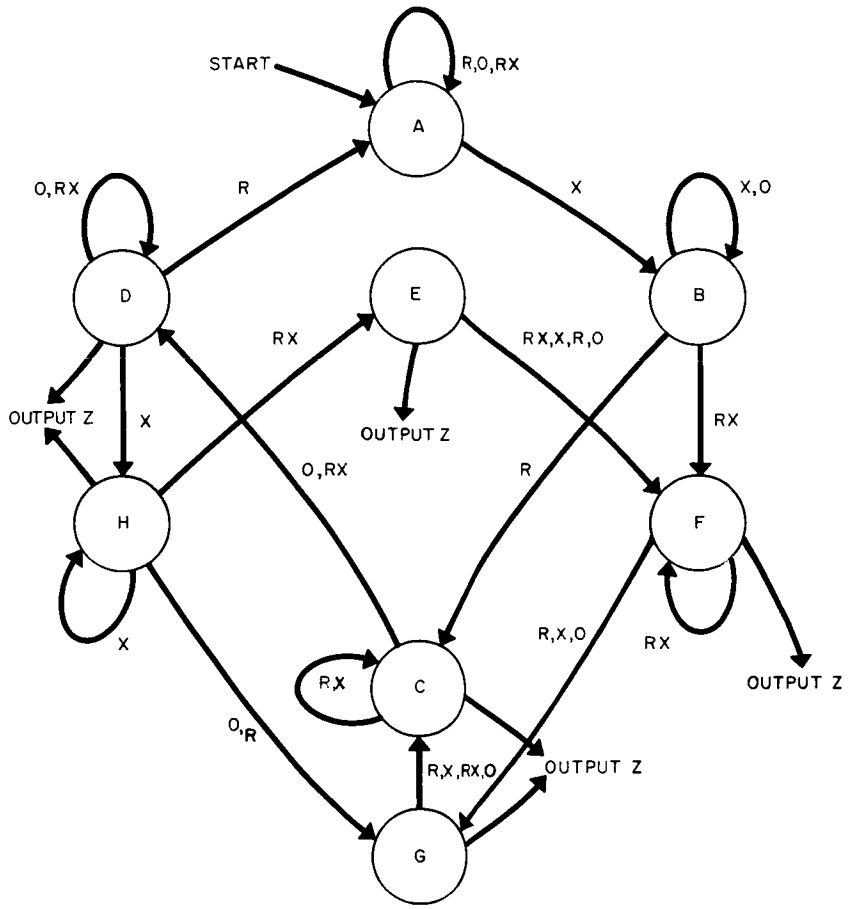


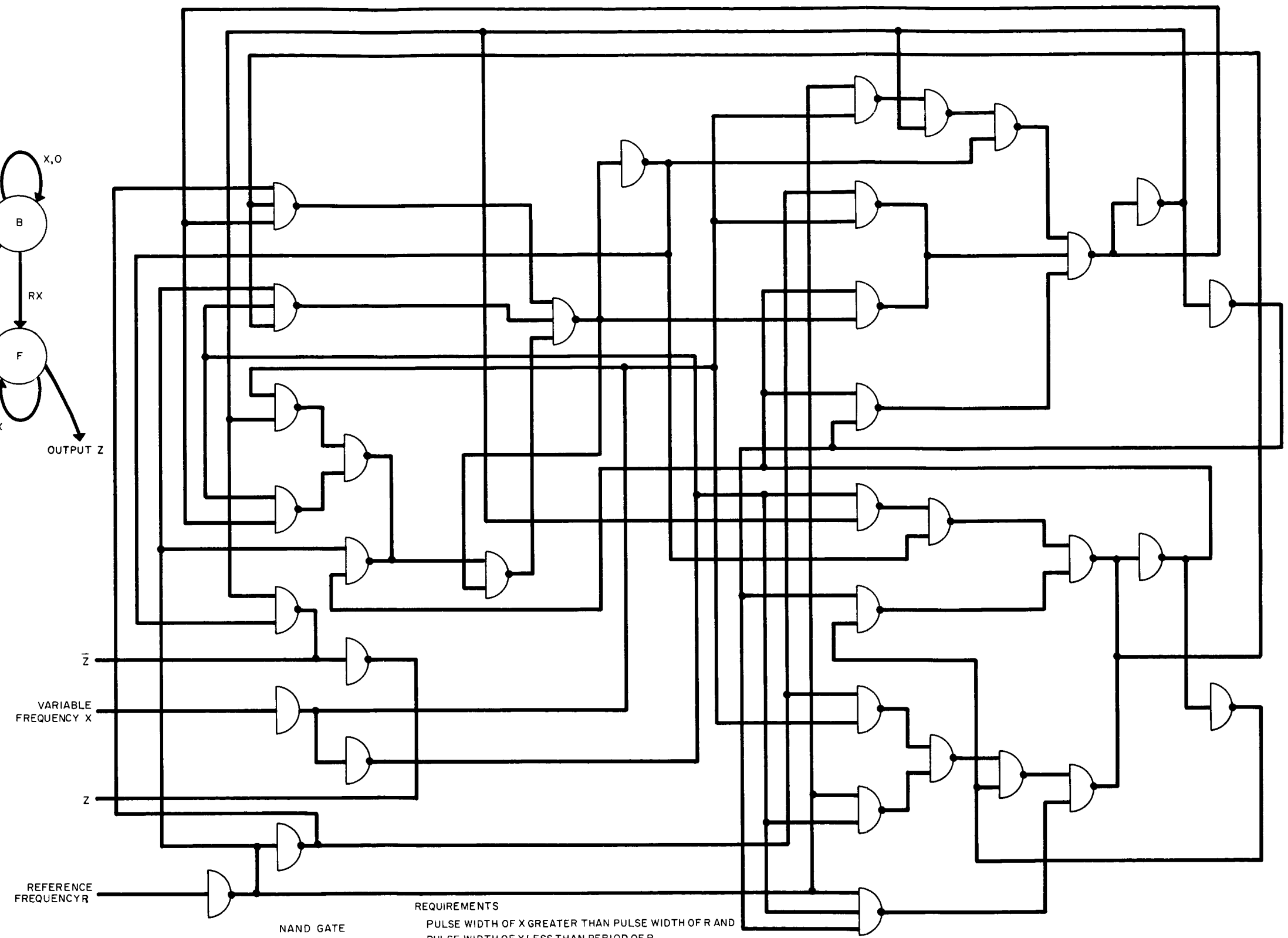
FIGURE 5-4 PROCESSING CIRCUIT FREQUENCY INPUT (RPM)



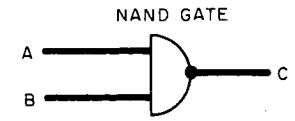
INDICATION OF THE STATE OF THE FREQUENCY-TO-ANALOG CONVERTER

O = ABSENCE OF R AND/OR X

RX = PRESENCE OF R AND X



NAND GATE



$\overline{A}\,\overline{B} = C$

REQUIREMENTS

PULSE WIDTH OF X GREATER THAN PULSE WIDTH OF R AND PULSE WIDTH OF X LESS THAN PERIOD OF R.

R = REFERENCE FREQUENCY

X = INPUT - VARIABLE FREQUENCY

Z = CONSTANT TIME BASE OUTPUT

$\overline{Z}$ = COMPLEMENTED CONSTANT TIME BASE OUTPUT

FIGURE 5-5

FREQUENCY-TO-ANALOG CONVERTER TG 101

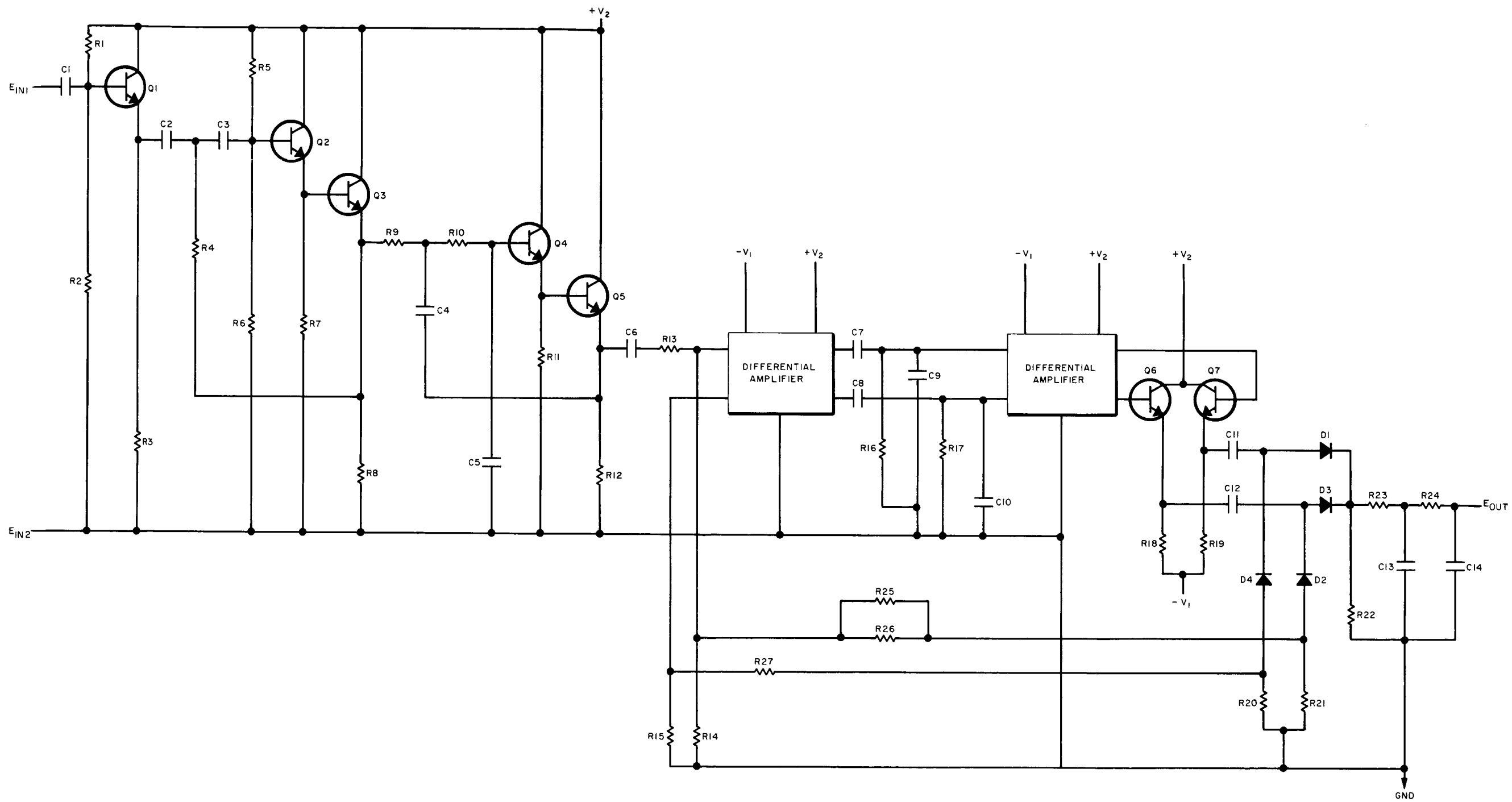


FIGURE 5-6
PROCESSING CIRCUIT,
FREQUENCY-AMPLITUDE INPUT (VIBRATION)

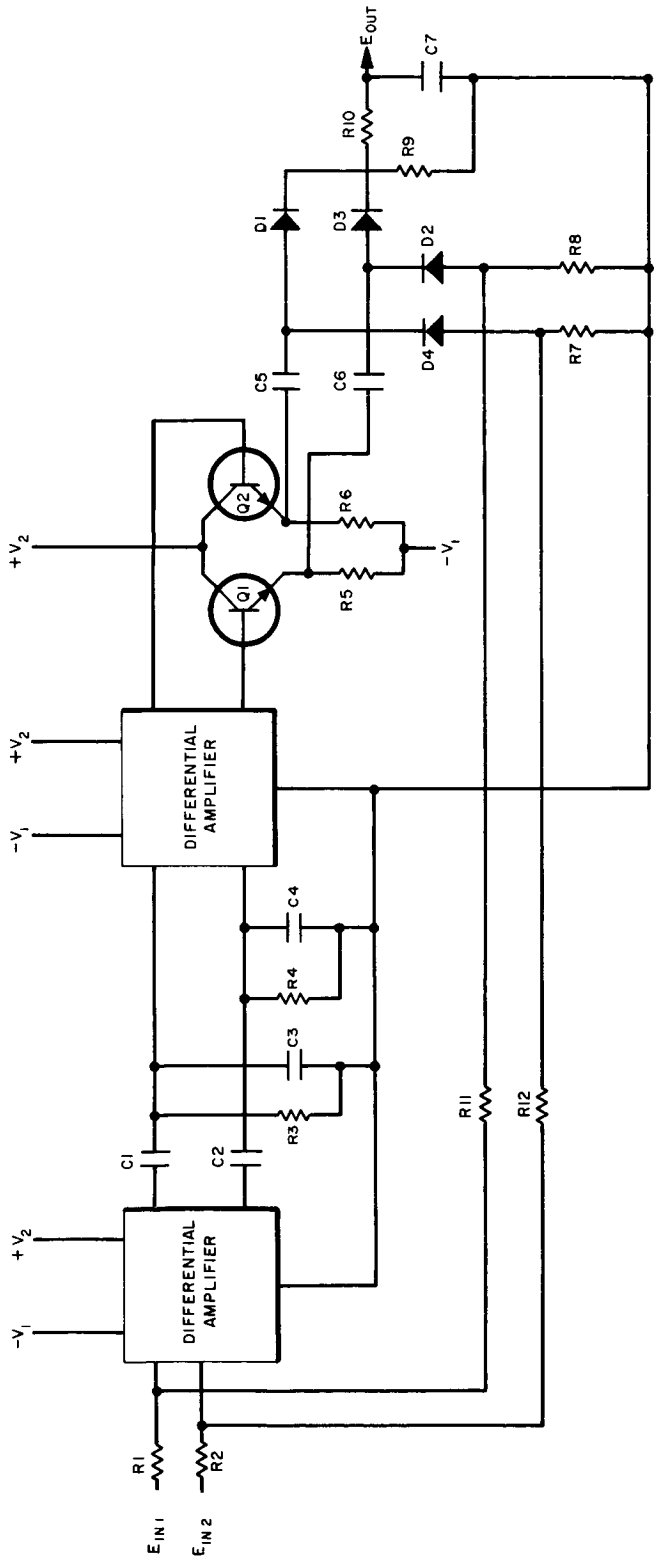


FIGURE 5-7
PROCESSING CIRCUIT-A-C INPUT (PRESSURE)

The amount of amplification required is determined by the magnitude of the applied input signal from the transducer. In figure 5-7, the transducer output signal is considered low level (refer to table 5-2); therefore, the gain of the amplifier is high. The amplified signal is then rectified and filtered for further signal processing.

f. Low-Level Comparator

All the signal conditioning circuits used in READI require conversion from an analog form to a digital form (1 or 0 state) for processing by the V-logic. The circuit developed to perform this function in READI is the low-level comparator C101. The comparator converts the output signals from the processing circuits into a binary state at a predetermined signal level. Figure 5-8 illustrates the circuit and required operating characteristics of the comparator. The circuit is a high gain d-c amplifier with positive feedback. The desired operating characteristics of the comparator are based upon the malfunction detection accuracy required and the peak-to-peak value of the ripple on the signal conditioning circuit output. The malfunction detection accuracy determines the accuracy of the pull-in* and drop-out* voltage, while the signal conditioning circuit output voltage determines the minimum hysteresis required to reduce random triggering of the comparator.

The accuracy of the pull-in and drop-out voltages of the comparator is dependent upon the drift characteristics of the d-c amplifier and the stability of the reference signal. The stability of the reference voltage is better than ±1.0 percent over the operating temperature range; therefore, the drift characteristics of the comparator are determined primarily by the magnitude of the d-c amplifier drift. The allowable comparator drift is ±10 millivolts (referred to input E_{IN}). The nominal reference voltage (E_R) is 1.0-volt dc, resulting in a drift error of ±1.0 percent. Therefore, the comparator has an error of slightly over 1.0 percent.

- - - - - - -

*The value of voltage which causes the output voltage to switch abruptly from one state to the other.

D. LOGIC CIRCUITS

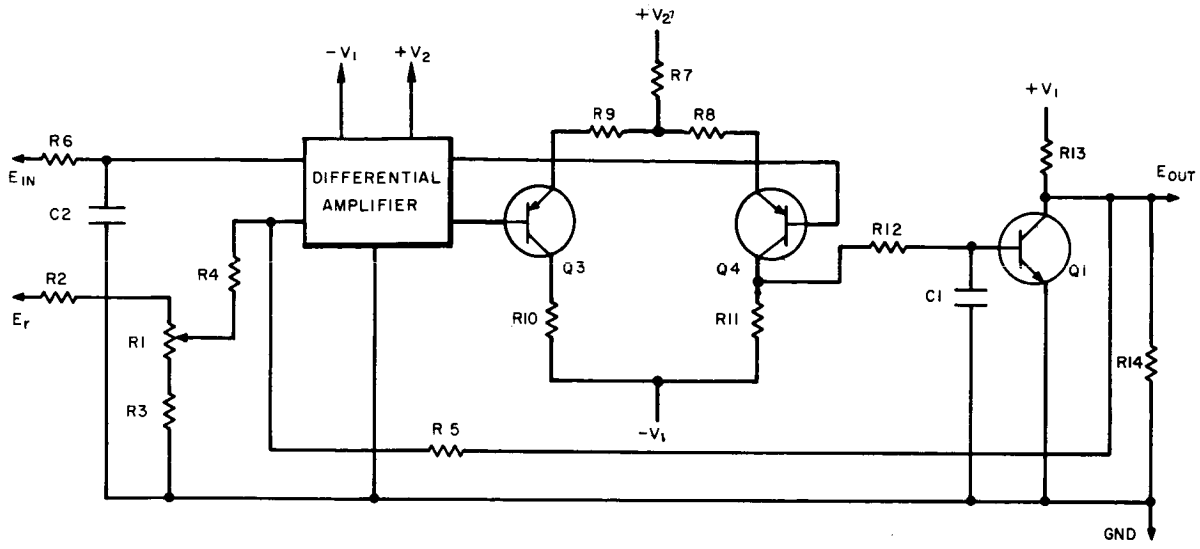
The micrologic elements used in this experimental READI system are the set of compatible, integrated logic building blocks shown in figure 5-9. The elements are manufactured using a process by which all the necessary transistors and resistors are diffused into a single silicon wafer (monolithic integrated circuit). The individual gates within the logic blocks are interconnected by metal over oxide. The Boolian functions for the micrologic elements are shown in figure 5-9 and are expressed in both positive logic (A = 1) and negative logic (A = 0). The following circuits have been developed from these building blocks to perform the required logic functions in READI.

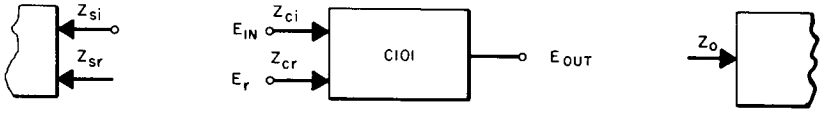
- V-logic
- Decision Logic
- Clock
- Time delay.

1. V-logic

The V-logic was developed to combine logically the processed engine data in order to sense an engine malfunction. Additional processed signals are applied to the V-logic in order to enable the logic to differentiate an engine malfunction from a failed transducer, thus minimizing the probability of false alarms (indication of an engine malfunction when none has occurred).

Figure 5-10 illustrates the circuit construction and the operation of the V-logic. The presence of a transducer failure (SC_m) prior to the occurrence of an engine malfunction (S_n) inhibits indefinitely any indication of an engine malfunction (V_i) associated with the failed transducer. The V-logic also requires that the potential engine malfunction must be present for two consecutive clock pulses before the engine malfunction is indicated, thus preventing false alarms caused by spurious noise pulses. Therefore, if the transducers associated with the potential engine malfunction have not failed, and the potential engine malfunction is present for two consecutive clocks pulses, the engine malfunction is indicated at the V-logic output (V_i). One other input which may be used to inhibit the V-logic output is the time delay input. The operation of this circuit will be discussed in detail later.





INPUT SIGNAL, E_{IN}

ALLOWABLE VOLTAGE RANGE - $\pm 3V$

ALLOWABLE SOURCE IMPEDANCE $Z_{si} < 10K\ \Omega$

INPUT IMPEDANCE $Z_{ci} > 50K\ \Omega$

REFERENCE SIGNAL E_r

ALLOWABLE VOLTAGE RANGE - $\pm 3V$

ALLOWABLE SOURCE IMPEDANCE $Z_{si} < 10K\ \Omega$

INPUT IMPEDANCE $750\ \Omega < Z_{cr} < 1000\ \Omega$

VOLTAGE FEEDBACK INTO $Z_{sr} < 100\ mv$

OUTPUT SIGNAL E_o

$E_o < +0.6$ FOR $E_{IN} > E_r + E_h \pm 0.01V$

$E_o = +2V$ FOR $E_{IN} < E_r$

HYSTERISIS $5mv < E_h < 20mv$

PULL-IN DRIFT $E_d < \pm 10mv$

$Z_o = 2K\Omega$ OR $4K\Omega$; COMPARATOR IS AJUSTABLE TO DRIVE ONE OR TWO LOGIC ELEMENTS

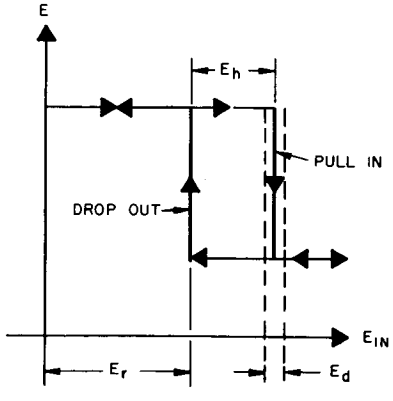
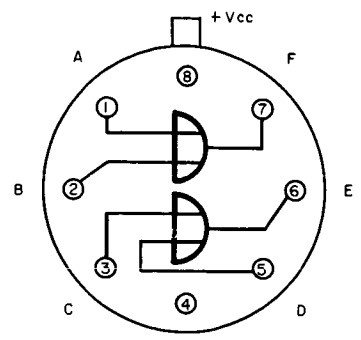


FIGURE 5-8

LOW LEVEL COMPARATOR, SCHEMATIC DIAGRAM

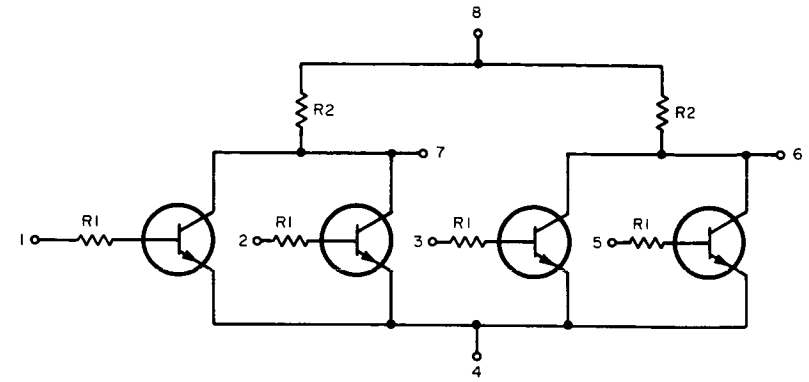
DUAL TWO-INPUT GATE



POSITIVE LOGIC: $F = \overline{\overline{A+B}} = \overline{A}\,\overline{B}$
$E = \overline{\overline{C+D}} = \overline{C}\,\overline{D}$

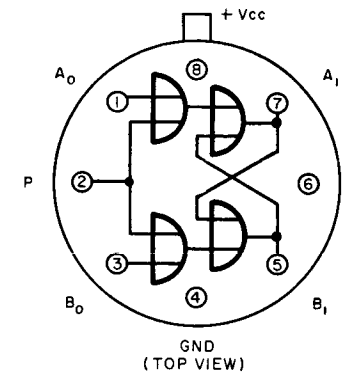
NEGATIVE LOGIC: $F = \overline{\overline{A}\,\overline{B}} = \overline{A}+\overline{B}$
$E = \overline{\overline{C}\,\overline{D}} = \overline{C}+\overline{D}$

DUAL TWO-INPUT GATE SCHEMATIC



TYPICAL RESISTOR VALUES
R1 = 450Ω
R2 = 640Ω

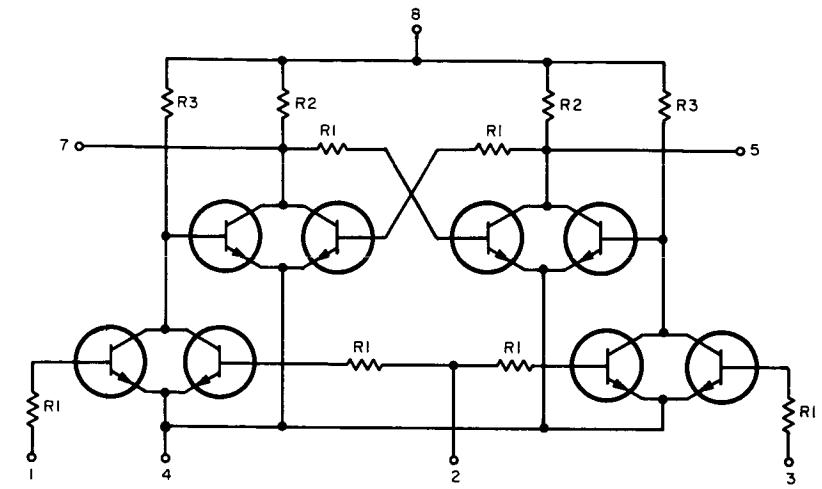
HALF SHIFT REGISTER ELEMENT
(WITHOUT INVERTER)



POSITIVE LOGIC: $A_1 = \overline{B_1}(A_0+P)$
$B_1 = \overline{A_1}(B_0+P)$

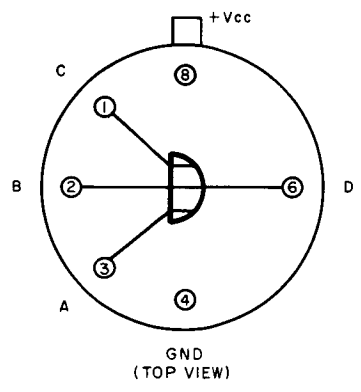
NEGATIVE LOGIC: $A_1 = \overline{B_1} + A_0 P$
$B_1 = \overline{A_1} + B_0 P$

HALF SHIFT REGISTER SCHEMATIC
(WITHOUT INVERTER)



TYPICAL RESISTOR VALUES
R1 = 450Ω
R2 = 640Ω
R3 = 800Ω

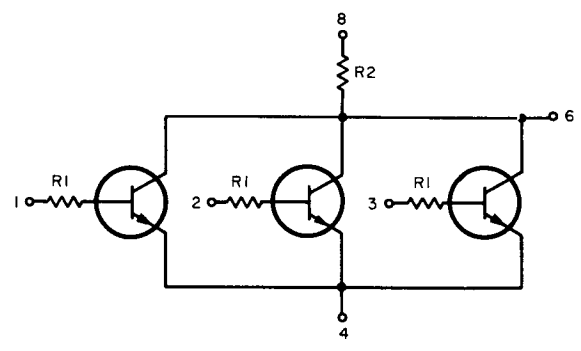
GATE ELEMENT



POSITIVE LOGIC: $D = \overline{A+B+C}$
$= \overline{A}\,\overline{B}\,\overline{C}$

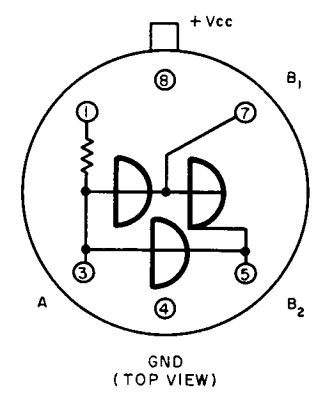
NEGATIVE LOGIC: $D = \overline{A\,B\,C}$
$= \overline{A}+\overline{B}+\overline{C}$

THREE-INPUT GATE SCHEMATIC



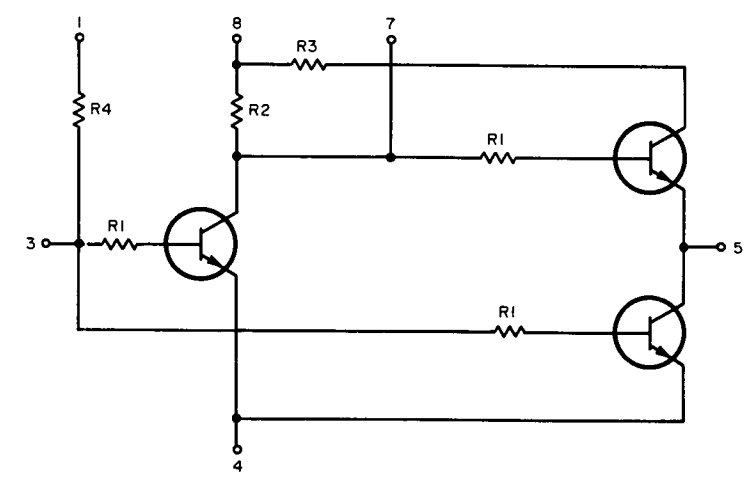
TYPICAL RESISTOR VALUES
R1 = 450Ω
R2 = 640Ω

BUFFER ELEMENT



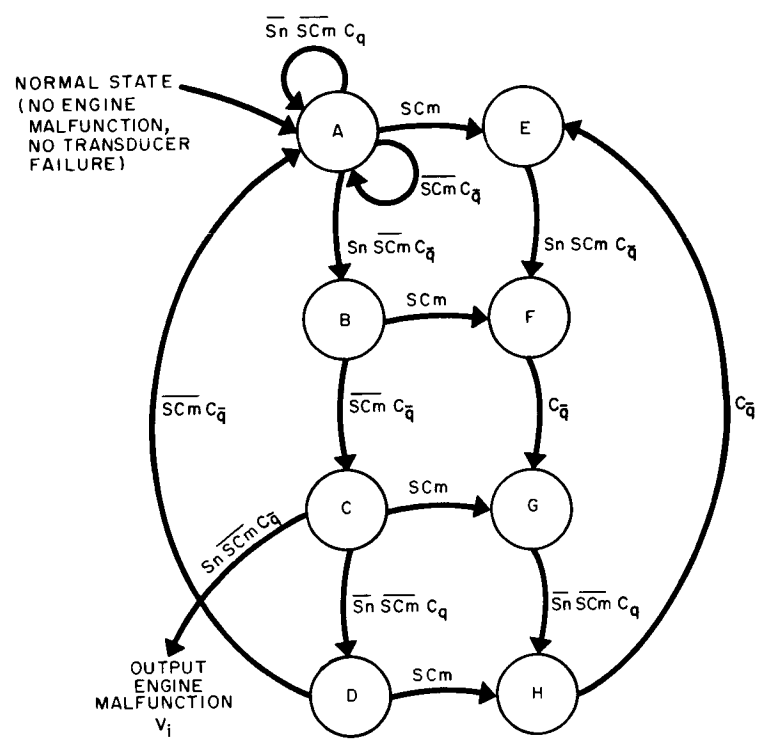
POSITIVE AND
NEGATIVE LOGIC: $B_1, B_2 = \overline{A}$

BUFFER ELEMENT SCHEMATIC



TYPICAL RESISTOR VALUES
R1 = 450Ω
R2 = 640Ω
R3 = 100Ω
R4 = 1000Ω

FIGURE 5-9
MICROLOGIC ELEMENTS



CLOCK PULSES C_q AND $C_{\bar{q}}$ OCCUR ALTERNATELY.
THE PRESENCE OF SCm INDICATES Sn IS PRESENT.

INDICATION OF THE STATE OF THE V-LOGIC

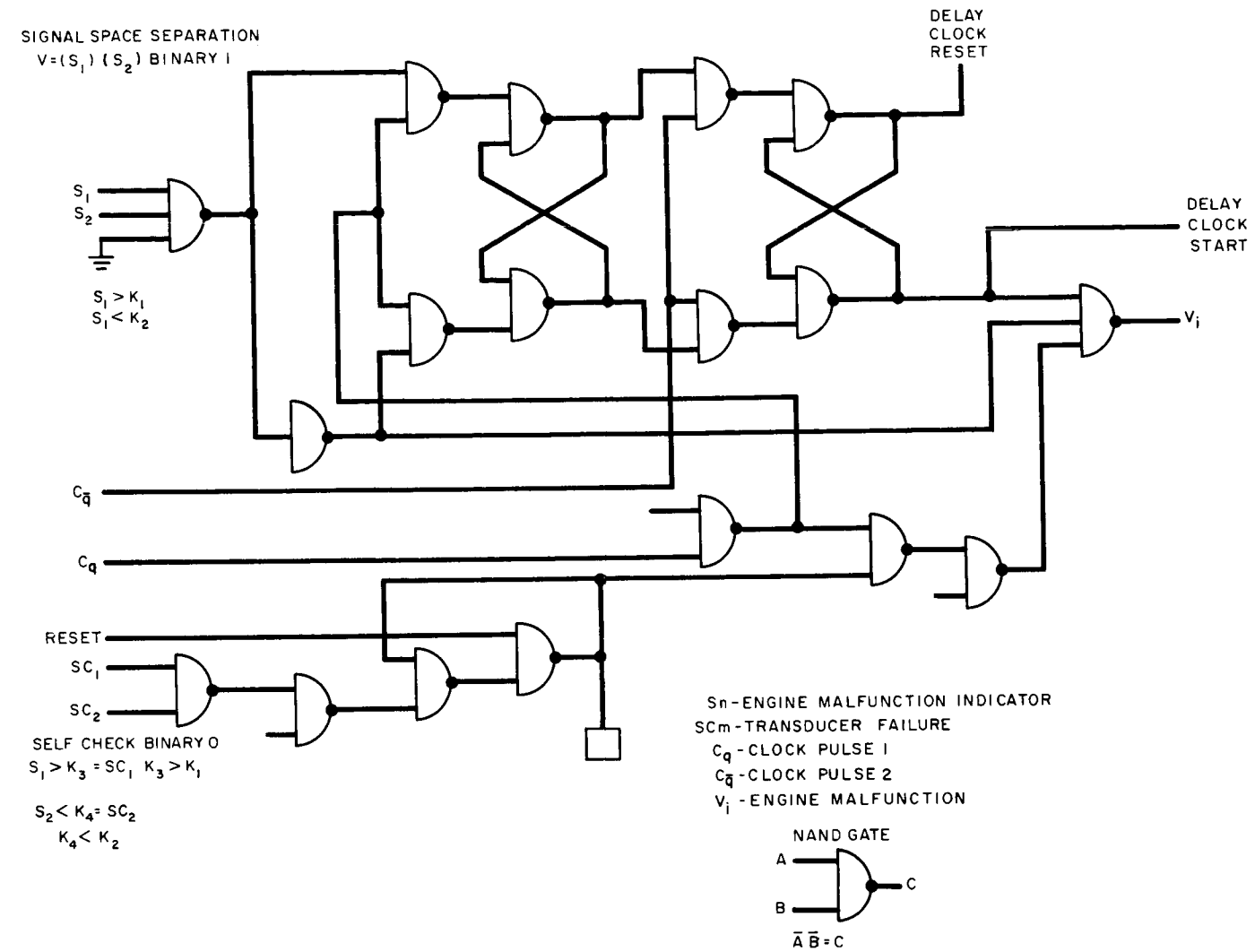


FIGURE 5-10
LOGIC FLOW AND CIRCUIT DIAGRAM

An input sometimes used to prevent an erroneous transducer failure indication is the output of the time delay from the stage start circuit. This signal inhibits the V-logic so that the initial abnormal conditions of the engine at start, when compared to the steady state running conditions of the engine, will not preclude the use of certain malfunction detection signals to determine engine malfunctions. When the start signal is given, all V-logic circuits are initially reset, thus insuring that erroneous information does not prevent READI from performing properly.

2. Decision Logic

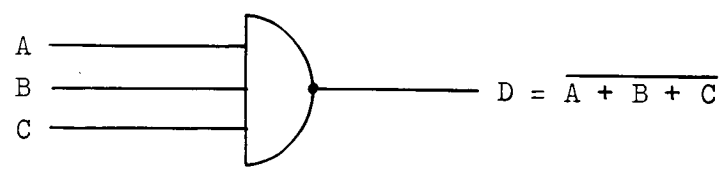
The V-logic output signal is further processed by the decision logic in accordance with the particular engine malfunction and mission phase. The decision logic outputs are also modified by the decision priority. The decision circuit was designed using logical combinations of NAND gates. As illustrated in Section III,

$$d_1 = V1 \cdot V2 \cdot \overline{V3}$$

$$d_2 = V1 \cdot V2 \cdot V3$$

Implementing these decisions using NAND gates results in the following:

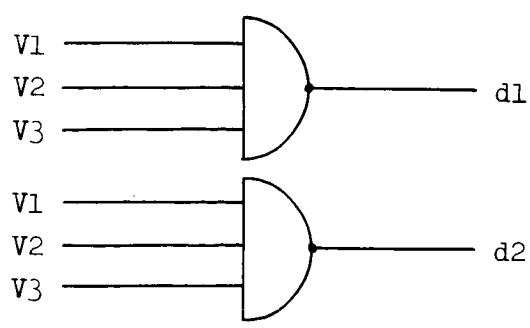
NAND GATE



Therefore,

$$d1 = \overline{\overline{V1} + \overline{V2} + V3}$$

$$d2 = \overline{\overline{V1} + V2 + V3}$$



3. Clock

All the timing signals in READI are derived from a central clock. The circuit for four stages of the central clock is shown in figure 5-11. Also shown in the figure is a truth table illustrating the operation of a stage of the clock. The various outputs of the clock stage are used in association with the other logic functions, such as:

- V-logic clock pulses - C_q and $C_{\bar{q}}$
- Frequency-to-analog converter reference frequency - C_q
- Cascaded clock stages - $C_{\bar{q}}$
- Time delay - q and $\bar{q}$
- Thermocouple reference frequency - q and $\bar{q}$

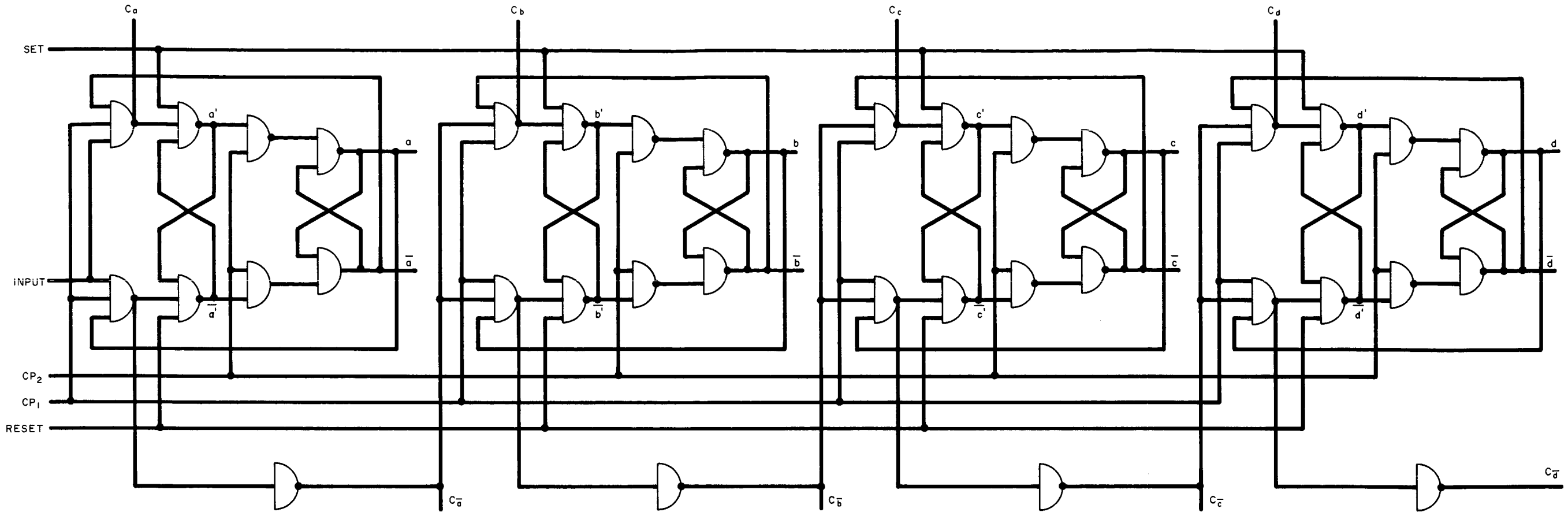
The central clock is presently compossd of twelve cascaded clock stages. The input frequency to the clock is 16 kc, thus providing clock frequencies down to $16/2^n$ kc, where n equals integers from 0 to 12.

4. Time Delay

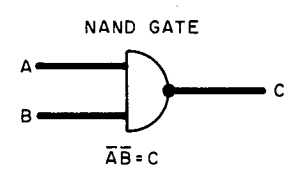
A time delay is generated by selectively gating a group of cascaded clock stages. These clock stages are separate from the required central clock stages previously discussed, but receive their input excitation from the central clock. The V-logic circuits require time delays for malfunction detection. Two such delays are:

- Time delay after start
- Time delay after a potential malfunction indication.

A typical time delay circuit is shown in figure 5-12. The clock is initiated by the V-logic circuit. The central clock pulse rate required for a specific time delay is such that the product of the number of input pulses and the reciprocal of the pulse rate is equal to the required time delay. When the time delay clock has received the correct number of pulses, the delay clock input is inhibited and the delay clock output enables the associated V-logic output. The time delay clock is immediately reset when a potential engine malfunction is absent, thus stopping the time delay and resetting to await another potential engine malfunction.



TRUTH TABLES FOR BINARY COUNTER STATES								
(FOR CP_1)					(FOR CP_2)			
q' (CP_1-1)	q (CP_2-1)	CP_1	$C_{\overline{q}}$	q' (CP_1)	q (CP_2-1)	CP_2	q'	q (CP_2)
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	0
0	0	1	0	0	0	1	0	0
0	0	1	1	1	0	1	1	1
0	1	0	0	0	1	0	0	1
0	1	0	1	0	1	0	1	1
0	1	1	0	0	1	1	0	0
0	1	1	1	0	1	1	1	1
1	0	0	0	1				
1	0	0	1	1				
1	0	1	0	1				
1	0	1	1	1				
1	1	0	0	1				
1	1	0	1	1				
1	1	1	0	1				
1	1	1	1	0				



C_q = TYPICAL CLOCK OUTPUT FOR V LOGIC
$C_{\overline{q}}$ = TYPICAL COMPLEMENTED CLOCK OUTPUT FOR V-LOGIC
q = TYPICAL COUNTER OUTPUT STATE
$\overline{q}$ = TYPICAL COUNTER COMPLEMENTED OUTPUT STATE

FIGURE 5-11
FOUR STAGE COUNTER

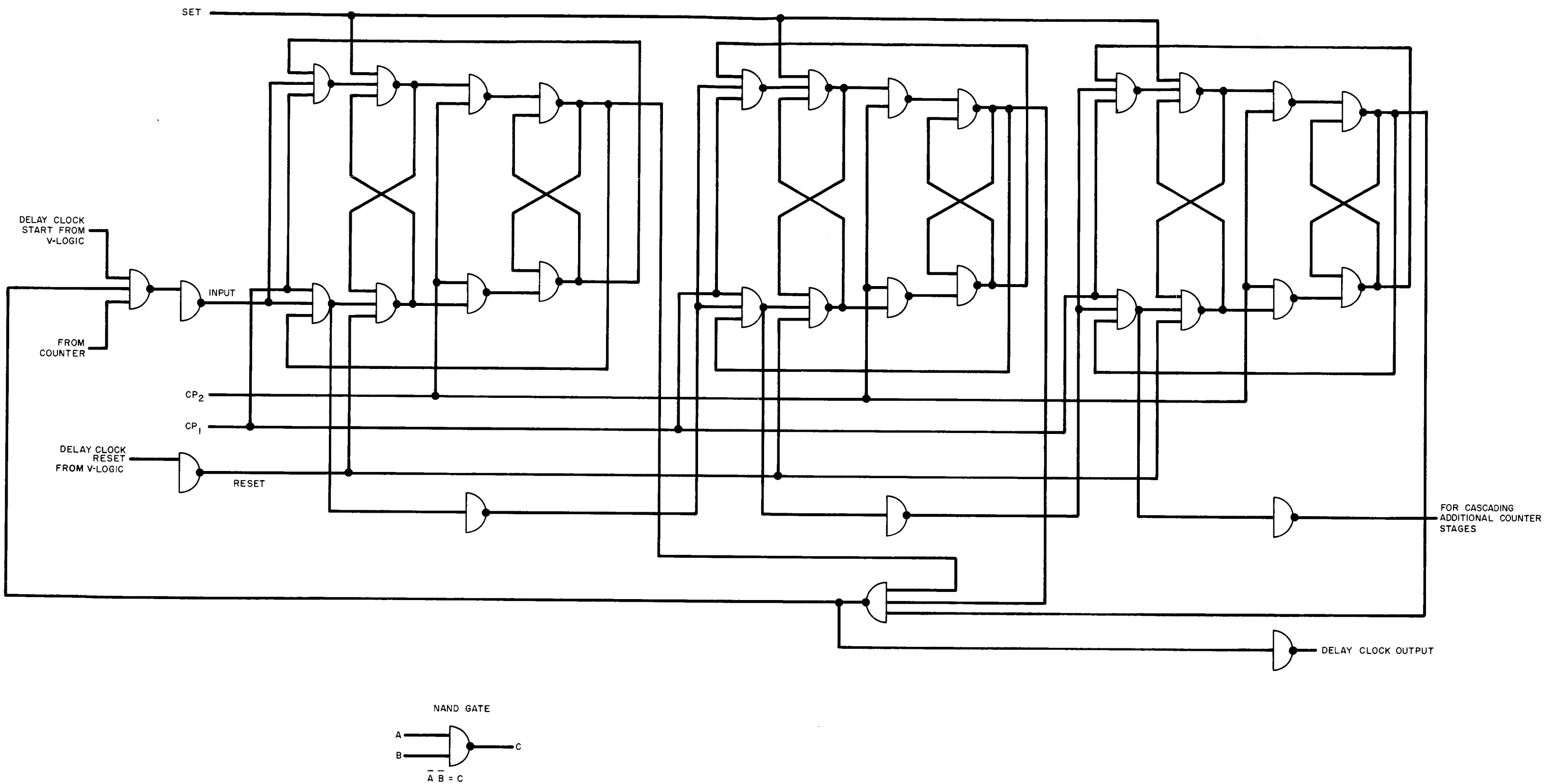


FIGURE 5-12
TIME DELAY CIRCUIT

E. PACKAGING REQUIREMENTS

There are three principle hostile environments which must be considered on the physical design of READI circuitry. They are:

- Shock and Vibration
- Ambient Pressure
- Temperature

Each of these are discussed in the following paragraphs.

1. Shock and Vibration

A dual approach to the shock and vibration isolation is necessary. Mechanical vibration from roughly 15 cps up can be effectively isolated through the use of resilient damping mountings, internal to the electronic unit housing, between the inside of the housing and the electronic assembly. Protection against very high acoustical fields, which are a particular problem in the first stage, is afforded by the use of a strong, relatively massive housing.

2. Ambient Pressure

It will be necessary to package the electronic chassis in a pressurized inert gas container in order to guard against the problems associated with near vacuum conditions. Those problems include electrical arcing, component bursting, explosion threat, and lack of connection cooling. A cylindrical container is recommended because of the ease with which it can be hermetically sealed.

3. Temperature

It does not appear that the temperature environment will be a major READI design problem. It will only be necessary to heat, prior to the firing of the engine, those portions of the system in proximity to the cryogenic propellant tanks. This may be accomplished by placing a heating jacket around the case. During flight, further temperature rises, due to engine burning, will remain within an acceptable range because of the large thermal lag of the case and the relatively short engine burning times. The potential temperature problem will be further alleviated as increased use of integrated microcircuits is made in the READI design.

This is because of the low power dissipation and relatively high temperature ratings of these elements.

As part of the Phase 1 investigation, a trade-off study was conducted to determine the optimum equipment configuration for a representative multi-stage vehicle. It was shown that a separate, self-contained system for each stage is preferable to a central system shared by each stage. (See Appendix B of the final report*.)

There are two basic approaches to the distribution of the equipment within each multi-engine stage. The first approach places all electronic circuits within a single package located on the aft compartment (above the heat shield, and close to an access port and the inter-stage cable tunnel). The second approach places the transducer signal conditioning circuits peculiar to each engine in individual packages for each engine. These units would be integrally assembled to the respective engine, with the resulting advantage that only a single flexible cable containing the output leads to a central stage package, would be required.

- - - - - - -

*Phase 1 Final Report, Sperry Report No. CA-4251-0160.

5-3. DEVELOPMENT OF EXPERIMENTAL SYSTEM

A. INTRODUCTION

The second prime objective of the equipment development program was to fabricate an experimental system suitable for test on a presently available rocket engine during the static test firing development phase. This task was undertaken for several reasons:

- To identify and solve the problems involved in the fabrication, installation and use of such equipment
- To make available equipment with which the functions and design integrity of READI may be tested experimently.

In order to carry out the task, it was first necessary to select an actual engine upon which to base the design. The H-1 engine was selected because of the rich history of developmental test data and analyses which are available and the availability of this engine for test programs.

This section describes the experimental READI system in detail, using the equipment organization outlined in paragraph 5-2.

B. MALFUNCTION DETECTION

The primary source of information for the compilation of detection techniques for the H-1 was data provided by MSFC on firings of the engine in which malfunctions occurred. This data was made available in the form of:

- Preliminary reports and summaries
- Analog oscillograph recordings
- Tabulated data.

The main objectives in the compilation of the malfunction detection techniques (V's) were

- To select V's which use a variety of transducer types and require a variety of processing techniques and logical operations
- To cover the malfunctions which are likely to occur in normal engine testing and those malfunctions which can be induced artificially in special tests

Additional consideration were:

- Availability of sensors and sensing locations on the H-1 engines scheduled for test during the first quarter of 1964
- Malfunction analyses previously performed by Rocketdyne and MSFC
- Availability of data to establish decision limits
- Test stand operational procedures.

The resulting detection techniques, V's, (signal space separations) have been arranged in a catalog, which is reproduced in Appendix E. Sample sheets from the catalog are shown in figure 5-13. The H-1 engine schematic is shown in figure 5-14. A key to the schematic and V catalog is given in table 5-3.

For each V, the following information is given:

- Input signal(s), such as chamber pressure
- Full range and critical range of signal. The critical range is the range in which a determination of engine condition is made
- Signal processing - for example, chamber pressure below a limit value
- Self-check limits, level and rate-of-change - for example, the maximum reasonable negative rate of chamber pressure is 8000 psi/sec
- Definition of V = 1, i.e., the Boolian statement which identifies the condition of the engine
- Engine malfunctions which cause the V to occur
- Corrective action(s) which can be taken to reduce risk.

A number of V's which indicate degradation-type failures have been broken down into two levels, one for shutdown, and one for shutdown after engine-out capability is achieved (see subsequent discussion of decision rules).

The following paragraphs will discuss the malfunctions and the detection techniques covered in the catalog and subsequent decision charts.

SIGNAL SPACE SEPARATION V 2.3.1

HIGH TURBINE SPEED OR ACCELERATION

Stage FIRST, & ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
NS	NS.3 > 35,000 RPM $\frac{dNS}{dt}$ > 50,000 RPM/SEC	—	—	NS 130,000 RPM/SEC	NS 200,000 RPM/SEC	0-40,000 RPM	18-40K RPM

Definition of V = 1

$(NS.3)(\frac{dNS}{dt})$

Malfunction(s) which cause V = 1

SEE V 2.2.1

Optimum Corrective Action

SHUTDOWN

Table B-1

FIGURE 5-13
SAMPLE PAGES FROM
DETECTION TECHNIQUES CATALOG

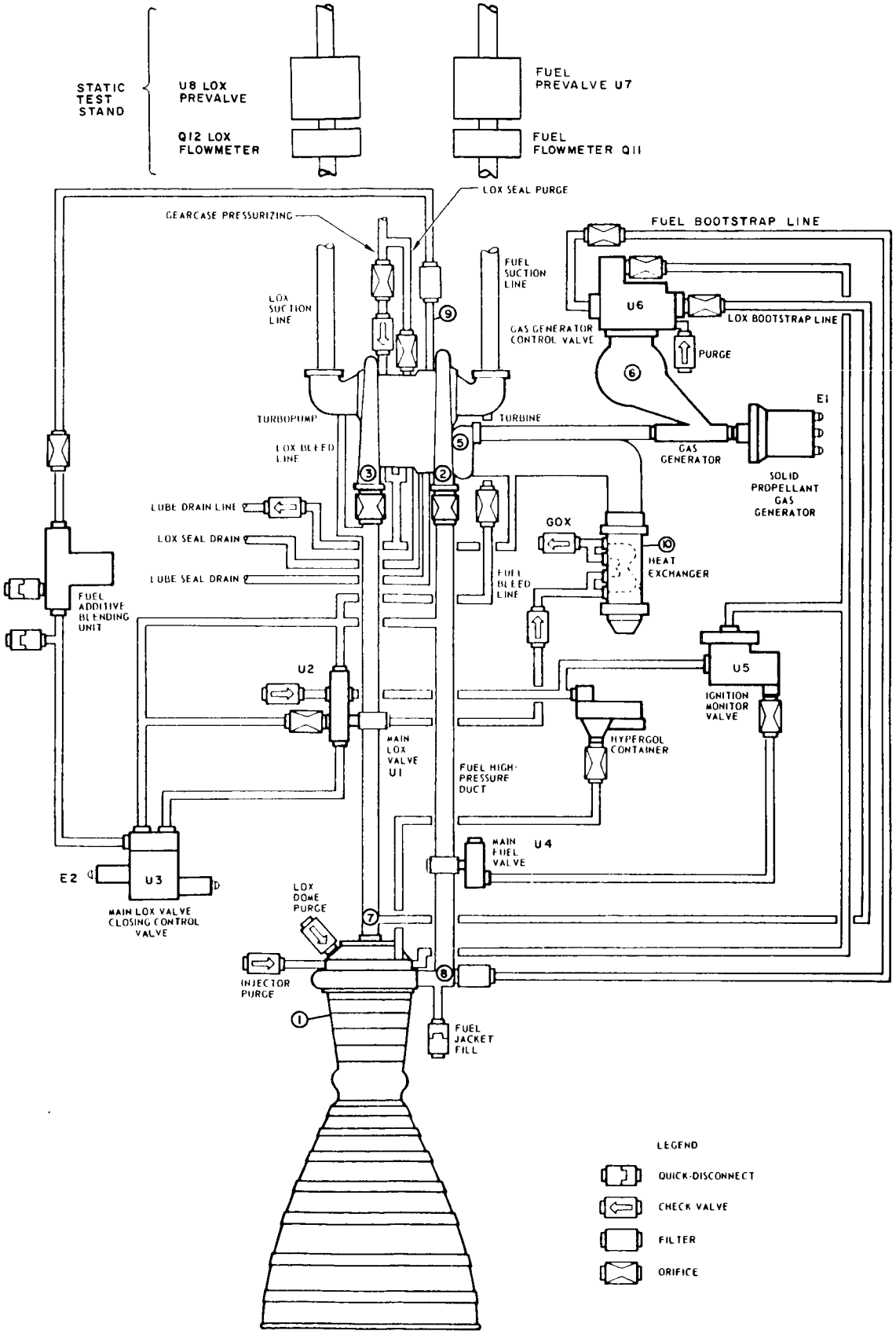


FIGURE 5-14
H-IA ENGINE SCHEMATIC DIAGRAM

Table 5-3

Key to Symbols Used in Subsequent Tables and Text

Signal Notation and Transducer Type	Engine Station Notation (Encircled Numbers in Figure 2-1)		Engine Component and Signal Designations	Time References	
	No.	Location		Notation	Time From
P Pressure	1	Main chamber	U1 Main lox valve	t1	E1 ($t_1 \approx$ burn time)
Q Volumetric flow	2	Fuel pump outlet	U2 Fuel igniter valve	t2	Chamber Vib. > 100g
T Temperature	3	Ox pump outlet	U3 MLV closing control valve	t3	E2
X Position	4	Gear case	U4 Main fuel valve	t4	T6 > 1300°F
N Rotary speed	5	Turbine	U5 Ignition monitor valve		
t Time	6	Gas generator	U6 Gas generator propellant valve		
A Vibration	7	Lox injector - inlet condition	U7 Fuel pre-valve		
F Fire detector	8	Fuel injector - inlet condition	U8 Ox pre-valve		
E Electrical control signal	9	Fabu inlet to turbo pump			
	10	Heat exchanger			
	11	Fuel suction line			
	12	Ox suction line			

Engine Command Signals

E1 start signal to SPGG (stored V, V21)

E2 stop signal to Conax valve (stored V, V22)

Lift-off Signal, E3

(Stored V, V23)

Engine-Out Capability

Alternate Mission V24

Prime Mission V25

Vehicle Attitude Stability Limit V26

(Note: V24, V25 and V26 are defined fully in their respective sheets in table 5-6.

Signal Space Separation, "V" Coding

V X.X.X

Decision Limit

Separation Equation

Characteristic Sensible Effect

1. V1 Malfunction Indicator

Combustion instability remains as one of the most severe problems in large liquid rocket engines. The signal processing used in the experimental READI system executes the rough combustion cut-off criterion used at MSFC in test stand operations.

Many other techniques, most of which involve various pressure measurements, are under consideration as part of combustion instability analyses of other large rocket engines. Particular emphasis has been placed on detection (and correction) on the incipient level. As long as shut down is the remedy, however, the corrective action is limited in speed by the closing rate of the main lox valve, and techniques which pick up instability a few cycles earlier are of little value.

2. V2.1 Malfunction Indicator

Turbine speed is a very sensitive indicator of engine condition. Many of the engine failures which finally result in loss of chamber pressure (P1) will first cause loss of, or low, speed (N5). Loss of P1 or N5 would call for engine shutdown, when the engine has fallen below the bootstrap level, to restrict damage and stop a possible overboard flow of propellant. This arrangement provides an example of information redundancy and avoids certain problems in providing self-check criteria.

3. V2.2 Malfunction Indicator

High turbine speed, as interpreted in V2.2, results from malfunctions in the bootstrap loop which cause excessive power delivery to the turbine. The shutdown decision is not implemented for V2.2 until the prime mission can be achieved with one engine shut down. The very high turbine speed limit is associated with severe malfunctions which can cause a turbopump explosion.

4. V3 Malfunction Indicator

The high gas generator temperature limit can be exceeded when a variety of malfunctions occur. These malfunctions include overlap in the liquid and solid generators and erosion of the lox injector in the liquid propelling gas generator. Engine shutdown would be called for under certain mission conditions to prevent severe turbine damage or gas generator rupture which could result in catastrophic engine loss. Another measurement, low gas generator temperature, can also be made from the same sensor. This

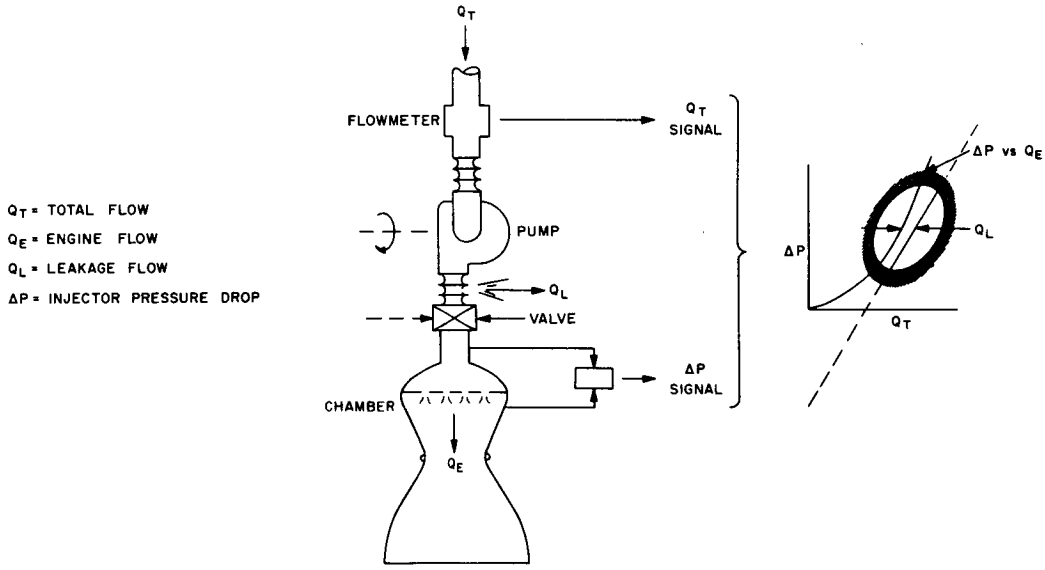
would be combined with other indicators, such as low turbine speed, used to separate failures in the start and run cycles which ultimately result in loss of thrust.

5. V5 Malfunction Indicator

A very dangerous situation can arise when the flow of fuel is cut off, even temporarily, and the lox flow continues. The engine can be destroyed before the loss of fuel pressure causes the main lox valve to close. There are at least eight independent engine and stage failures which can result in this condition.

6. V7 and V8 Malfunction Indicators

Large propellant leaks, about 10 percent of mainstage flow, present a fire and explosion hazard and can cause premature propellant depletion. A simple way of detecting such leaks is by comparing the stage (or test stand) flowmeter output with the drop across the injector. As noted in the sketch below, a straight line approximateion to the normal injector pressure drop curve in the normal operating range is utilized.



For the H-1, temperature corrections to account for density variations are probably unnecessary because of the narrow range of propellant temperatures encountered in tests. Detection of leaks much smaller than 5 percent of nominal flow is questionable because of the inexact nature of the measurement, and the stringent accuracy requirements which must be placed on the sensors and processing circuits.

Note that in the detailed processing requirements given in Appendix E that two delays, t1.1 and t3.1, are employed. The delay, t1.1> 1.0 second, is to insure that the engine is near the normal operating point before a determination is made. The delay t3.1 1.0 second, requires that the condition (i.e. leak) exists for one second before a determination is made. This nearly eliminates the false alarms which can be caused by turbine meter cavitation. Prolonged cavitation of the turbine meter, beyond approximately one second, will cause pump cavitation, with an attendent overspeed transient. Therefore, the complement of high turbine speed (V2.2.1, turbine speed not high) is included in the processing equation.

7. V9 and V11 Malfunction Indicators

Measurement of turbopump vibration and lube-additive system pressure fall into a family of indicators with measurements of bearing temperature which are indicative of insipient turbopump mechanical failure. The initiating malfunction can have a variety of origins. The value of such measurements is that they alert the READI system to shut down the engine, if the mission phase is suitable, and reduce the chance of catastrophic turbopump failure.

The two limits on turbopump vibration, V9, recognize the proportional nature of malfunctions which cause high vibration, and permit the shutdown decision to be made selectively depending on mission phase. The complement of combustion instability (V1.1.1) is included in the processing equation for V9, since a different decision is required for V1.1.1 than for V9; also, it is quite possible for combustion instability vibration to trigger the V9 limit, because of the physical proximity of the main chamber and the turbopump.

8. V13 Malfunction Indicator

Indication of a violent explosion, particularly above the heat shield, can be used for abort sensing. This indication is in a class with indicators of complete loss of propellant pressure and high vehicle attitude rates, which call for immediate abort. The processing used for V13 measures the rate of rise of ambient pressure as an indication of explosion.

9. V14 Malfunction Indicator

Two different effects, which cover different failure modes of the heat exchangers, are indicated in the V14 processing. The heat exchanger can fail through internal burn-out, in which case lox will bleed into the

heat exchanger cusing a great rise in heat exchanger exit temperature (T10) and rapid disintegration of the whole assembly. Alternately, or as a result of the lox leak, the exterior of the assembly can burn out. When this burnout condition is quite serious (i.e., large burned-out area near turbine flange), the exit temperature, T10, will decrease slightly and the back pressure on the turbine, P5, will fall below normal.

10. V15 Malfunction Indicator

Malfunctions in the lube drain system can cause a rise in gear-case pressure which will, at a sufficiently high level, cause the explosion of the gear case.

C. SELF-CHECK AND REDUNDANCY PROVISIONS

The use of self-check and redundancy in a READI system would normally evolve from the optimization step in designing the system. In the experimental system the objective was to illustrate these special techniques as they might appear in an operational system. Analyses have clearly shown that the greatest penalty traceable to READI equipment failures results from false alarms; therefore, the use of redundancy and self-check methods was generally directed toward the reduction of false alarms.

1. Self-Check Applications

Most of the self-check channels incorporated in the experiment READI are based on limits of rate-of-change of a variable. In all, eight different self-check examples are included. These are summarized in Appendix E.

2. Transducer Redundancy

Transducer and analog signal processing circuit redundancy was used in the following three channels of the system:

1. Chamber vibration (A1) - two transducers with OR logic (because the false alarm probability of the transducer used is very low and missed alarms are disasterous)
2. Lube manifold pressure (P9) - two transducers with AND Logic (because no suitable self-check method is available to control false alarms)
3. Turbine exhaust pressure (P5) - two transducers with AND logic (used for the same reason as for channel 2 above).

3. Information Redundancy

Two examples of information redundancy are explicitly noted in the catalog of V's (Appendix E). These are:

1. Low turbine speed (N5) and low main chamber pressure (Pc).
2. Loss of turbine speed (N5) and low chamber pressure (Pc).

D. DECISION RULES

Decision rules are an indication of the required actions or combination of actions that should be taken to reduce risk when a malfunction takes place. Listed below are the remedial actions used in making up decision rules for the experimental READI.

ao No action

a1 Normal shutdown, subject engine (open main lox valve, close control valve and conax valve)

a2 Prepare for fast shut down of subject engine (bypass main lox valve closing rate restriction)

a3 Close pre-valves, subject engine (de-energize pilot stages of lox and fuel pre-valves)

a4 Normal shutdown, all engines

a5 Initiate abort sequence

These actions are combined to make the following decisions:

Decision	Action
do - No decision	a0
d1 - Normal shutdown	a1 and a3
d2 - Fast shutdown	a1, a2, and a3
d3 - Pre-valve shutdown	a3
d4 - Shut down all engines	a4
d5 - Abort	a4 and a5

Normal shutdown is accomplished by simultaneously activating the main lox valve, MLV, closing the control valve and deactivating the pilot stages of the pre-valves. The MLV closes faster than the lox pre-valve so the engine shutdown rate is controlled by the MLV.

Fast shut down is accomplished by bypassing the restriction which controls the closure rate of the MLV. This decision is used for malfunctions such as combustion instability and turbine runaway where the normal 300 millisecond MLV closing time is too slow. This is an example of a corrective action which, by itself, degrades engine reliability, but is a justified action once an engine malfunction has occurred (see figure 3-7). This is the only corrective action programmed in the experimental system which implies any modification to the engine or stage.

The H-1 engine can be safely shut down with the stage pre-valves. This is an attractive alternate shutdown mode for malfunctions involving large propellant leaks between the pre-valves and main engine propellant valaves. Normal shutdown results in the lines between these valves being full of propellant which will continue to escape after normal shut down if a leak exists. Since the amount of entrapped propellent is considerable in a large launch vehicle, the leak hazard (fire, damage to other engines, explosion) is not reduced to the fullest extent by normal shutdown. Shutdown via the pre-valves in contrast, results in rapid exhaustion of the plumbing system downstream of the pre-valves.

1. Decision Priority

When a severe engine malfunction takes place it is possible for the cause and effect relationships which are used to compile malfunction detection techniques to deviate from the predicted pattern. Before a decision is implemented, several indicators (V's) calling for different decisions may appear. To cope with this situation, a decision priority circuit is incorporated in the system. This circuit accepts any or all indicated decisions and gates out the most appropriate one, based on a stored priority list. The priority list for the experimental system is as follows:

d5 Abort

d4 Shut down all engines

d2 Fast shutdown

d1 Normal shutdown

d3 Pre-valve shutdown

2. Decision Rule Chart

Malfunction detection techniques often include "gating" terms (refer to Appendix E), which may be related directly to the malfunction, as

in t_2, or may be related to the engine start signal. An extension of this gating concept is the incorporation of mission phases in the decision rules. The decision, d, is then expressible in terms of the malfunction detection technique, V, and the phase, p. The boundaries of mission phases are points where, within the limitations of available corrective actions, decisions based on some V should be changed to obtain a greater risk reduction. These phases take into consideration such things as whether lift-off has occurred, whether an engine can be shut down and still make the prime mission, etc. The phases programmed are:

- Engine start to lift-off
- Lift-off to attainment of alternate mission engine-out capability, EOC
- Alternate engine-out capability to prime mission engine-out capability
- Stage cut-off.

3. Mission Phase Considerations

It is assumed that a ground complex monitors the vehicle up to engine ignition. Before lift-off many malfunctions call for shut down of all engines since it is pointless to risk a launch unless all subsystems are near normal. Immediately after launch, obviously, the situation is quite different; only very severe malfunctions call for engine shutdown since this is tantamount to abort.

4. Stage Thrust Degradation Limits

At some time during the operation of almost any multiengine stage, it is possible to shut down an engine and make the required stage velocity increment by burning the residual propellants in the operating engines. For an eight-engine first stage with adaptive guidance in subsequent stages, it is quite reasonable to assume that single engine-out capability is achieved some time during stage burning. At a later time, probably near normal cut-off, dual engine-out capability is achieved. Similarly, an engine-out capability may be computed for alternate missions. For simplicity in setting up the programmed decisions in table 5-4, the required velocity increment for all alternate missions has been assumed to be the same. This velocity increment, however, is less than that required for the prime mission.

Multiengine failures must also be considered. The likelihood of a single failure is much greater than for multiple engine failures, but, as can be seen in table 5-5, the multiengine failure situation cannot be disregarded completely. For a single engine reliability of 0.98, the probability of having more than one failure in an eight-engine cluster is over one percent.

Table 5-4

H-I Ready Programmed Decisions for 8-Engine Cluster

V	CHARACTERISTIC SENSIBLE EFFECT	PROGRAMMED DECISION BY MISSION PHASE						MAX PROCESS TIME (M SEC)	MAX ALLOWABLE ERROR IN V (±%) (SEE NOTE 1)
		START ACCEL. TO LIFT-OFF VA	MAINSTAGE				STAGE CUTOFF VF		
			NO ALT. MISSION VB	ALT. MISSION VC	PRIME MISSION VD	LOSS OF ATTITUDE CONTROL VE			
1.1.1	MAIN CHAMBER ROUGH COMBUSTION	(D2)(D4)	(D2)(D5)	D2	D2	(D2)(D5)	D2	20	10
2.1.1	LOW TURBINE SPEED AND LOW MAIN CHAMBER PRESSURE	D0	D0	D0	D1	D0	D1	500	10
2.1.2	LOSS OF TURBINE SPEED AND LOW MAIN CHAMBER PRESSURE	D4	D5	D1	D1	D5	D1	500	10
2.2.1	HIGH TURBINE SPEED	D0	D0	D0	D1	D0	D1	50	5
2.2.2	VERY HIGH TURBINE SPEED	(D2)(D4)	(D2)(D5)	D2	D2	(D2)(D5)	D2	20	5
3.1.1	HIGH GG TEMPERATURE	D0	D0	D0	D1	D0	D1	200	5
3.1.2	VERY HIGH GG TEMPERATURE	D4	D0	D1	D1	D5	D1	200	5
5.1.1	LOSS OF FUEL FLOW WITHOUT LOSS OF OX FLOW	D4	D5	D1	D1	D5	D1	200	10
7.1.1	3% FLOW DISCREPANCY, LOX FLOWMETER TO INJECTOR	D0	D0	D0	D3	D0	D3	1000	3
7.1.2	10% FLOW DISCREPANCY, LOX FLOWMETER TO INJECTOR	(D3)(D4)	D0	D3	D3	D0	D3	1000	3
8.1.1	3% FLOW DISCREPANCY, FUEL FLOWMETER TO INJECTOR	D0	D0	D0	D3	D0	D3	1000	3
8.1.2	10% FLOW DISCREPANCY, FUEL FLOWMETER TO INJECTOR	(D3)(D4)	D0	D3	D3	D0	D3	1000	3
9.1.1	HIGH TURBOPUMP VIBRATION	D0	D0	D0	D1	D0	D1	100	10
9.1.2	VERY HIGH TURBOPUMP VIBRATION	D4	D0	D1	D1	D0	D1	100	10
11.1.1	LOSS OF LUBE PRESSURE	D4	D0	D0	D1	D0	D1	2000	10
13.1.1	EXPLOSION, ENGINE AREA	D5	D5	D5	D5	D5	D5	20	15
14.1.1	HEAT EXCHANGER FAILURE	D4	D0	D1	D1	D0	D1	500	10
15.1.1	HIGH GEARCASE PRESSURE	D4	D0	D1	D1	D0	D1	50	10

DECISION LIMIT
SEPARATION EQUATION
CHARACTERISTIC SENSIBLE EFFECT

DECISIONS	STORED V'S
D0 NO ACTION	V21 START ALL ENGINES
D1 NORMAL SHUTDOWN OF SUBJECT ENGINE	V22 STOP ALL ENGINES
D2 FAST SHUTDOWN OF SUBJECT ENGINE	V23 LIFT OFF
D3 PREVALVE SHUTDOWN OF SUBJECT ENGINE	V24 ALTERNATE MISSION ACHIEVABLE IF SUBJECT ENGINE IS SHUT DOWN
D4 SHUT DOWN ALL ENGINES, HOLD ON PAD. NO ABORT OF CAPSULE	V25 PRIME MISSION ACHIEVABLE IF SUBJECT ENGINE IS SHUT DOWN
D5 SHUT DOWN ALL ENGINES. SIGNAL ABORT OF CAPSULE	V26 VEHICLE ATTITUDE CONTROL WILL BE LOST IF SUBJECT ENGINE IS SHUT DOWN

MISSION PHASE LOGIC (NON-MINIMUM)

$$VA = (V21)(\overline{V22})(\overline{V23})(\overline{V24})(\overline{V25})(\overline{V26})$$

$$VB = (V21)(\overline{V22})(V23)(\overline{V24})(\overline{V25})(\overline{V26})$$

$$VC = (V21)(V22)(V23)(V24)(V25)(V26)$$

$$VD = (V21)(\overline{V22})(V23)(V24)(V25)(\overline{V26})$$

$$VE = (V21)(\overline{V22})(V23)(V24 + \overline{V24})(V25 + \overline{V25})(V26)$$

$$VF = (V21)(V22)(V23)(V24 + \overline{V24})(V25 + \overline{V25})(V26 + \overline{V26})$$

NOTE 1: THE ALLOWABLE ERROR IN V IS A ROUGH INDICATION OF HOW ACCURATELY THE SIGNAL SPACE SEPARATIONS MUST BE IMPLEMENTED AT THE DECISION LEVEL. THIS ERROR MUST BE DISTRIBUTED OVER TRANSDUCERS AND PROCESSING CIRCUIT.

Table 5-5

Multiengine Failure Probabilities

	Single Engine R	
	0.990000	0.980000
1 Probability that no engine fails	0.922745	0.850763
2 Probability that one, and only one, engine fails	0.074565	0.138900
3 Probability that more than one engine fails	0.002690	0.010337

Conditions
- 8-engine cluster
- Reliability of single engine is R
- All engines identical
- Probability of failure of any engine is independent of the state of other engines.

In addition to attainment of the stage velocity increment, it is necessary to insure that if the subject engine is shut down, the vehicle can maintain attitude control. For example, consider an eight-engine cluster similar to Saturn I where four engines are fixed and tightly clusted in the center while the four remaining outboard engines are gimballed. For such a vehicle, a suitable criteria may be to abort whenever two outboard (gimballed) engines must be shut down or loose thrust. Such a limit criterion is included in the experimental system.

E. CIRCUITRY

Figure 5-15 shows the block diagram of the experimental READI system for the H-1 engine. The signal conditioning circuits for the selected group of malfunction detection techniques utilize the standard functional building blocks to process the transducer output signals into a common range of d-c voltages. The list of transducer input signals and standard functional building blocks also appear in figure 5-15. These conditioned transducer signals are processed by the comparator circuits, which convert the analog level of the conditioned signal into a binary state at a predetermined voltage threshold. The comparator output states are then operated on by the V logic in accordance with the requirements of the particular malfunction

detection techniques. The decision logic circuit accepts the output signals from the V logic and, in combination with mission phase signals, decision priority, and blanking requirements, produces the desired decision outputs.

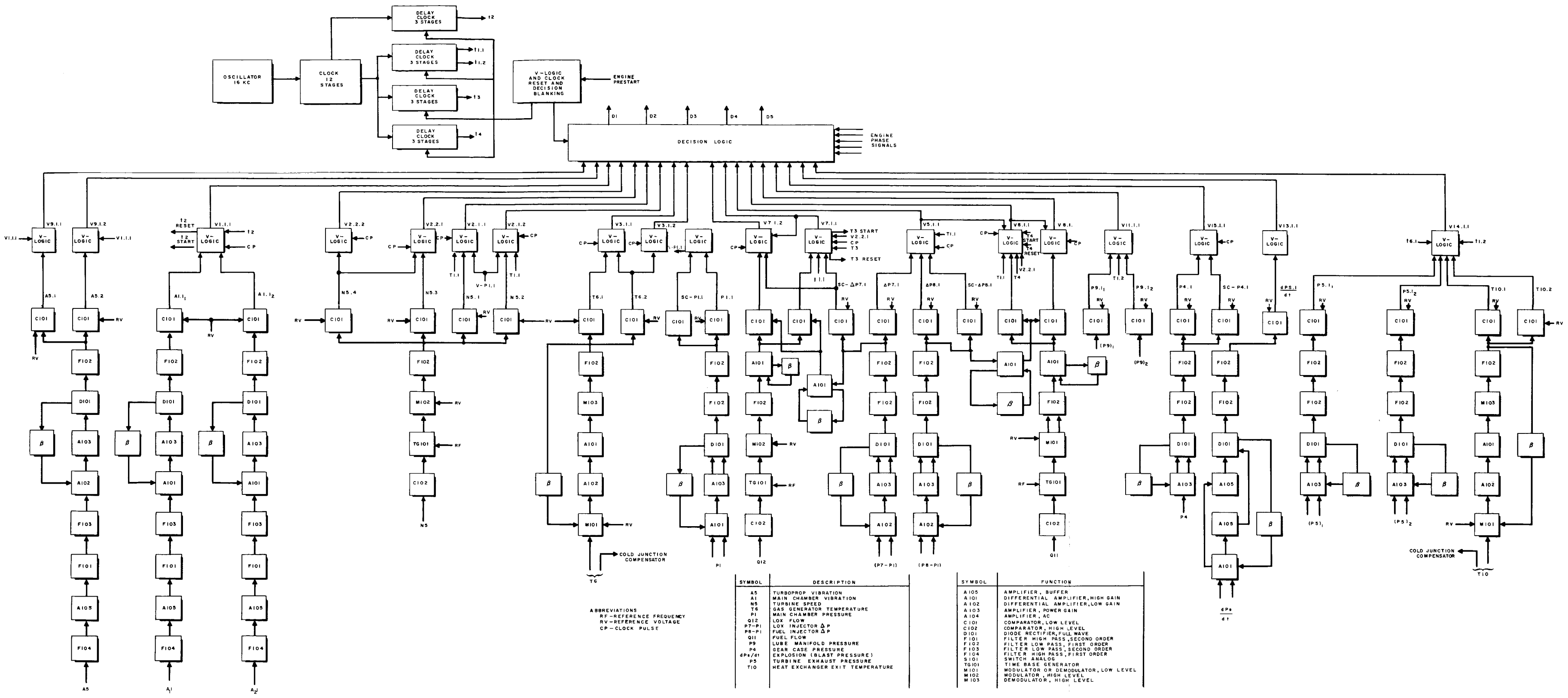
Figure 5-15 also illustrates additional circuits required by READI. These include the central clock consisting of twelve binary counter stages. The central clock provides all the timing pulses required by the processing circuits. Also shown are the various time delays required by the V logic. These are:

Time Delay Output	Delay Time
t1.1	1.0 second after engine start
t1.2	1.5 seconds after engine start
t2	100 milliseconds after main chamber vibration exceeds 100 g rms
t3	1.0 second after initial LOX flow discrepancy occurs
t4	1.0 second after initial fuel flow discrepancy occurs.

To insure that no premature decisions will occur, the pre-launch condition signal is used to blank all decisions from READI. This same blanking signal is used to reset the V logic and the time delay circuits prior to engine start.

This section of the report is devoted to the specific processing circuits developed for the H-1 engine; however, with slight modifications they may be applied to any engine. The signal conditioning circuits are illustrated in detail, with test results, in figures 5-16 through 5-28.

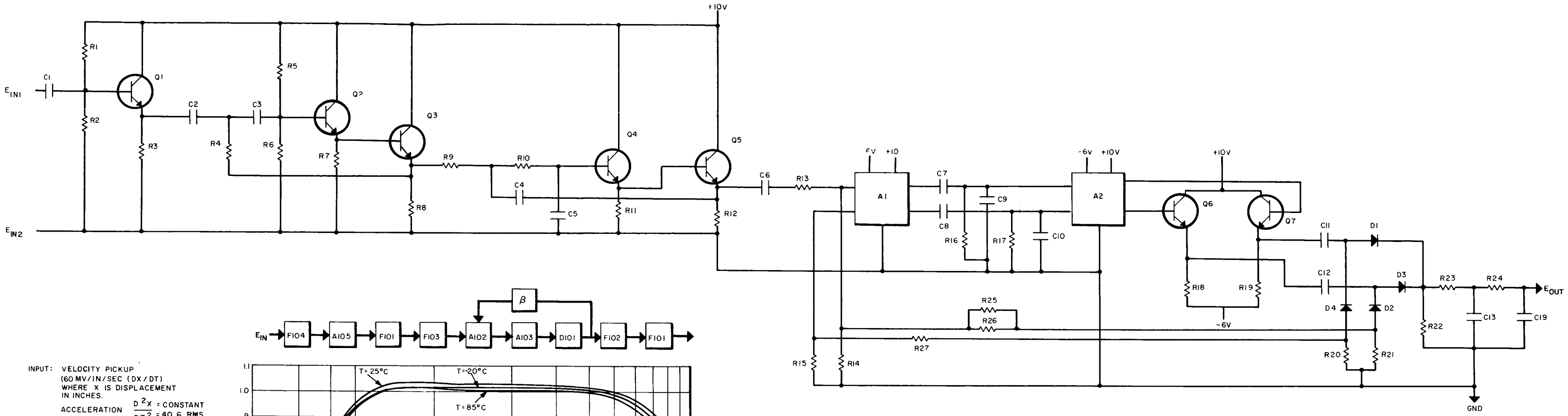
The low level comparator, C101, is illustrated with test results in figure 5-29. The logic circuits are illustrated in figure 5-30. In some instances (V logic, clock, and time delay) the circuits and test results are deleted in this section since their general functional description is adequate and appears in paragraph 5-2. The decision logic circuit is illustrated with the Boolian expressions required for the H-1 engine in accordance with the engine malfunction and mission phase (table 5-4). The decision logic outputs are also modified by the decision priority requirement as specified in paragraph 5-3D. The blanking of decision outputs is used during pre-start to prevent erroneous decision outputs.



SYMBOL	DESCRIPTION
A5	TURBOPROP VIBRATION
A1	MAIN CHAMBER VIBRATION
N5	TURBINE SPEED
T6	GAS GENERATOR TEMPERATURE
P1	MAIN CHAMBER PRESSURE
Q12	LOX FLOW
P7-P1	LOX INJECTOR ΔP
P8-P1	FUEL INJECTOR ΔP
Q11	FUEL FLOW
P9	LUBE MANIFOLD PRESSURE
P4	GEAR CASE PRESSURE
dPe/dt	EXPLOSION (BLAST PRESSURE)
P5	TURBINE EXHAUST PRESSURE
T10	HEAT EXCHANGER EXIT TEMPERATURE

SYMBOL	FUNCTION
A105	AMPLIFIER, BUFFER
A101	DIFFERENTIAL AMPLIFIER, HIGH GAIN
A102	DIFFERENTIAL AMPLIFIER, LOW GAIN
A103	AMPLIFIER, POWER GAIN
A104	AMPLIFIER, AC
C101	COMPARATOR, LOW LEVEL
C102	COMPARATOR, HIGH LEVEL
D101	DIODE RECTIFIER, FULL WAVE
F101	FILTER HIGH PASS, SECOND ORDER
F102	FILTER LOW PASS, FIRST ORDER
F103	FILTER LOW PASS, SECOND ORDER
F104	FILTER HIGH PASS, FIRST ORDER
S101	SWITCH ANALOG
TG101	TIME BASE GENERATOR
M101	MODULATOR OR DEMODULATOR, LOW LEVEL
M102	MODULATOR, HIGH LEVEL
M103	DEMODULATOR, HIGH LEVEL

FIGURE 5-15
SIGNAL PROCESSING DIAGRAM
FOR H-I ROCKET ENGINE



INPUT: VELOCITY PICKUP
(60 MV/IN/SEC (DX/DT)
WHERE X IS DISPLACEMENT
IN INCHES.

ACCELERATION $\frac{D^2X}{DT^2}$ = CONSTANT = 40 G RMS

PROCESSING: IV DC = 40 G RMS
RIPPLE < 50 MV P-P

PROCESSING TIME
REQUIRED = 100 MS
ACTUAL = 40 MS

BANDPASS: 66CPS TO 525CPS

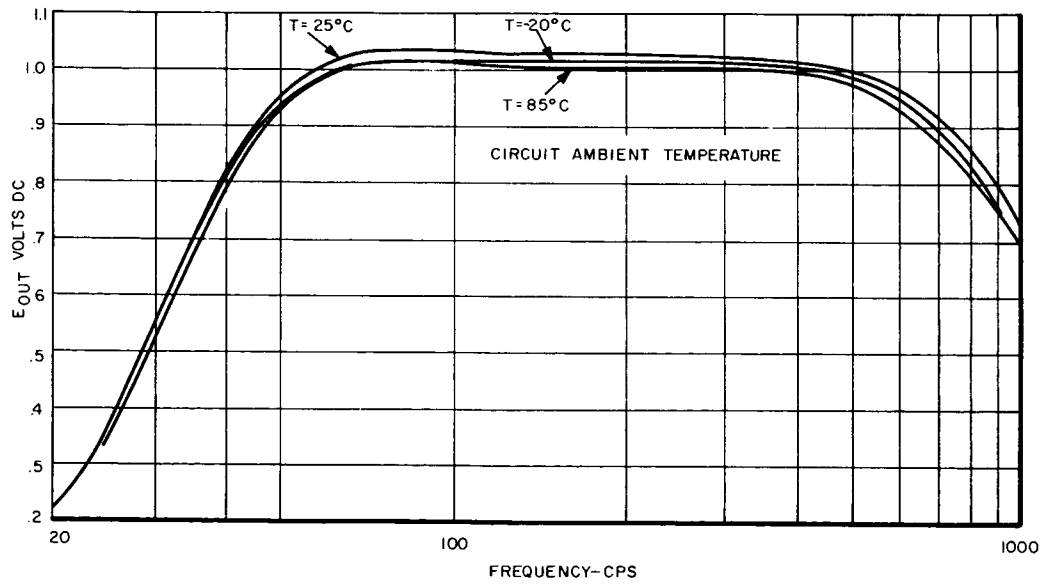
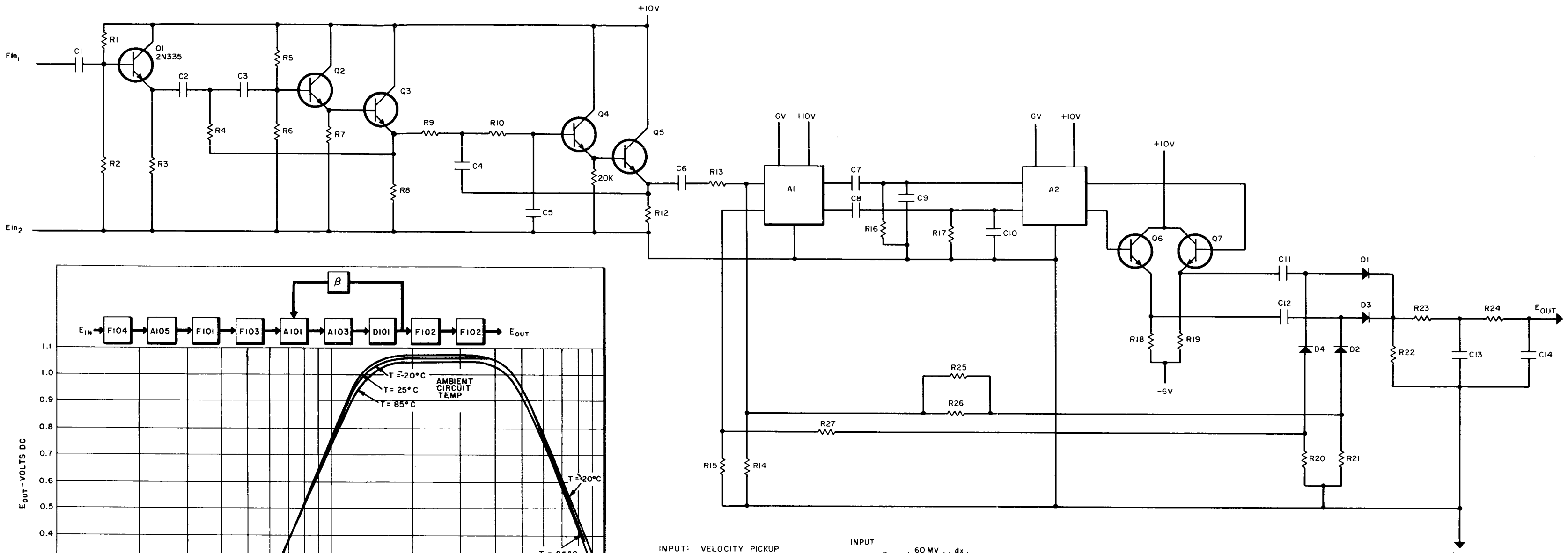
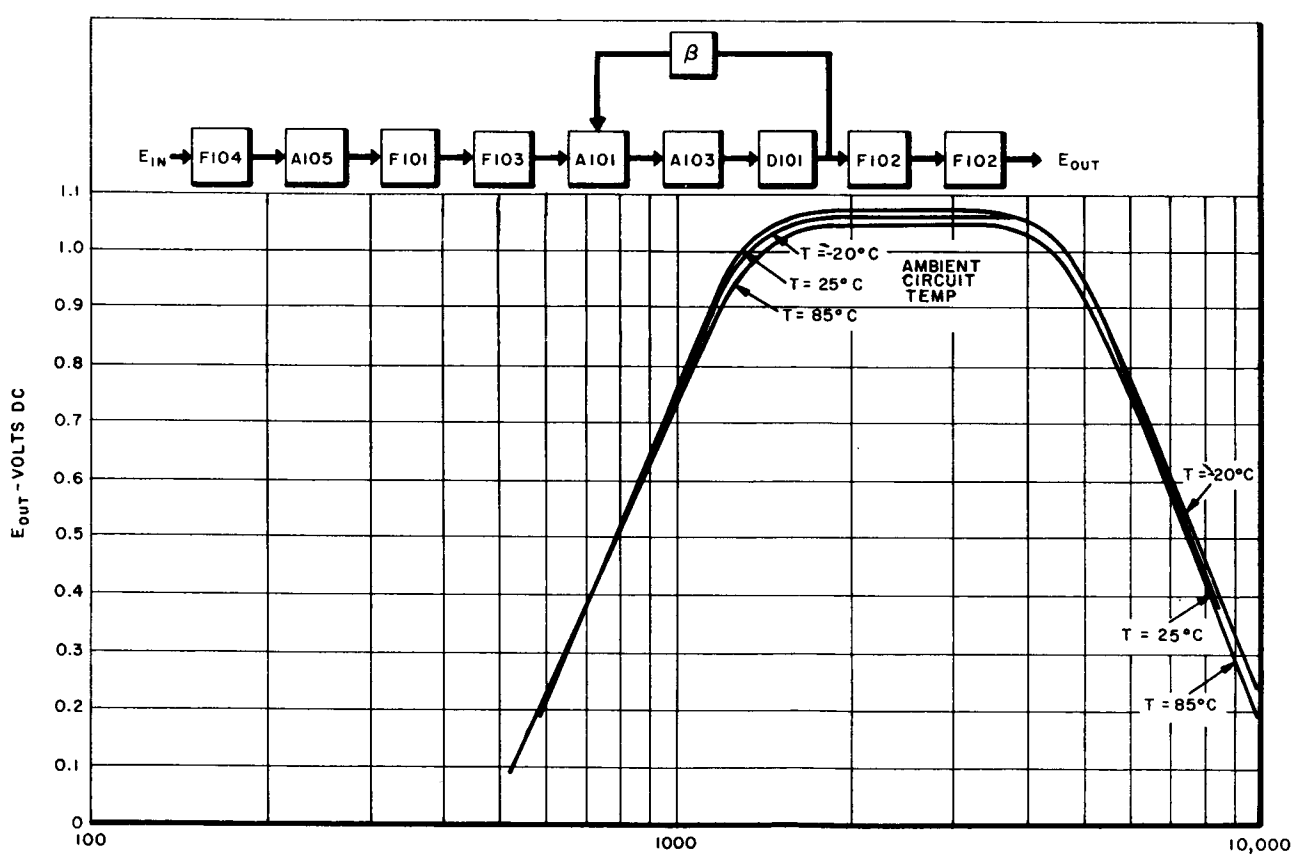


FIGURE 5-16
TURBOPUMP SIGNAL PROCESSING CIRCUIT, A5 (V9.1)





INPUT: VELOCITY PICKUP
60MV/IN/SEC

PROCESSING: 1VDC = 100 GRMS
RIPPLE = 20 MV P-P
PROCESSING TIME
REQUIRED 20MS
ACTUAL 6.5 MS
BANDPASS 960 CPS TO 6000 CPS

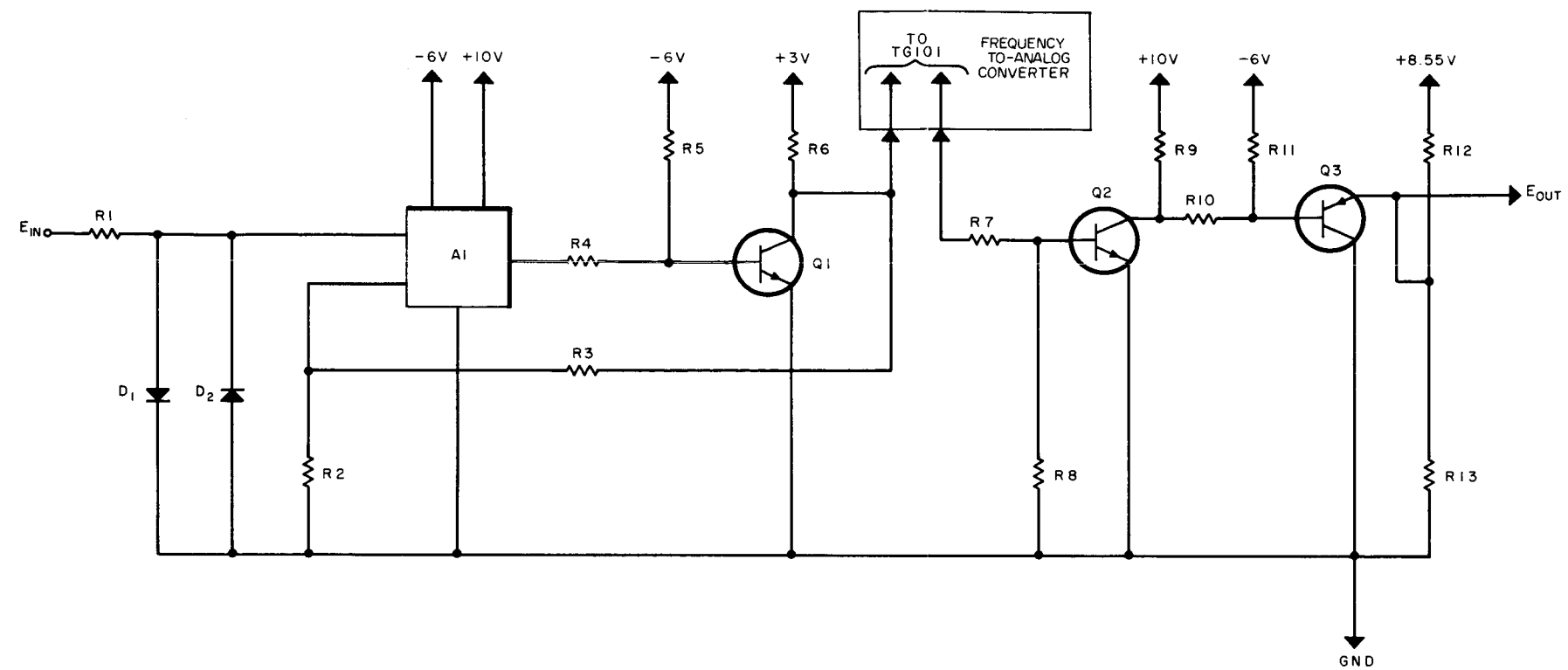
INPUT

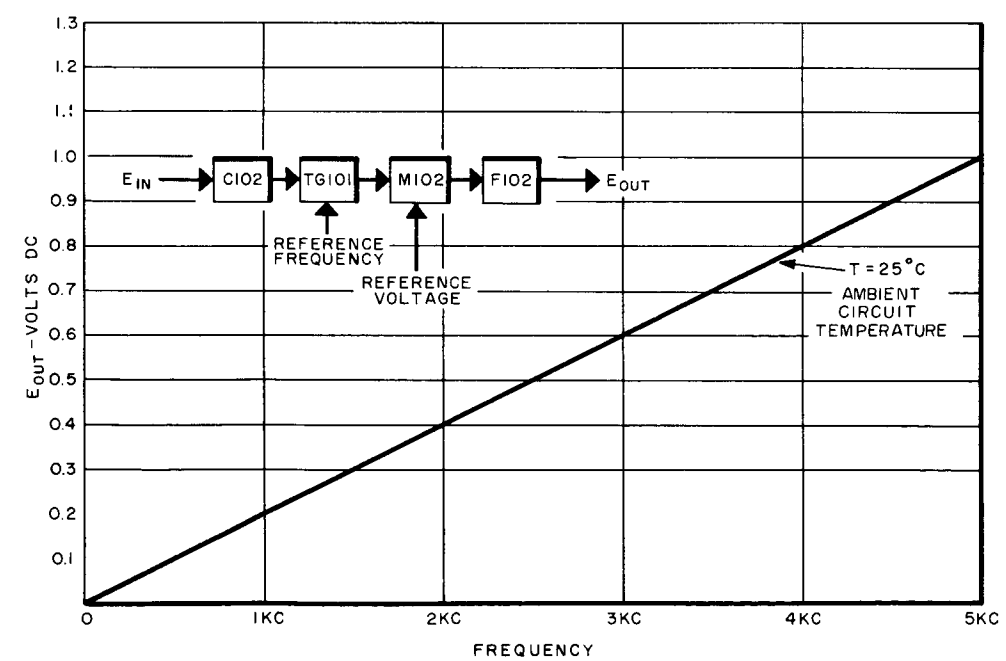
$$E_{in} = \left(\frac{60\,MV}{IN/SEC}\right)\left(\frac{dx}{dt}\right)$$

WHERE X IS THE DISPLACEMENT IN INCHES

ACCELERATION, $\left(\frac{d^2x}{dt^2}\right)$ = CONSTANT = 100 GRMS

FIGURE 5-17
MAIN CHAMBER
VIBRATION SIGNAL PROCESSING CIRCUIT





INPUT: PULSE PICKUP
E_{IN} = 1 CPS/10 RPM

PROCESSING:

1.0 V DC = 50,000 RPM RIPPLE<50MV P-P
PROCESSING TIME
REQUIRED<50MS
ACTUAL<20MS

FIGURE 5-18
TURBINE SPEED SIGNAL
PROCESSING CIRCUIT
N5(V2.1, V2.2)

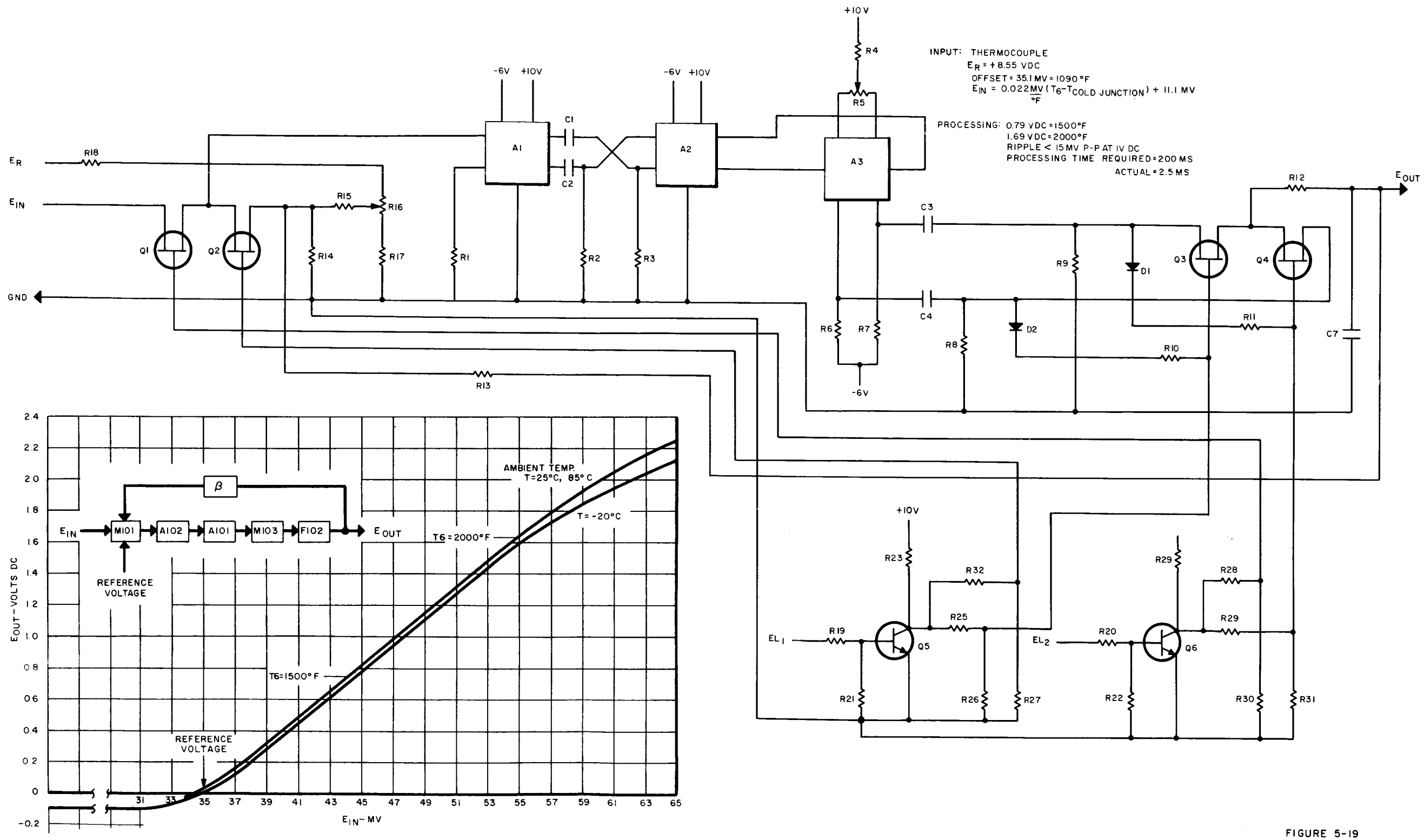
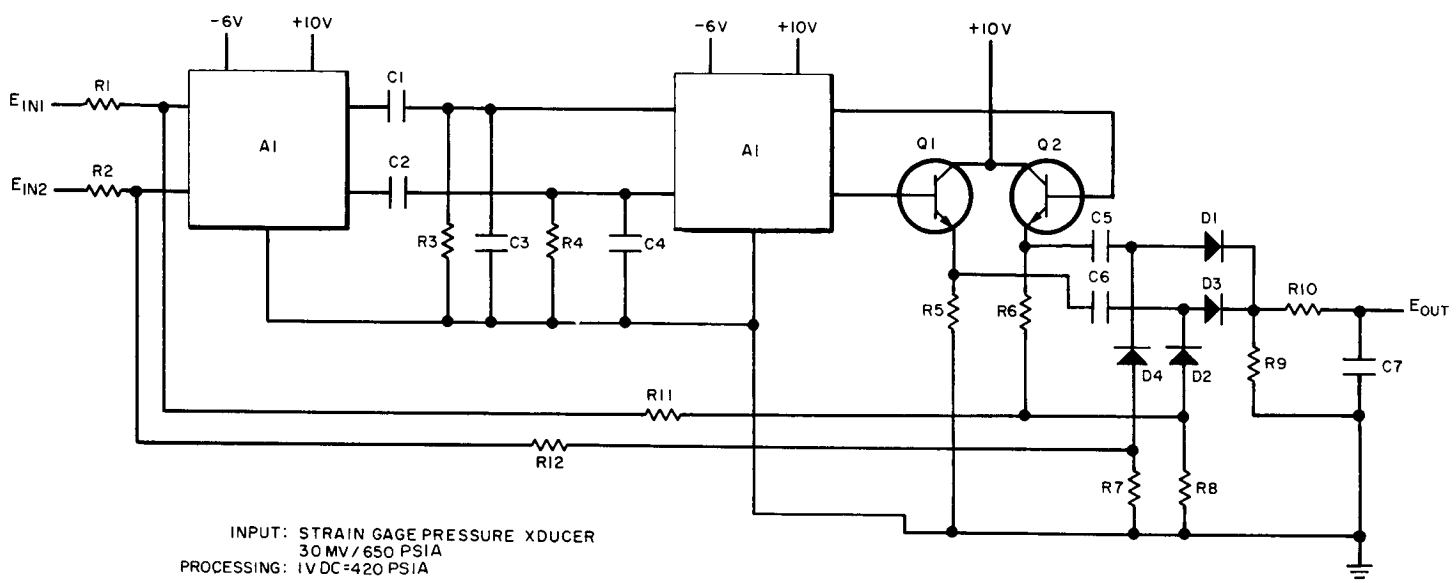


FIGURE 5-19
GAS GENERATOR THERMOCOUPLE SIGNAL PROCESSING CIRCUIT, T6 (V3.1, V14.1.1)



INPUT: STRAIN GAGE PRESSURE XDUCER
30 MV / 650 PSIA
PROCESSING: 1 V DC = 420 PSIA
RIPPLE < 20 MV P-P
PROCESSING TIME
REQUIRED = 500 MS
ACTUAL = 8.75 MS

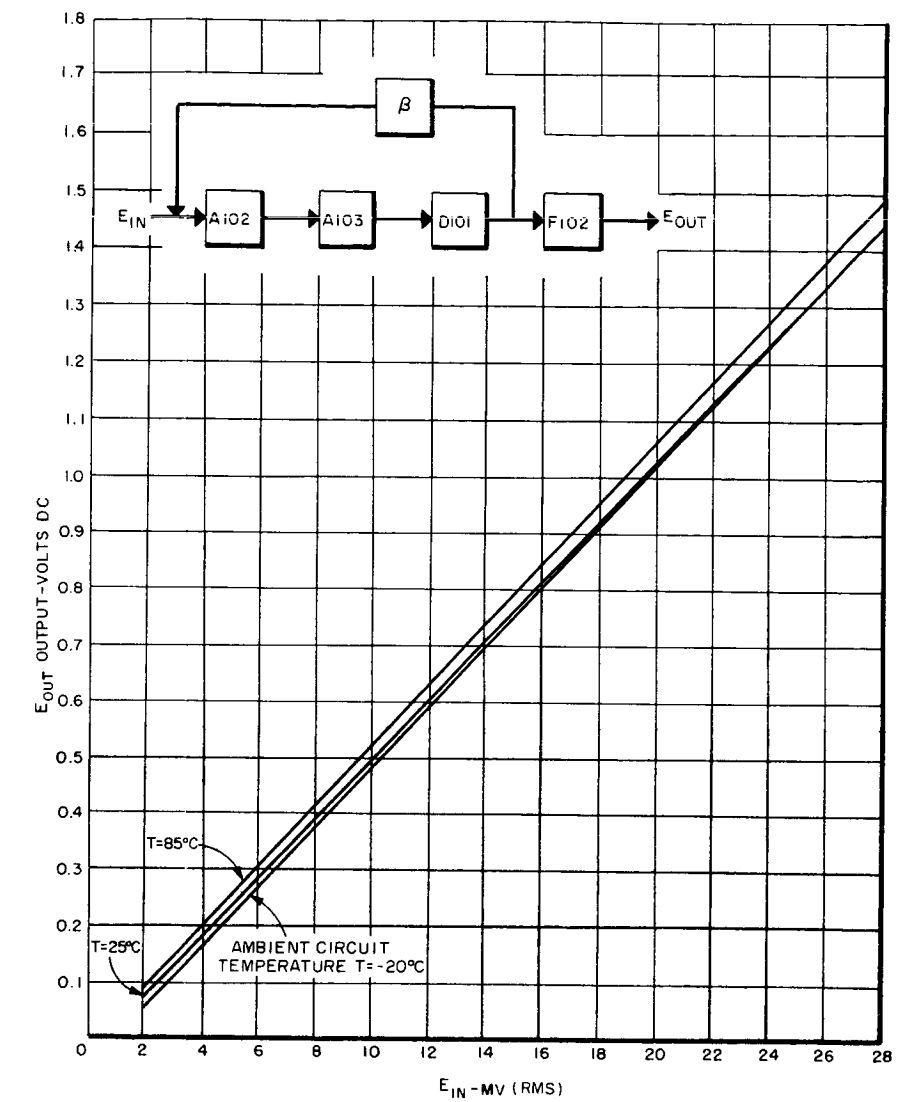
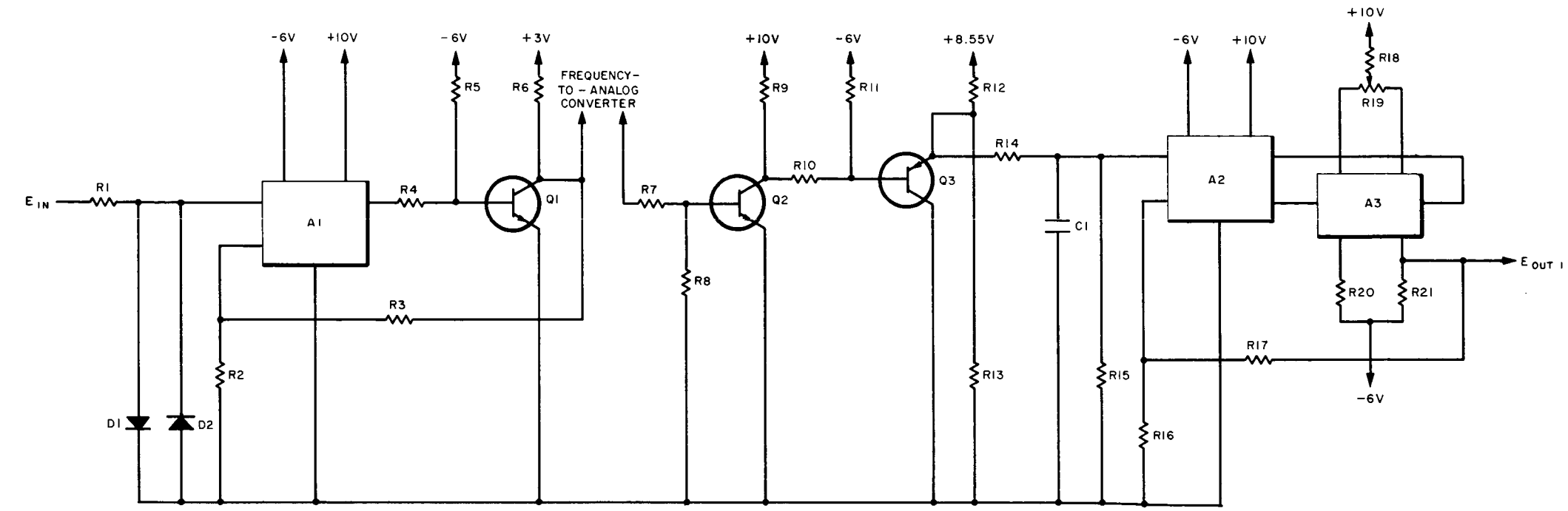
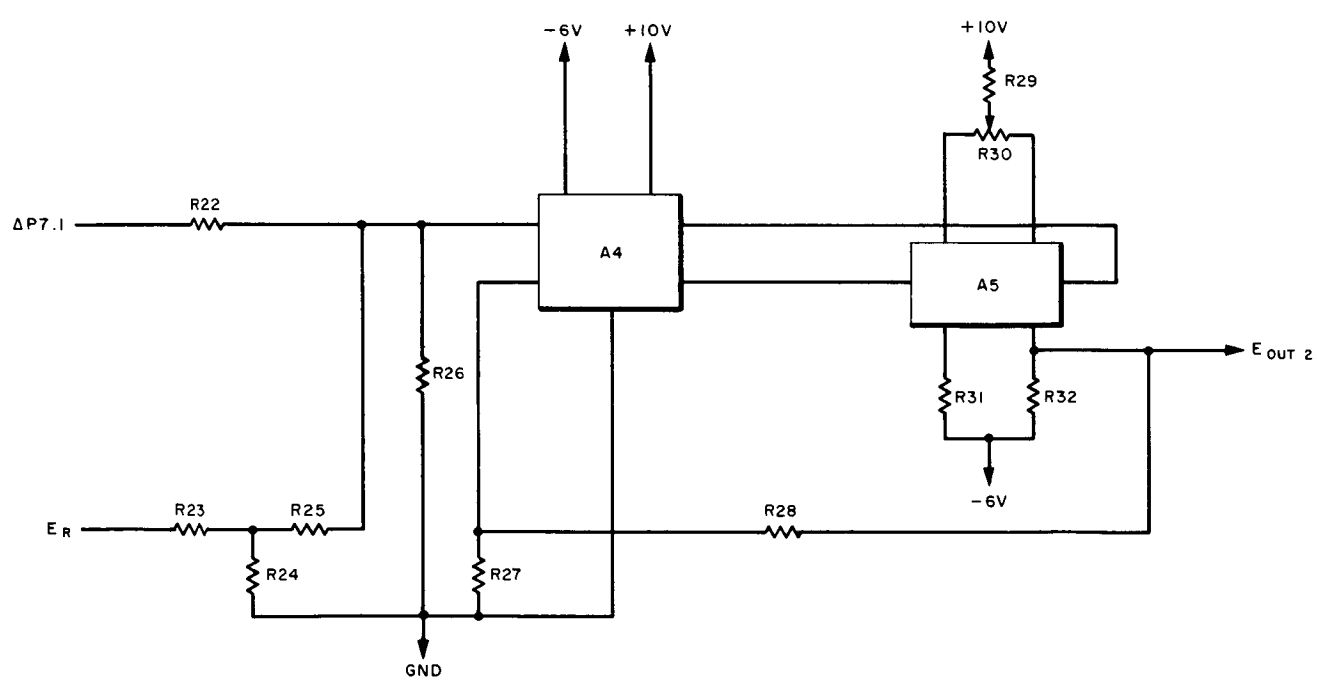


FIGURE 5-20

MAIN CHAMBER PRESSURE
SIGNAL PROCESSING CIRCUIT, P1 (V2-1)





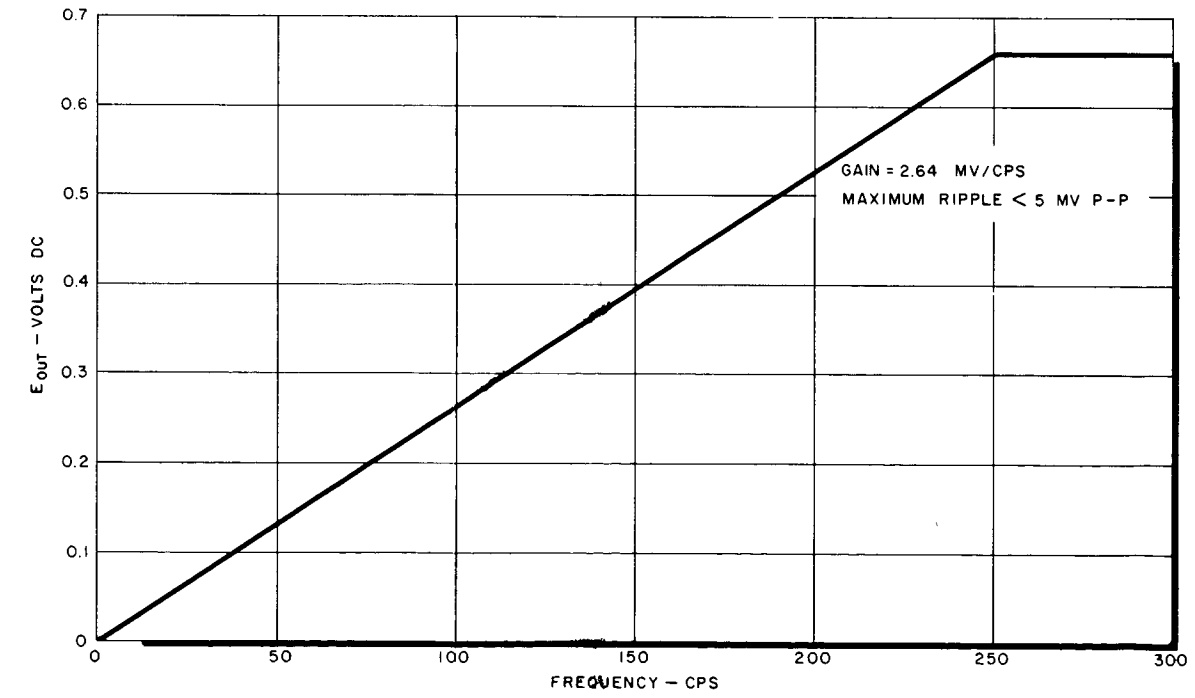
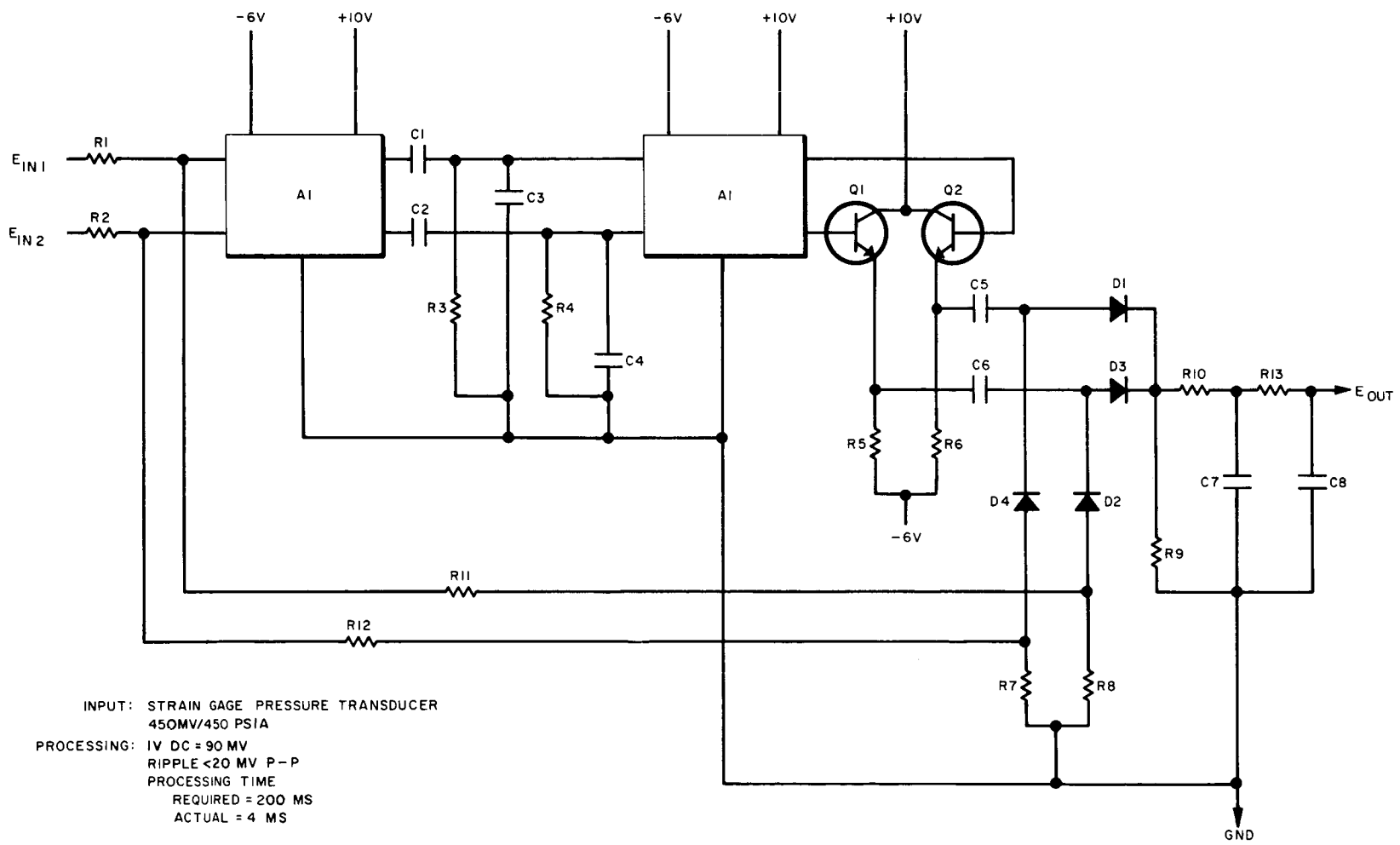


FIGURE 5-21
LOX FLOW SIGNAL PROCESSING CIRCUIT
Q12 (V7.1)



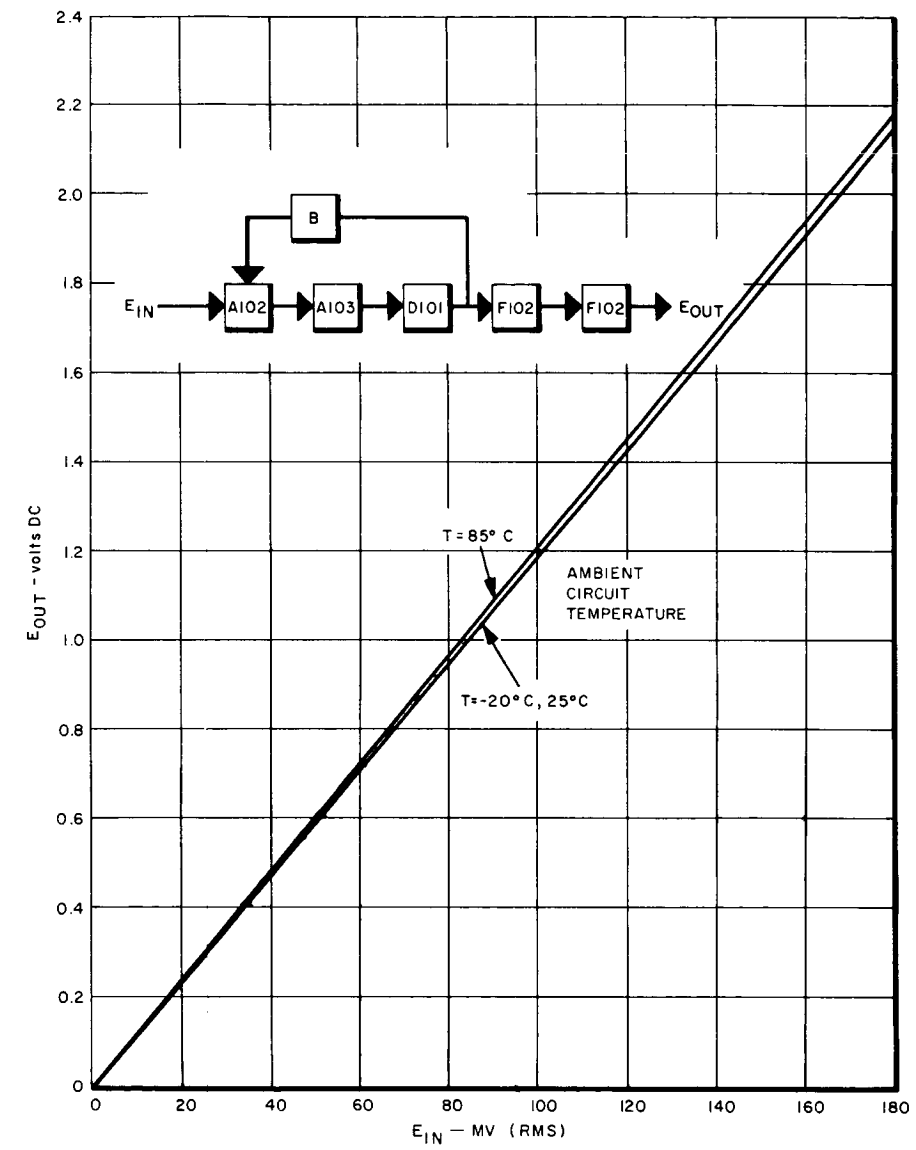
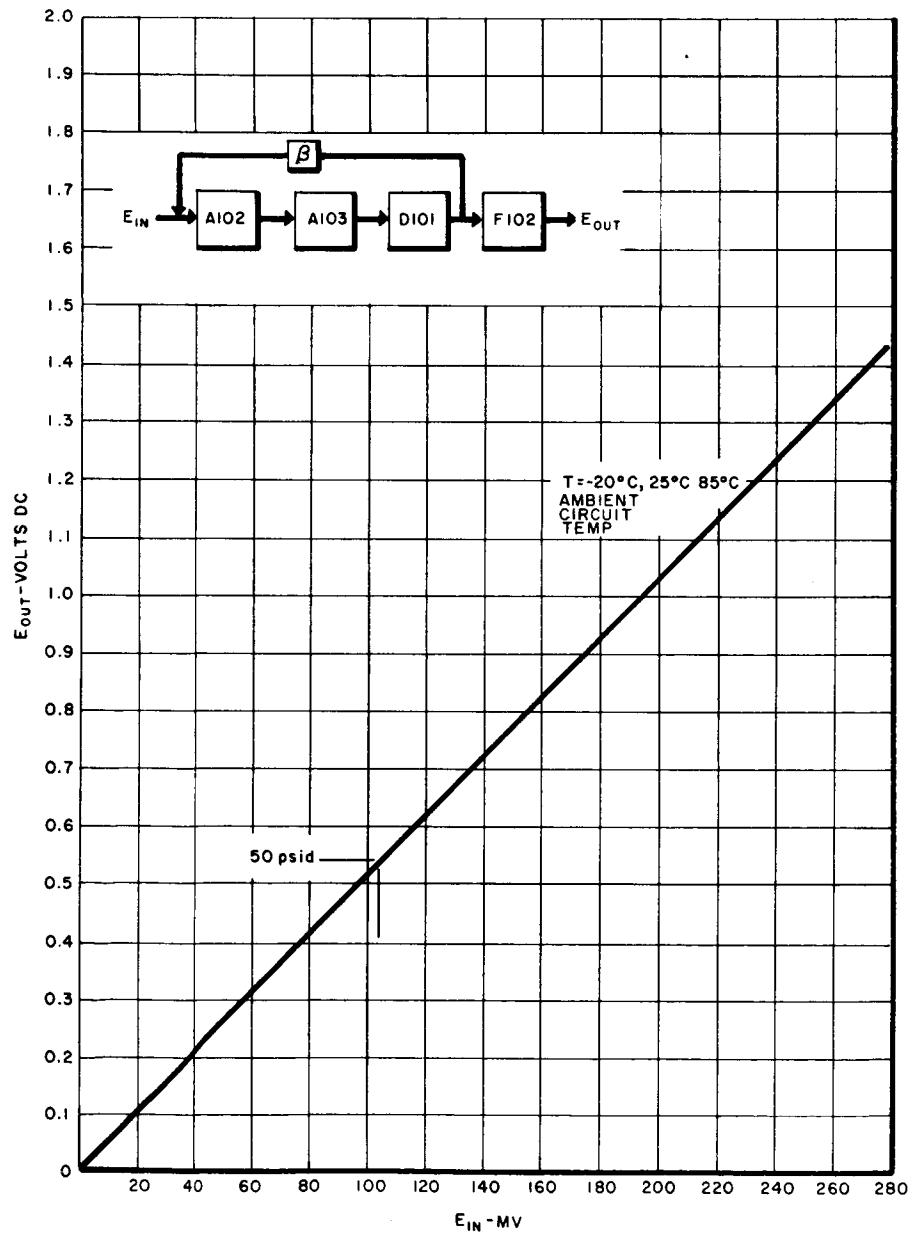
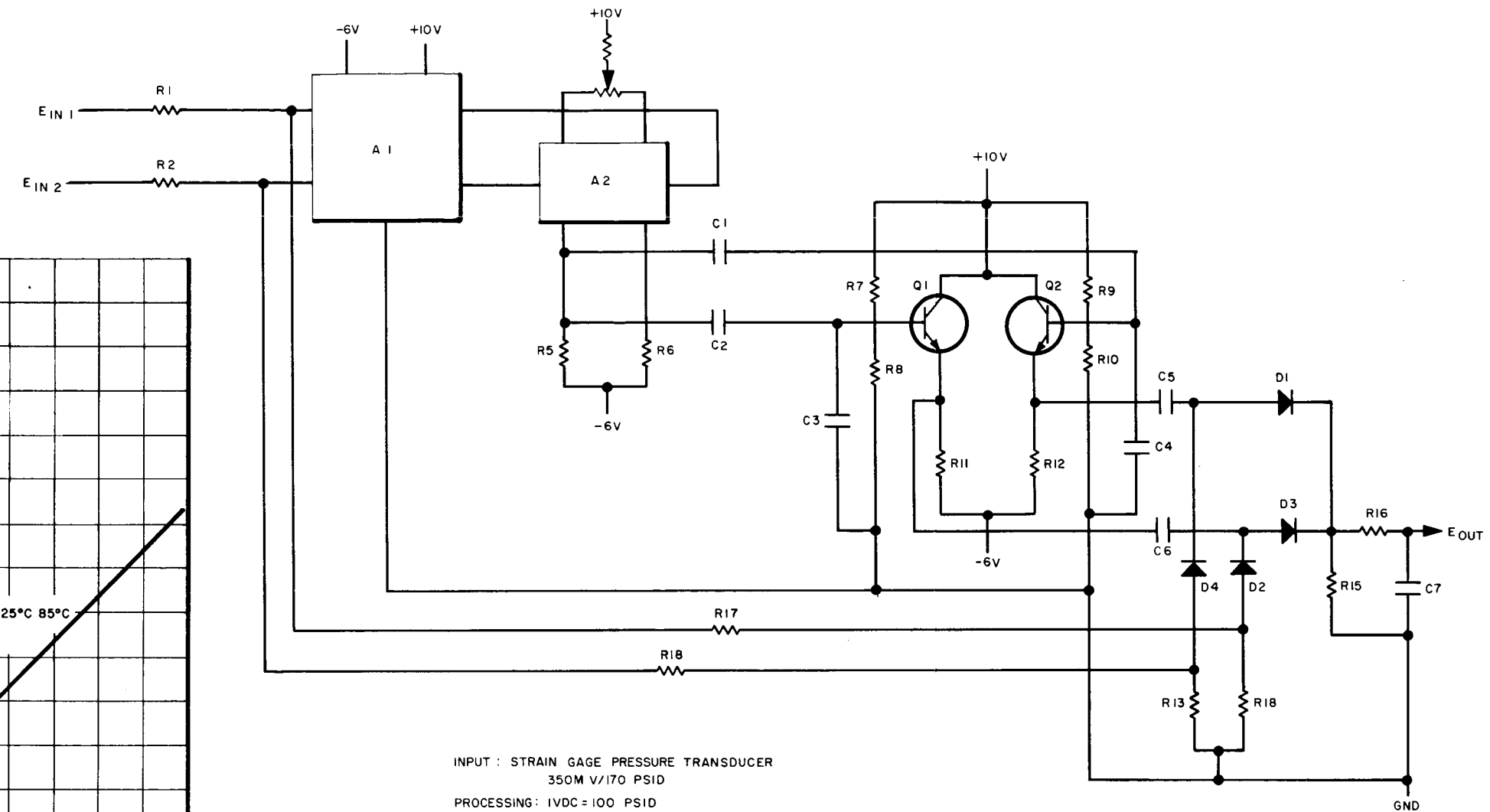


FIGURE 5-22
LOX INJECTOR PRESSURE SIGNAL
PROCESSING CIRCUIT, P7-P1 (V5.1, V7.1)

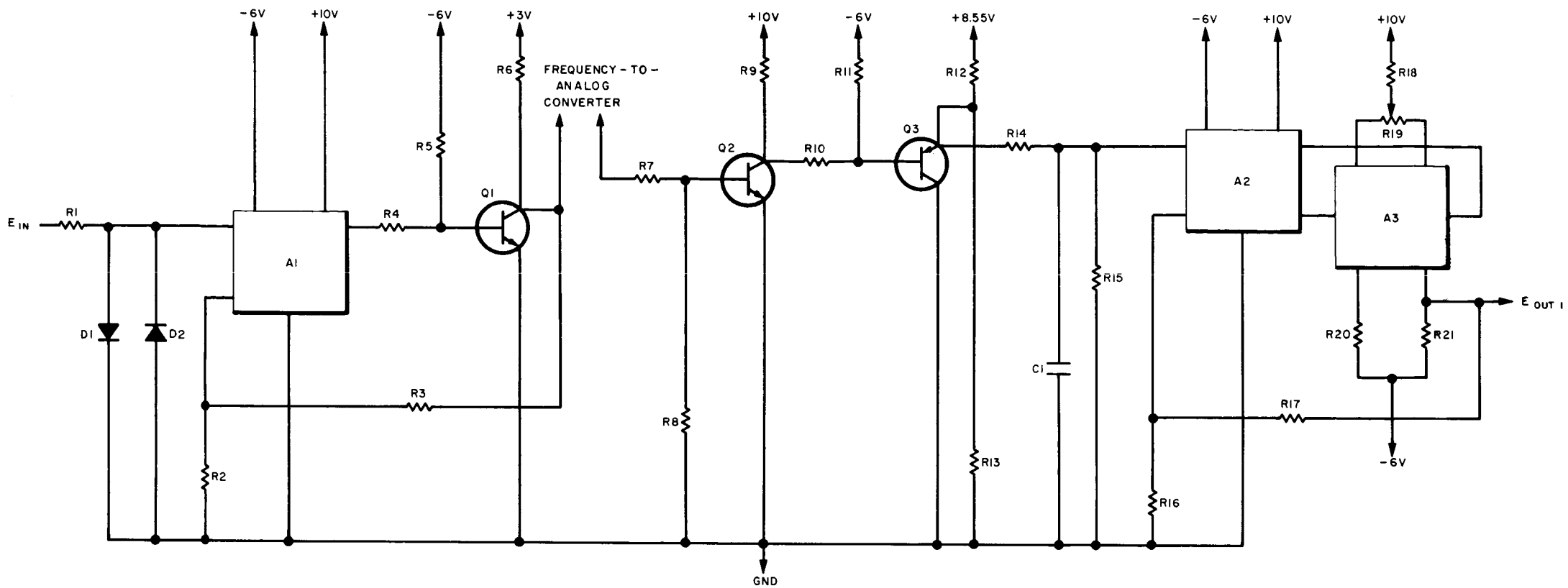


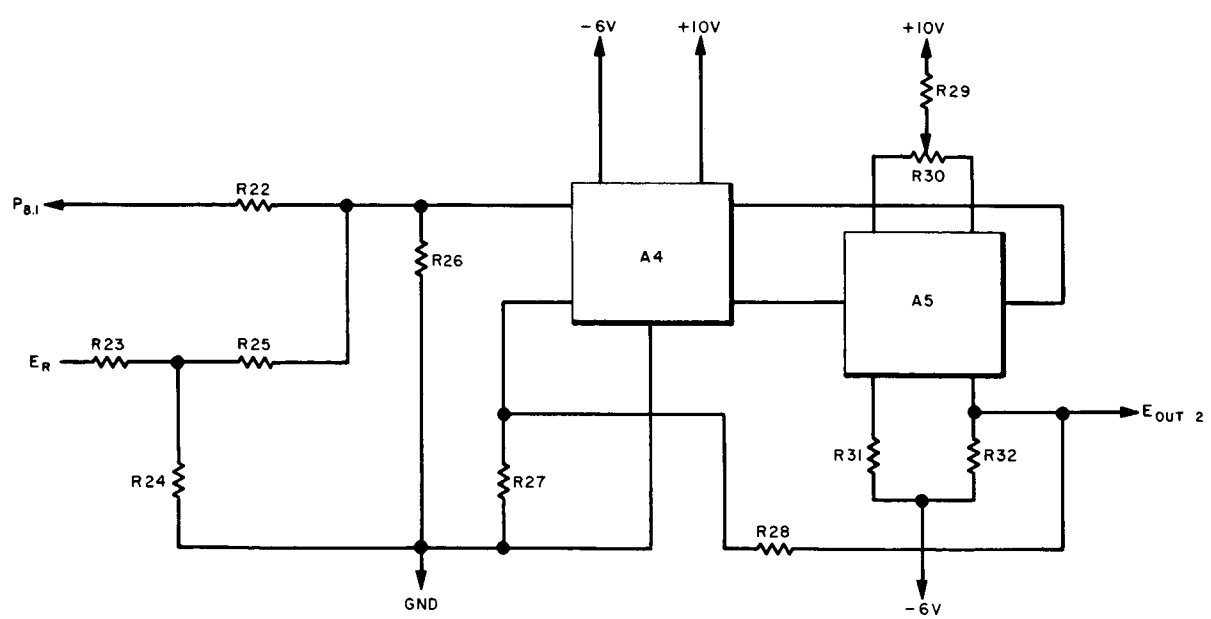


INPUT : STRAIN GAGE PRESSURE TRANSDUCER
350M V/170 PSID

PROCESSING: 1VDC = 100 PSID
RIPPLE < 20mv
PROCESSING TIME
REQUIRED = 200MS
ACTUAL = 4MS

FIGURE 5-23
FUEL INJECTOR PRESSURE SIGNAL PROCESSING CIRCUIT, P8-P1(V5.1,V8.1)





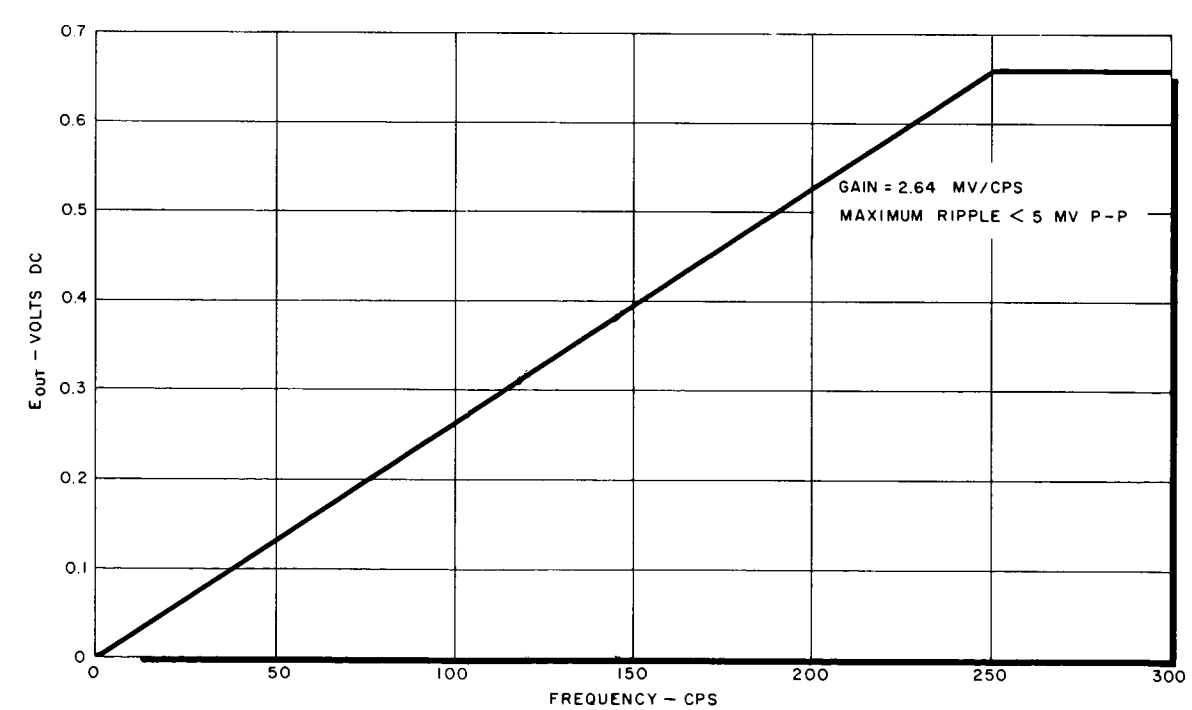
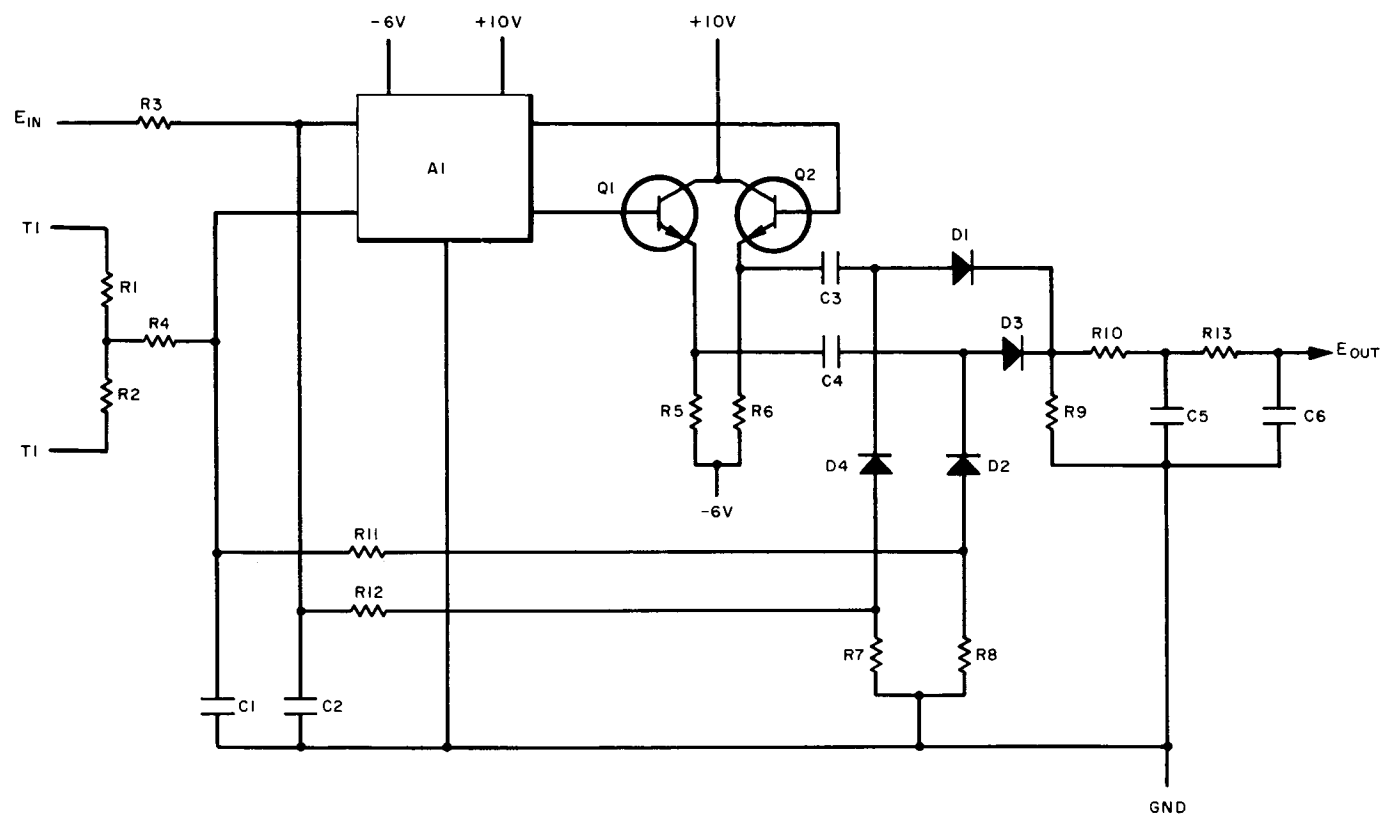


FIGURE 5-24
FUEL FLOW SIGNAL PROCESSING CIRCUIT
Q11 (V8.1)



INPUT: VARIABLE RELUCTANCE
PRESSURE TRANSDUCER
500MV/25 PSIG

PROCESSING: 1V DC = 15 PSIG
RIPPLE < 20MV P-P
PROCESSING TIME:
REQUIRED = 50MS
ACTUAL = 9 MS

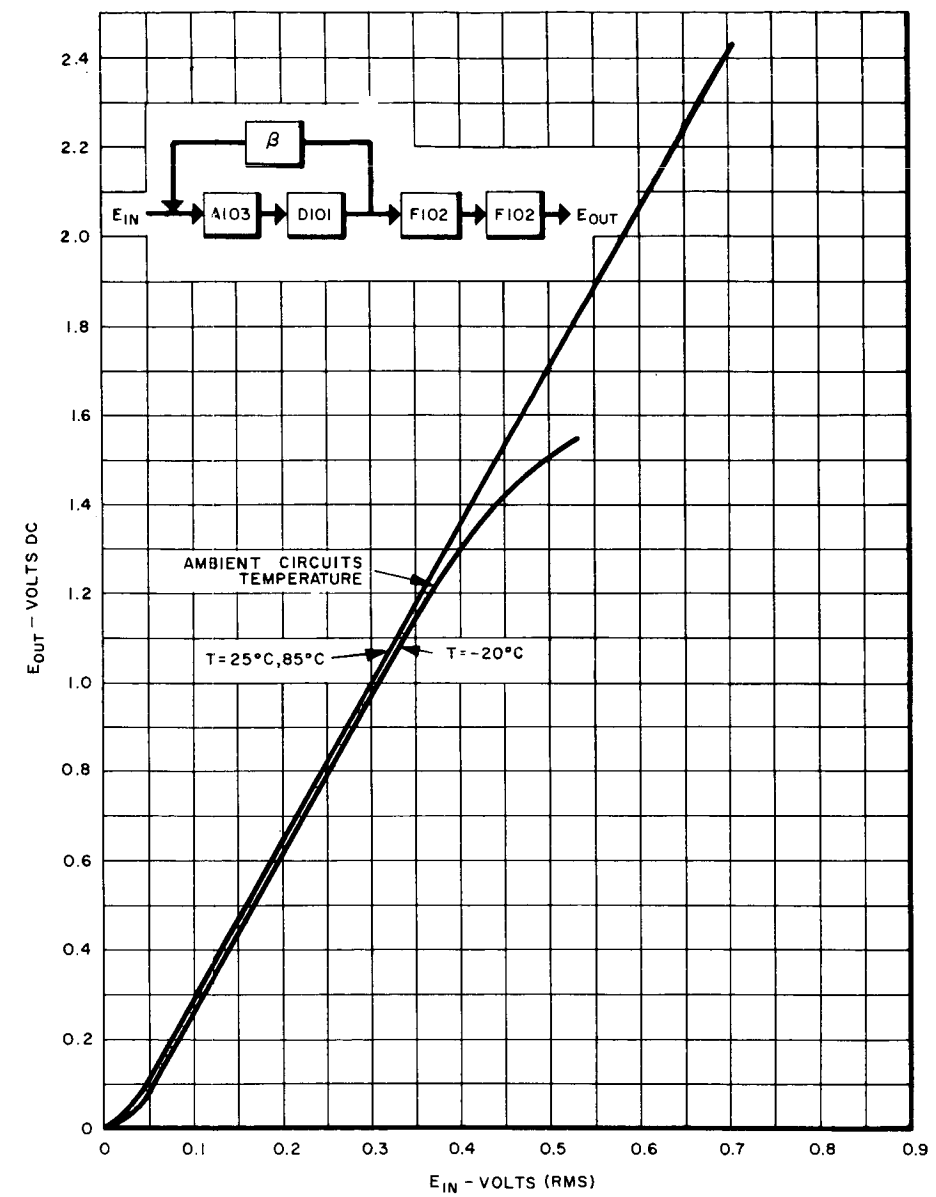
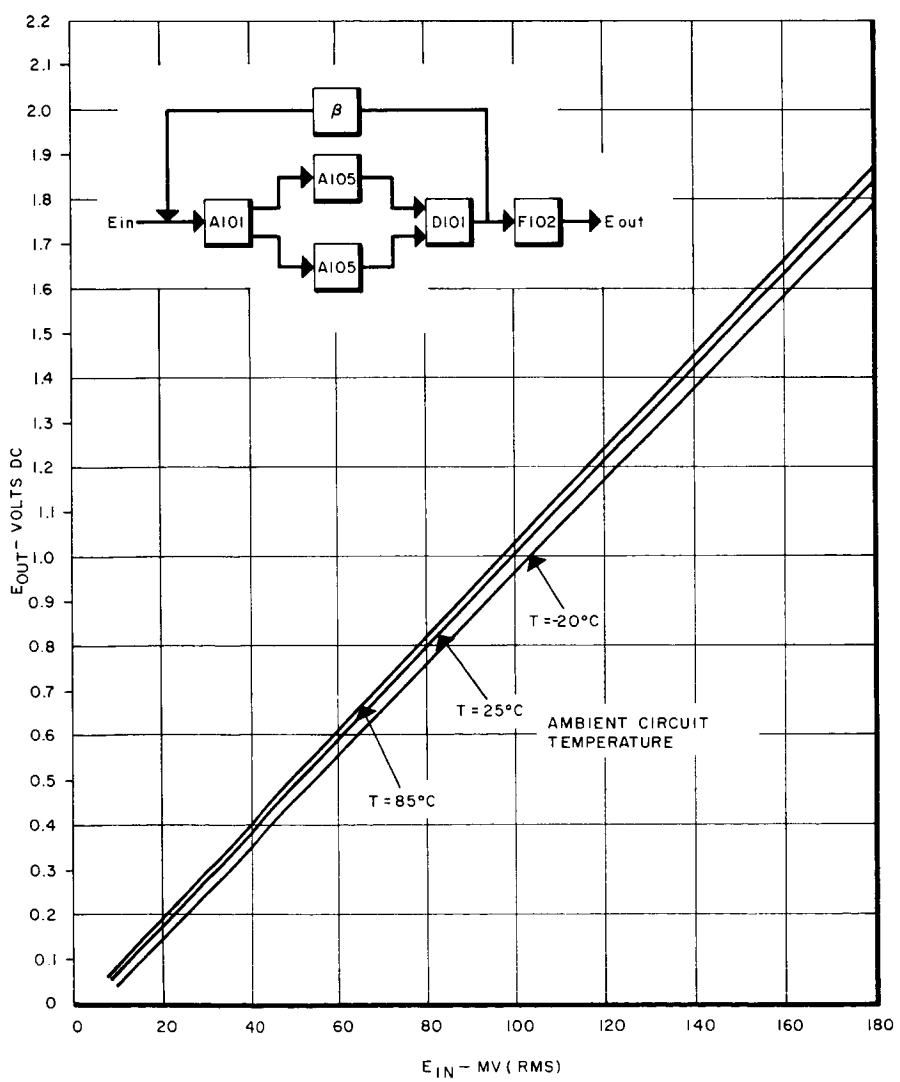
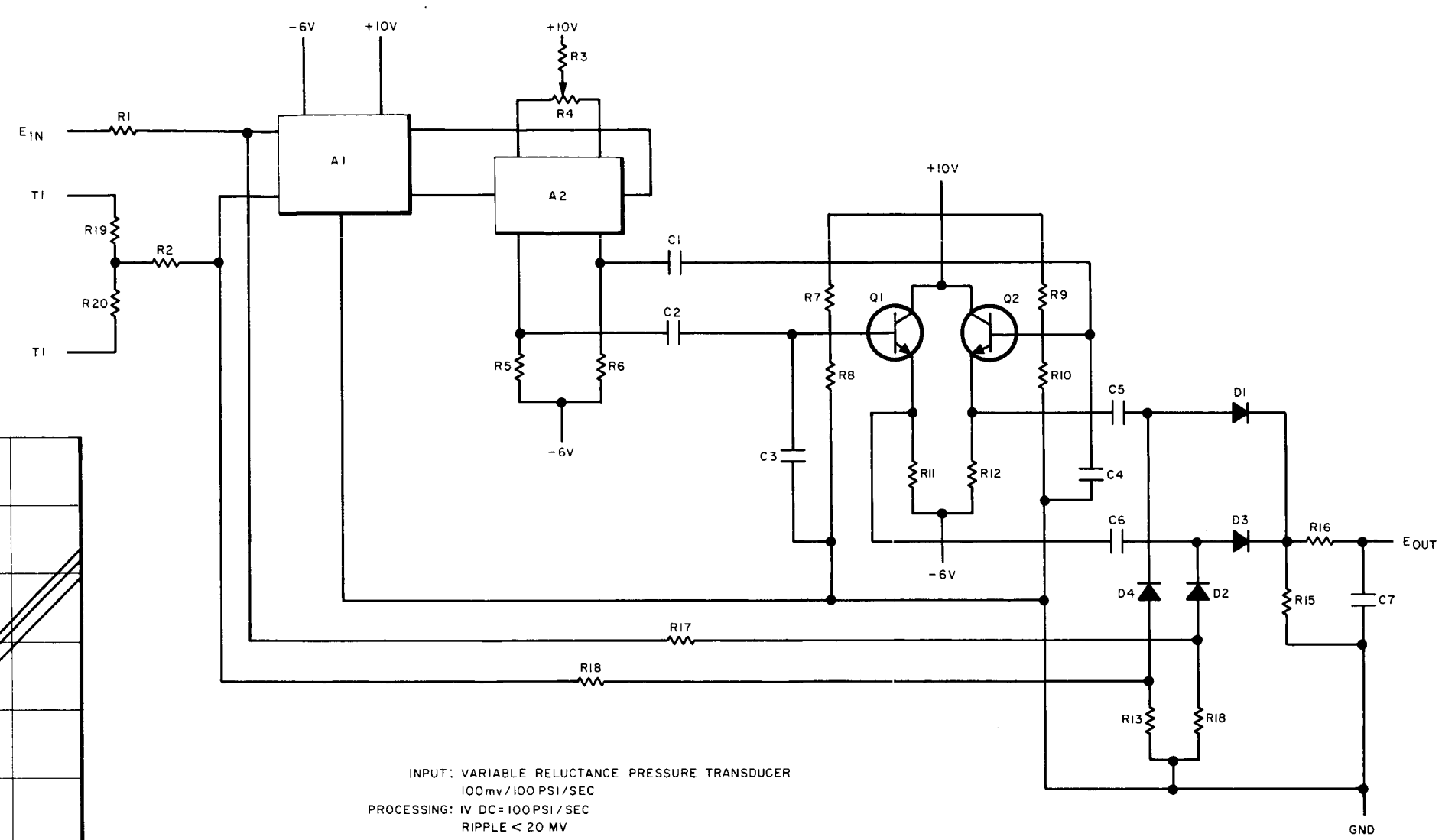


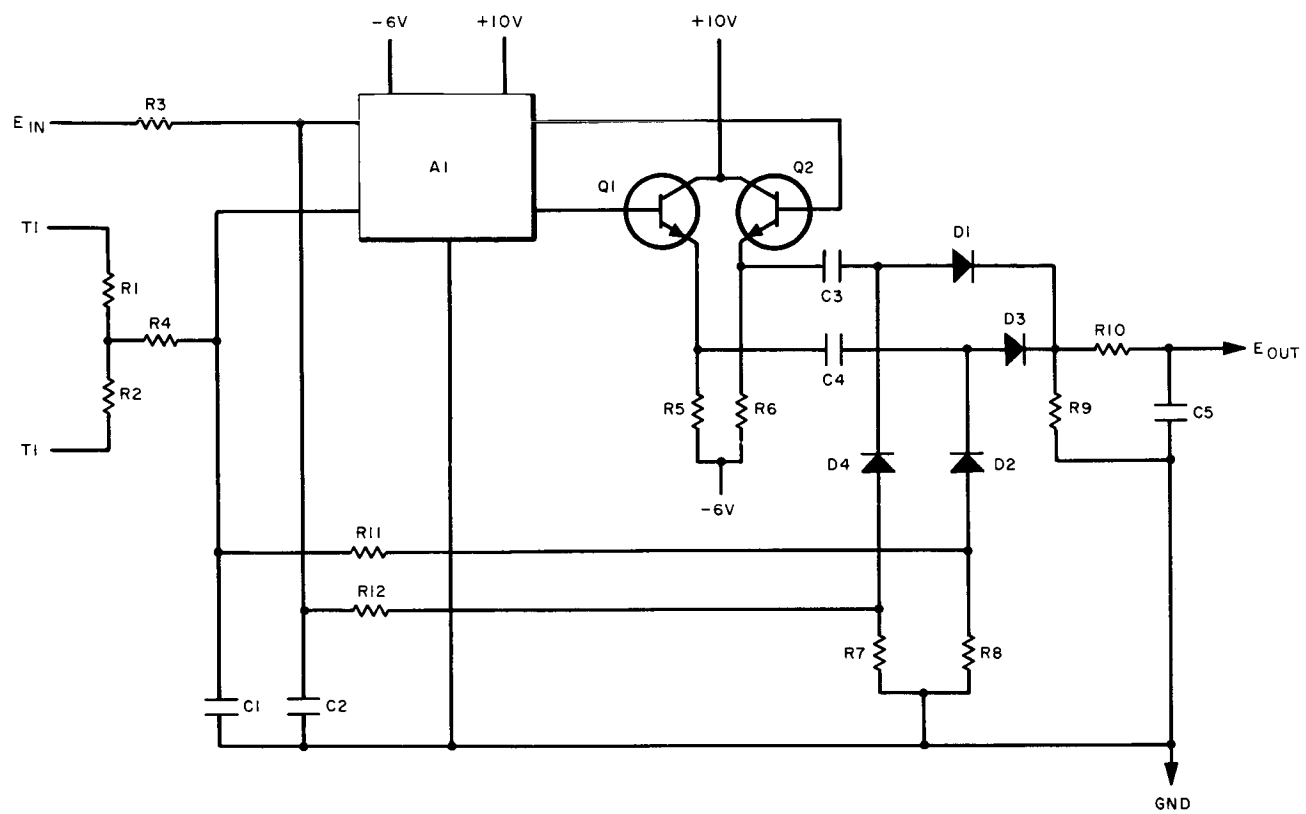
FIGURE 5-25
GEAR CASE PRESSURE
SIGNAL PROCESSING CIRCUIT, P4 (V15-1)





INPUT: VARIABLE RELUCTANCE PRESSURE TRANSDUCER
100mv/100 PSI/SEC
PROCESSING: IV DC = 100 PSI/SEC
RIPPLE < 20 MV
PROCESSING TIME
REQUIRED = 20 MS
ACTUAL = 4 MS

FIGURE 5-26
BLAST PRESSURE
SIGNAL PROCESSING CIRCUIT, dPs/dt



INPUT : VARIABLE RELUCTANCE
PRESSURE TRANSDUCER
1V/8psig

PROCESSING : 1V DC = 3 PSIG
RIPPLE < 20MV P-P
PROCESSING TIME :
REQUIRED = 500 MS
ACTUAL = 9 MS

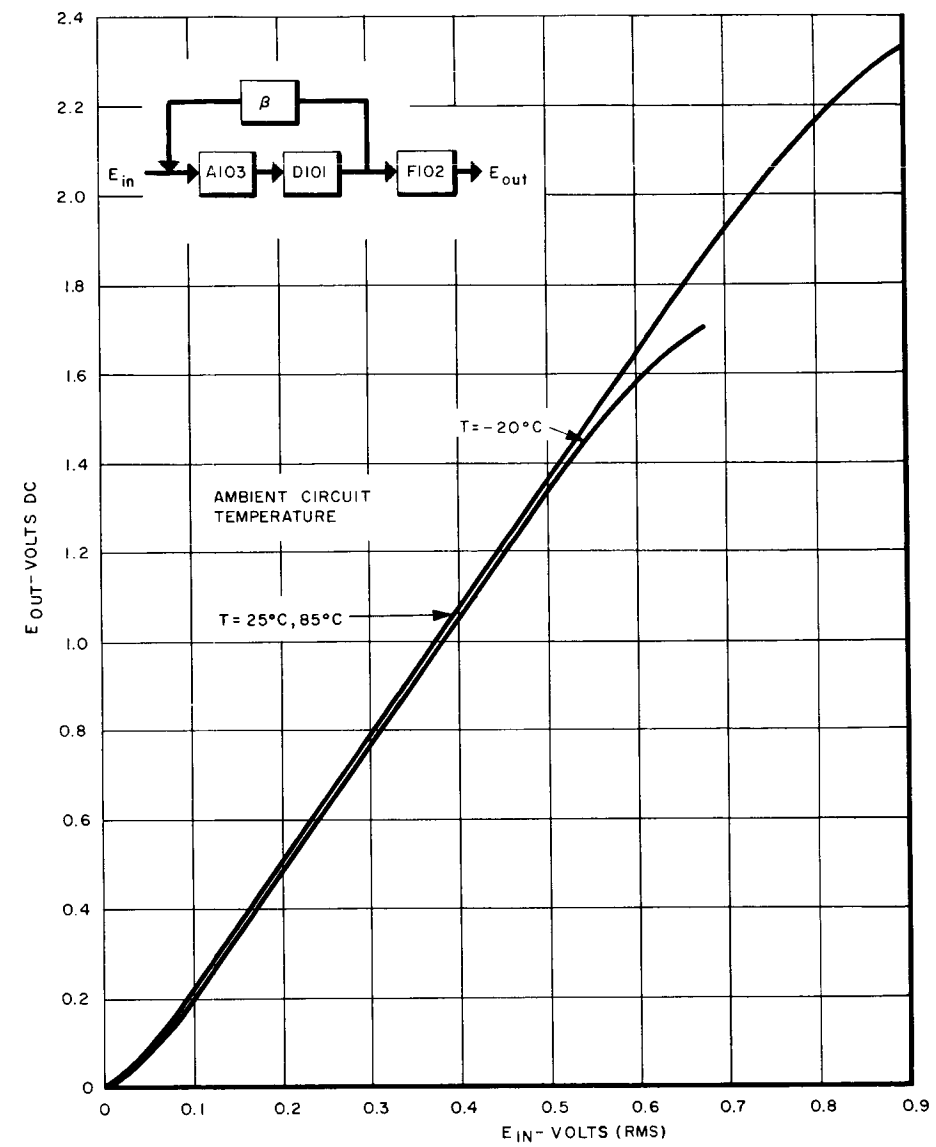
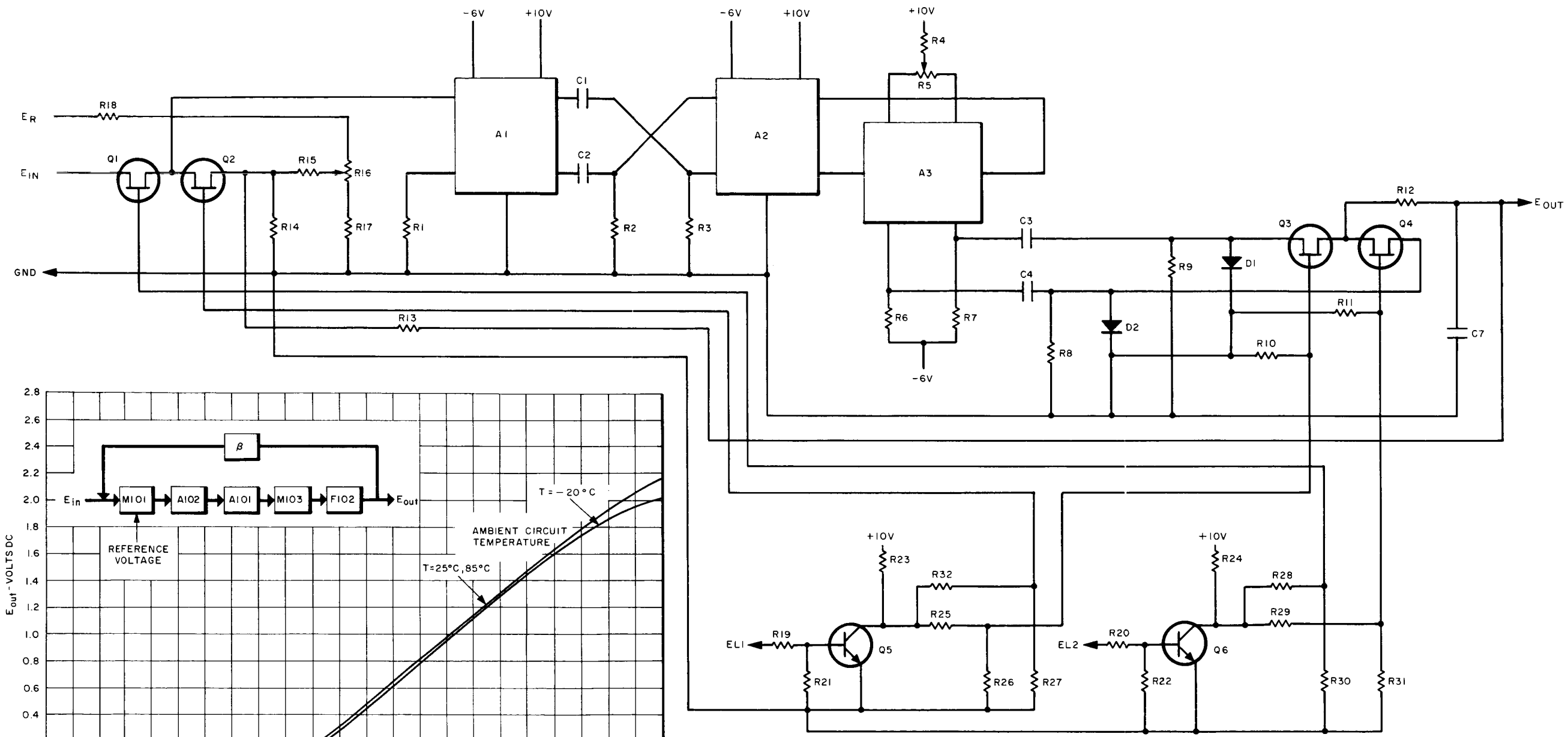


FIGURE 5-27

TURBINE EXHAUST PRESSURE
SIGNAL PROCESSING CIRCUIT, P5 (V14.1)



INPUT: THERMOCOUPLE
E_{IN} = 11.1 MV + 0.022 MV/°F
E_R = + 8.55 V DC
OFFSET = 18.1 MV
PROCESSING = 700°F, = 1200°F
RIPPLE < 15MV P-P AT 1V DC
PROCESSING TIME:
REQUIRED = 500 MS
ACTUAL = 2.5 MS

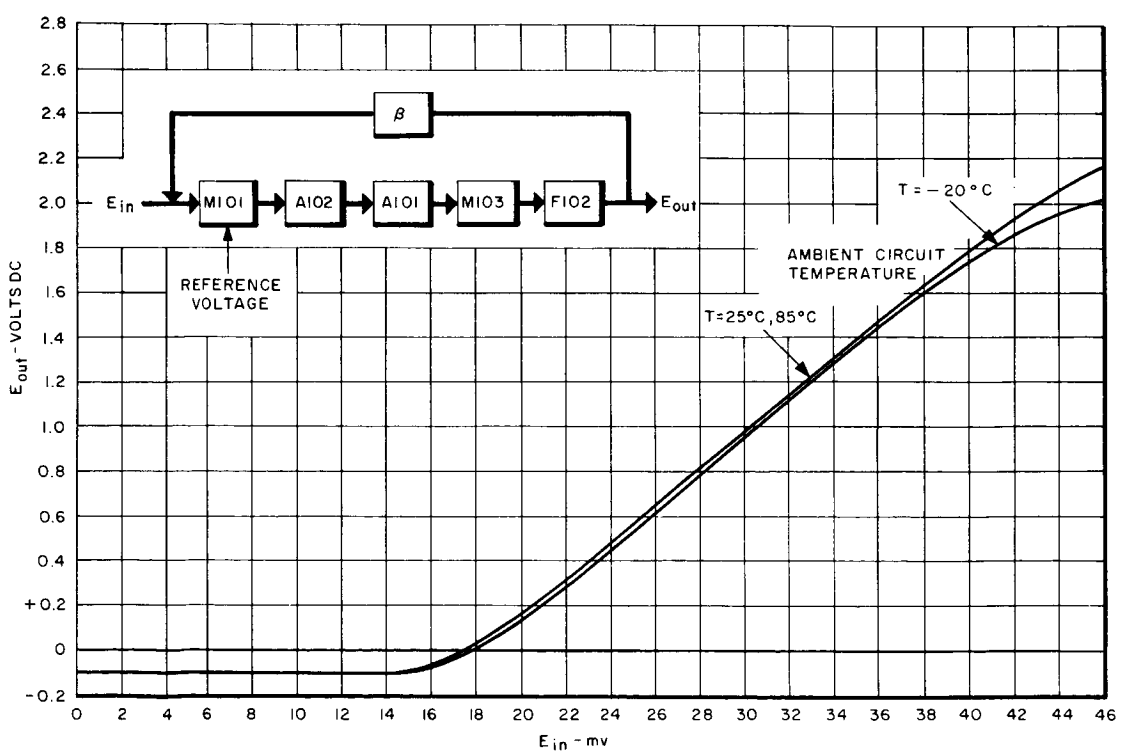
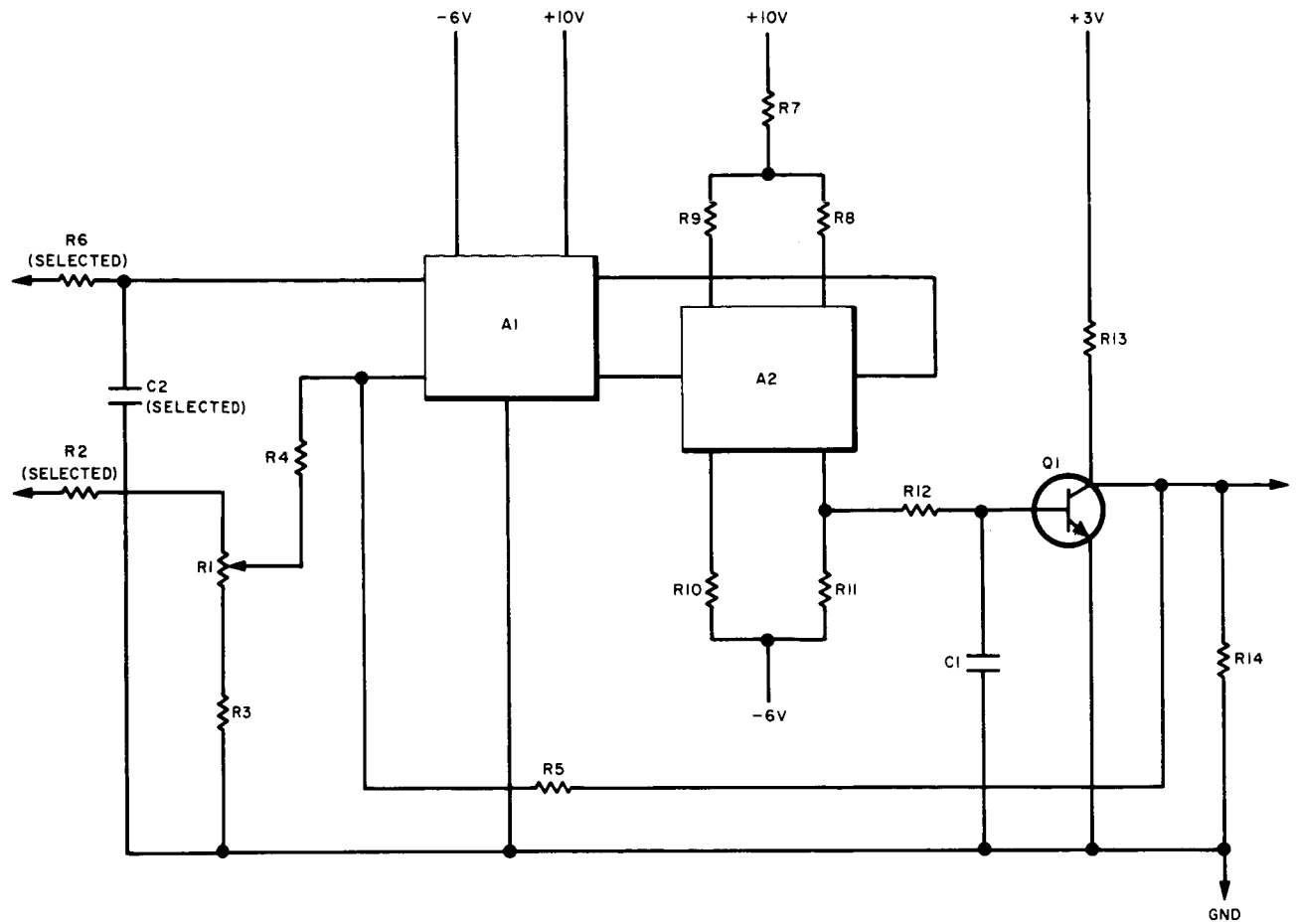


FIGURE 5-28

HEAT EXCHANGER EXIT
THERMOCOUPLE SIGNAL PROCESSING CIRCUIT, T10(V14.1)



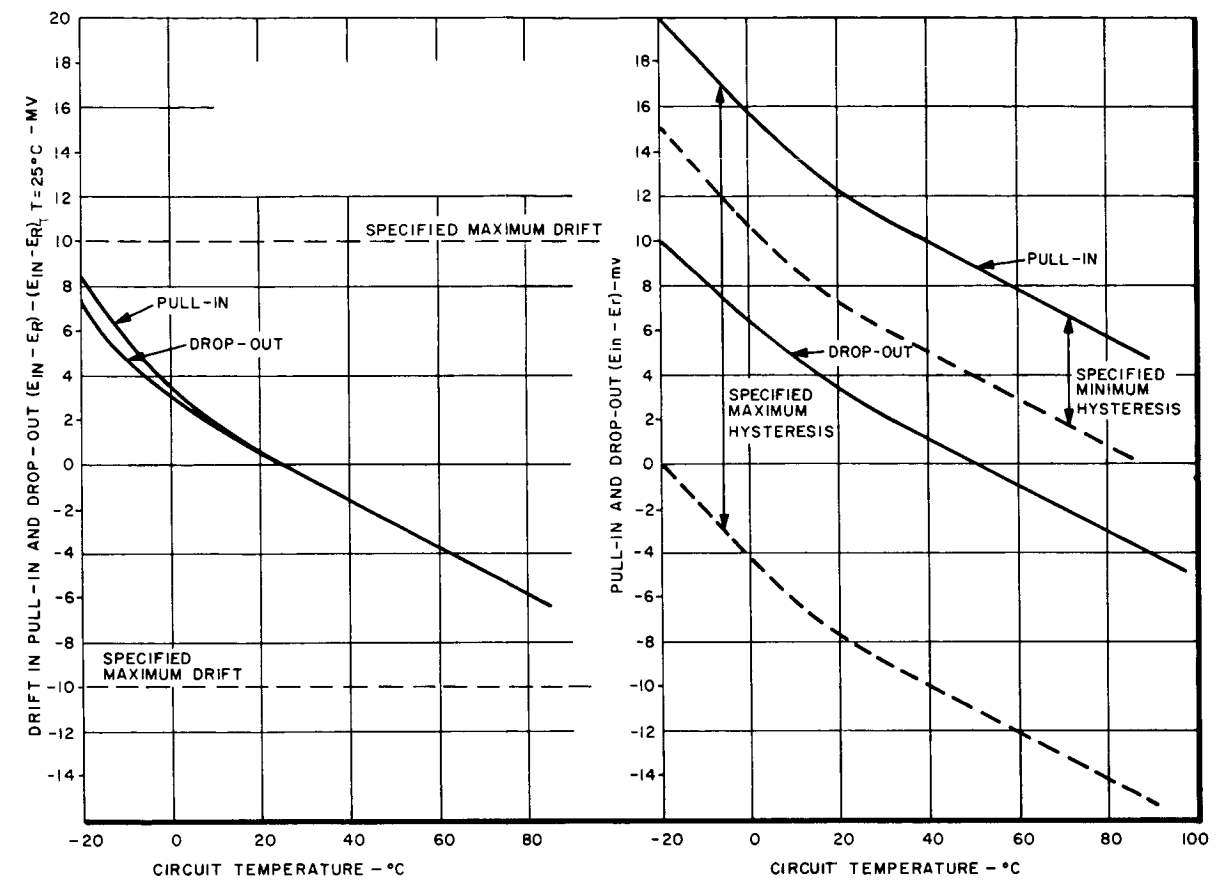


FIGURE 5-29
LOW LEVEL COMPARATOR C101

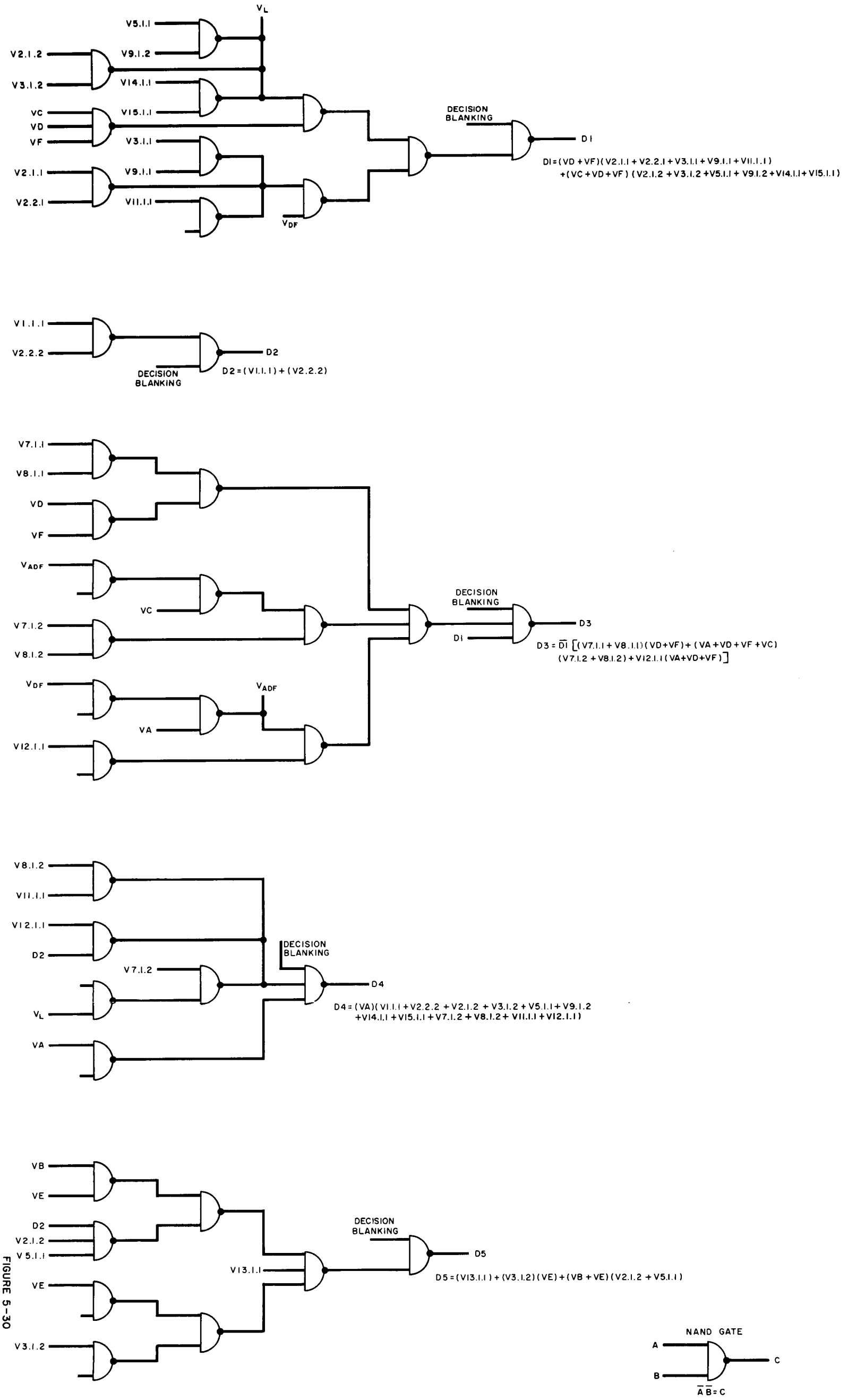


FIGURE 5-30
DECISION LOGIC CIRCUIT DIAGRAM

F. EQUIPMENT CONFIGURATION

1. Experimental READI System Transducers

The objectives in the selection of transducers for the experimental READI system were twofold: first to provide the required signals for the selected set of malfunction detection channels of the system (refer to Appendix E), and second, to cover the variety of transducer types which may be anticipated in a future airborne system. Table 5-2 shows the variety of types and ranges of output signals which are covered in the experimental system. The actual transducers employed are shown in table 5-6. Figure 5-31 shows several of the pressure transducers which are used in the system. The velocity type transducer used to sense main chamber and turbopump vibrations is shown in figure 5-32. This type of vibration pickup was selected because of its excellent ability to withstand a severe vibration environment and its self-generating electrical property which precludes failures causing false alarms.

2. Electronic Assembly Unit

In accordance with program objectives, the experimental READI design effort has been directed principally to developing advanced circuit techniques applicable to eventual production, in microelectronic form, for a vehicle installed READI system. No effort has been made to design the electronic package in final airborne form. The packaging philosophy, rather, is to fabricate a reliable, and serviceable experimental system, using conventional assembly techniques, and without imposing critical constraints on overall equipment size. As a result, the experimental electronic unit constructed has a relatively low packaging density, but is nevertheless quite suitable for engine test stand evaluation.

All processing and logic circuitry are mounted on plug-in cards measuring 4-1/2 inches wide by 5 inches high. The flat substrate geometry and plug-in method of module interconnection is well suited for circuit modification, troubleshooting, and repair. The cards consist of both printed wired, epoxy glass and hand wired, metal base boards. Printed boards were specially fabricated for those microelectronic circuits where repetitive circuits exist with a commonality of interwiring. Each board includes compact arrays of landless plated thru holes, which simplify the assembly and soldering of the TO-5 microelectronic elements. There are 32 double-sided, printed boards in the electronics unit. Four printed circuit boards were designed to accommodate the V logic, four stage counters, frequency-to-analog

converter, and decision logic modules. Each of these modules is functionally described in paragraph 5-3,E. The V logic and four stage counter modules are shown in figures 5-33 and 5-34. The metal base cards are reserved for the analog processing circuits which comprise a high percentage of conventional components. The card used is a standard Sperry design with 70 holes, aligned on a grid system, available for component and teflon insert mounting. Such a versatile board is dictated by the appreciable dissimilarity between the transducer signal conditioning circuits. Twenty metal-base modules are assembled in the experimental system. Two such modules namely the Blast Pressure (dP_s/dt) and Lox Injector Pressure (P7-P1) signal processors are shown in figures 5-35 and 5-36, respectively. The electrical design of each of these modules is described in paragraph 5-3,E.

All cards are mounted in a card file frame, shown in figure 5-37, which is constructed as an integral part of a chassis. Electrical interconnections between the card modules and other READI system components is accomplished through the card connectors and a wiring harness below the chassis deck. This is illustrated in figure 5-38. The card frame-chassis assembly is constructed entirely of aluminum, with three rows of slotted guide plates for card insertions. A total of 66 modules can be accommodated; thus for the experimental system as it now stands, space exists for 14 additional cards to allow for functional growth and for modification. The power supplies, oscillator, fan, and other large conventional circuit components are mounted directly to a deck plate at the front end of the chassis.

Physically, the integral chassis assembly is enclosed within a reinforced, pressurized case, which measures 11-7/8 inches high by 16-3/4 inches wide by 23-3/8 inches deep. Total unit weight is approximately 50 pounds. An external view of the unit is shown in figure 5-39. Both the chassis and case are designed to protect the circuits against the environmental hazards of an open test stand installation, and thereby insure reliable operation. The essence of this environmental design is discussed in the following paragraphs.

1. Vibration and Acoustics

Both the chassis-card file and case are rigid, relatively large mass constructions which will effectively absorb the high frequency acoustical disturbances generated by the engine. In addition, a vibration isolation rack is provided for case mounting, designed to effect a system

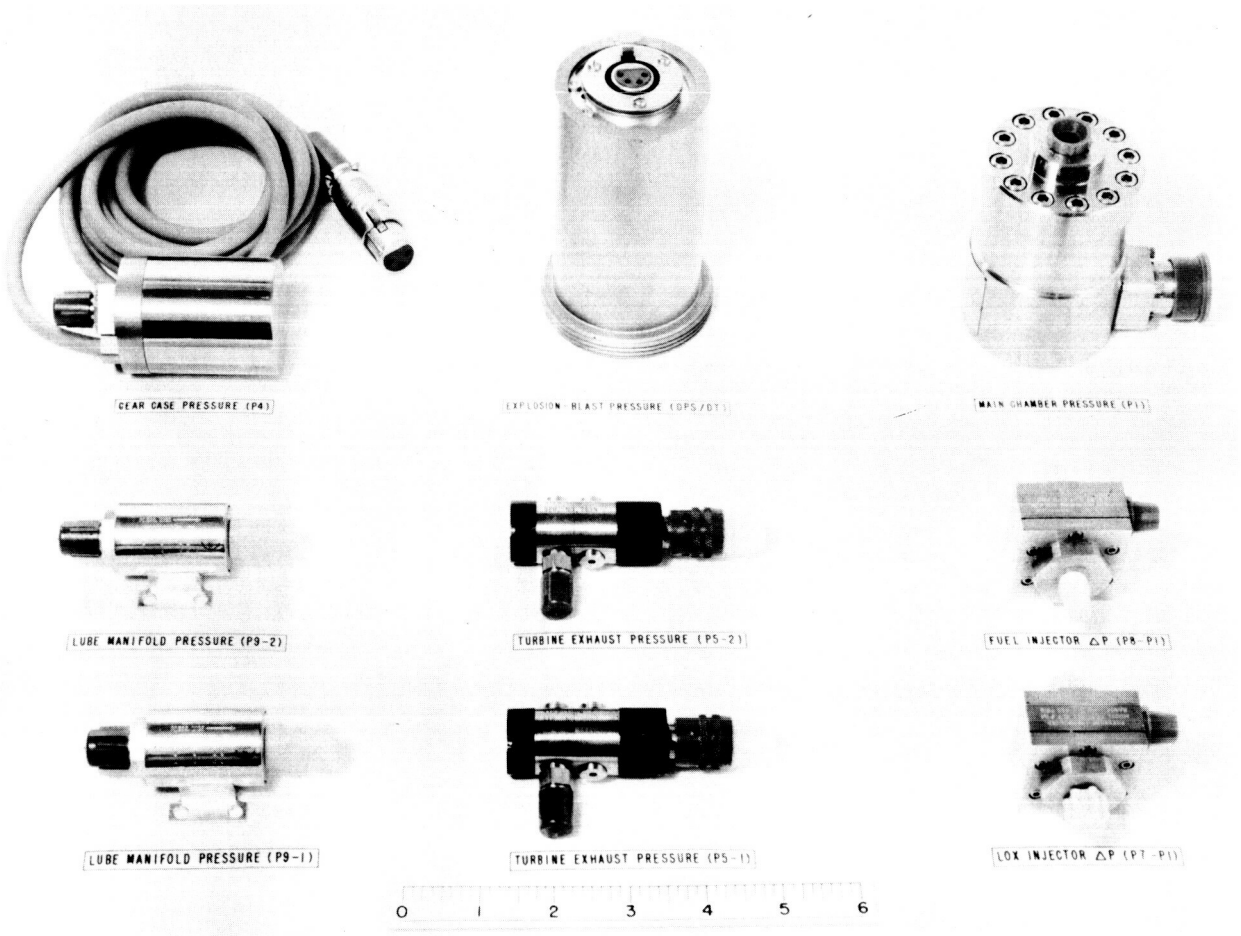


FIGURE 5-31
TYPICAL PRESSURE TRANSDUCERS USED IS EXPERIMENTAL READI

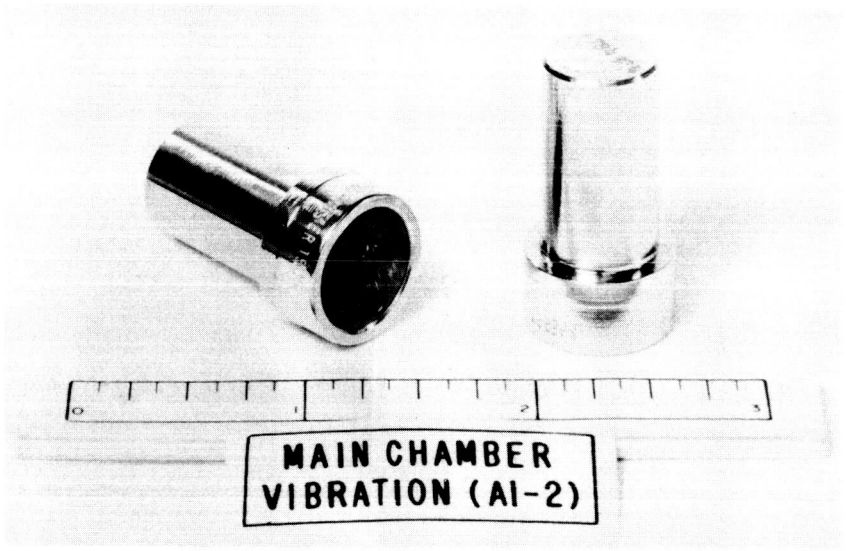


FIGURE 5-32
VELOCITY - TYPE VIBRATION TRANSDUCER

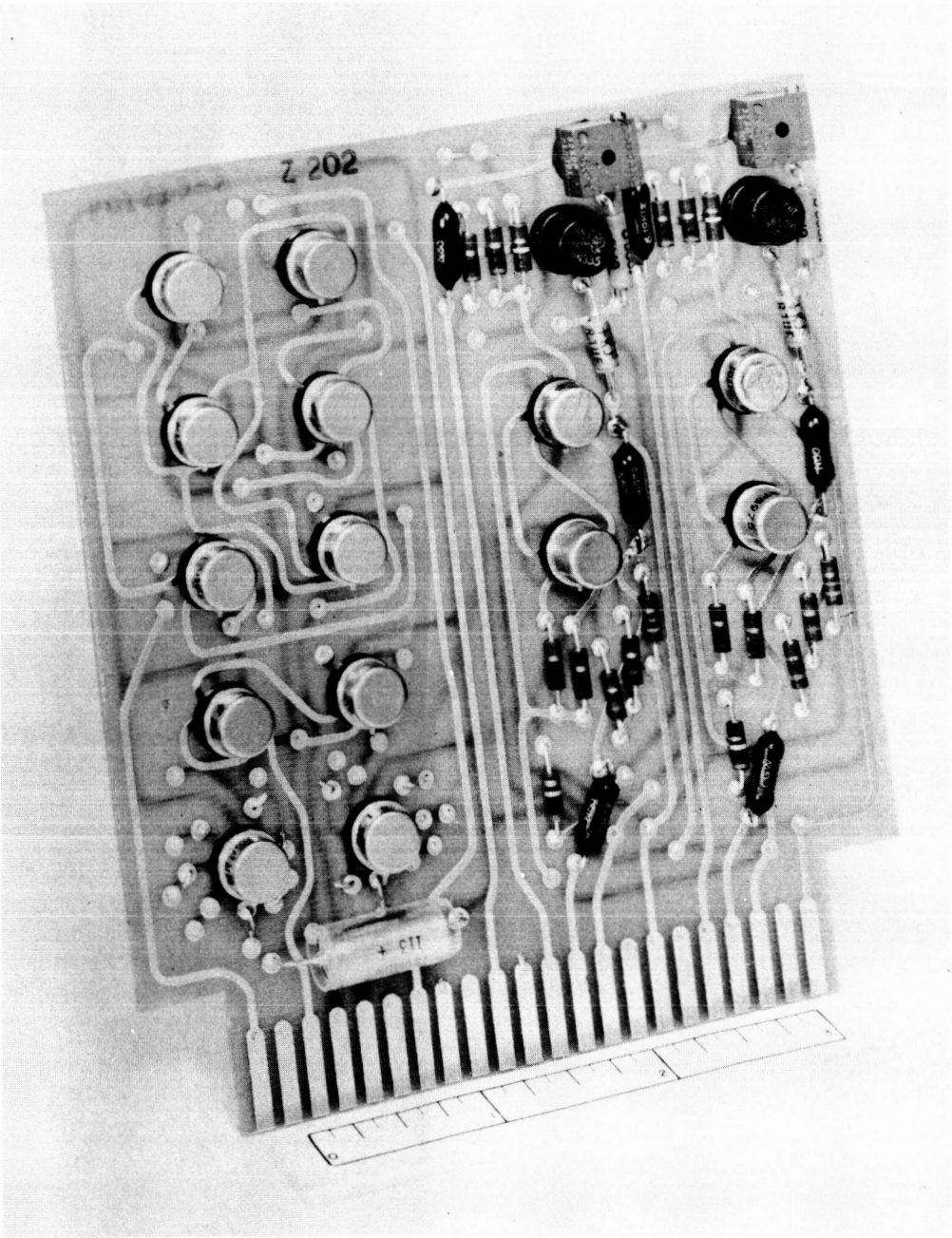


FIGURE 5-33
V-LOGIC MODULE

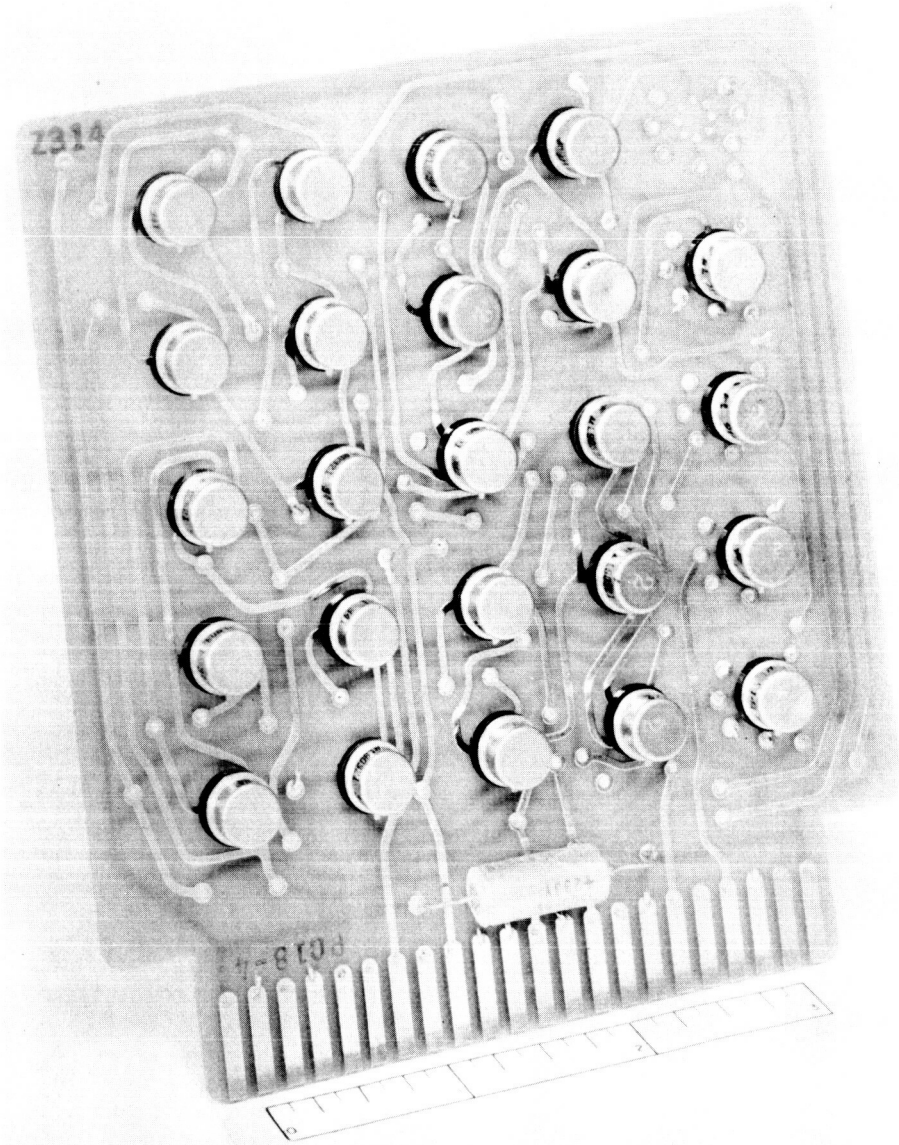


FIGURE 5-34
FOUR — STAGE COUNTER MODULE

4

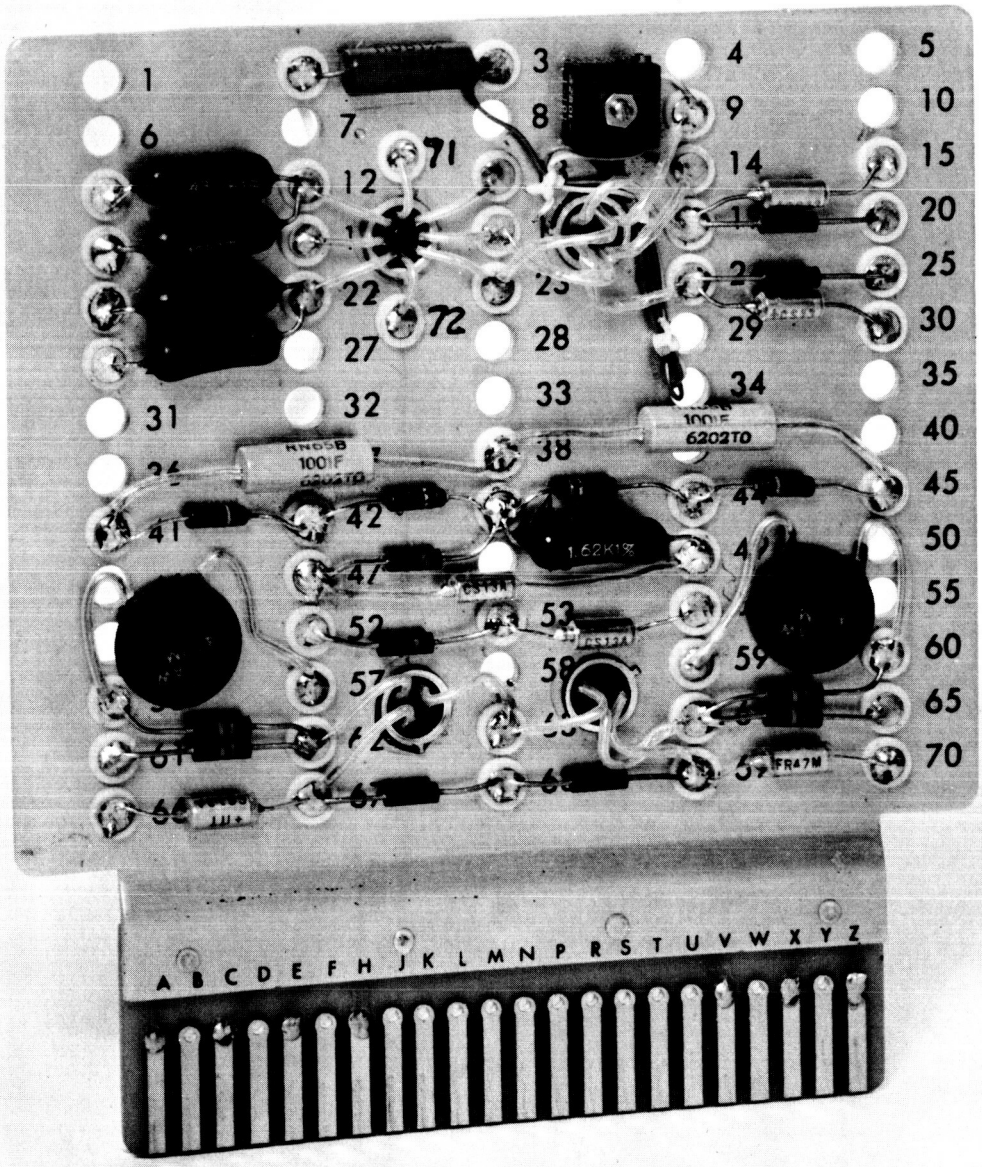


FIGURE 5-35

BLAST PRESSURE (dPs/dt) SIGNAL PROCESSING MODULE

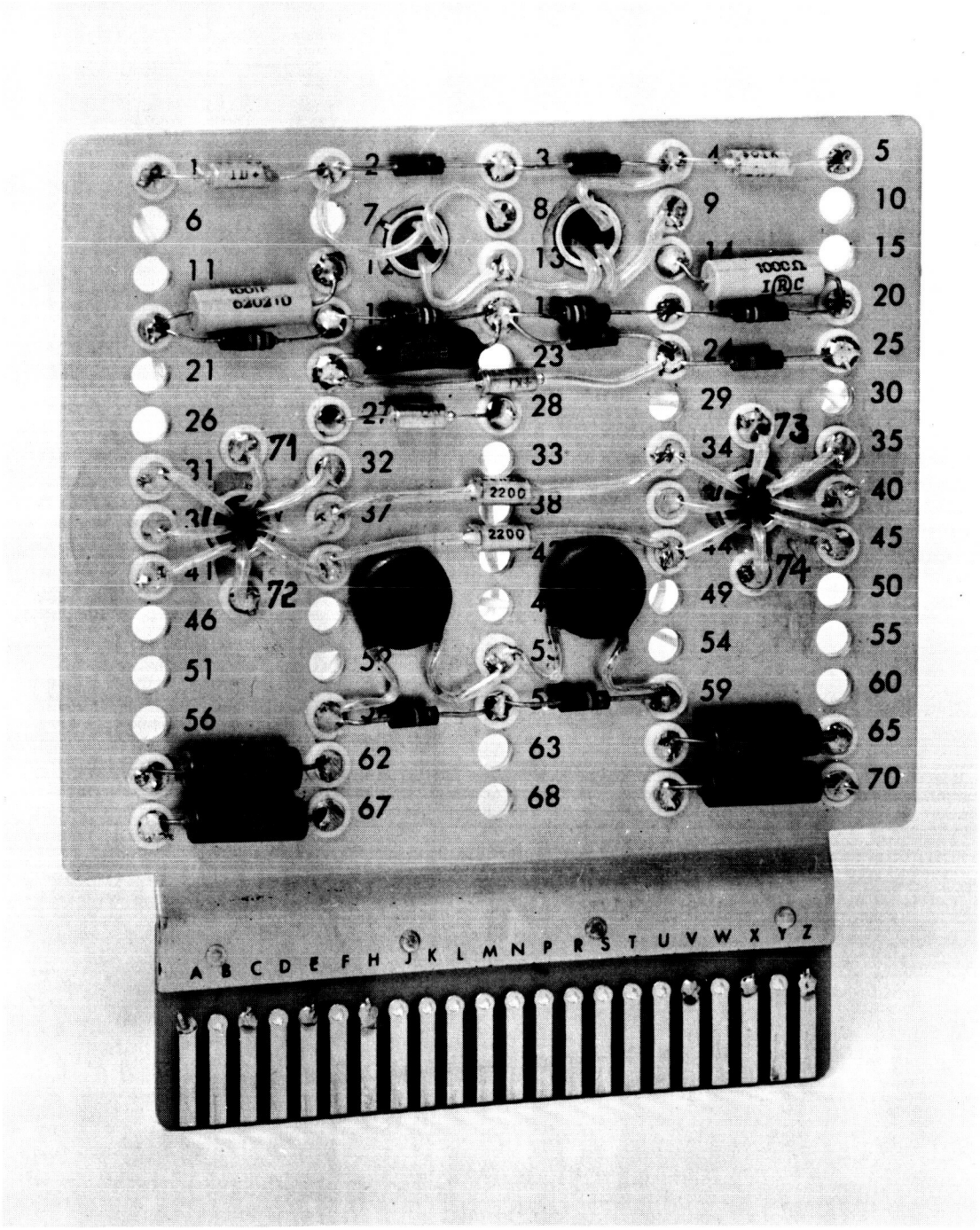


FIGURE 5-36

LOX INJECTOR PRESSURE, P7-PI, SIGNAL PROCESSING MODULE

FIGURE 5 - 37
ELECTRONIC CHASSIS ASSEMBLY FOR EXPERIMENTAL READI

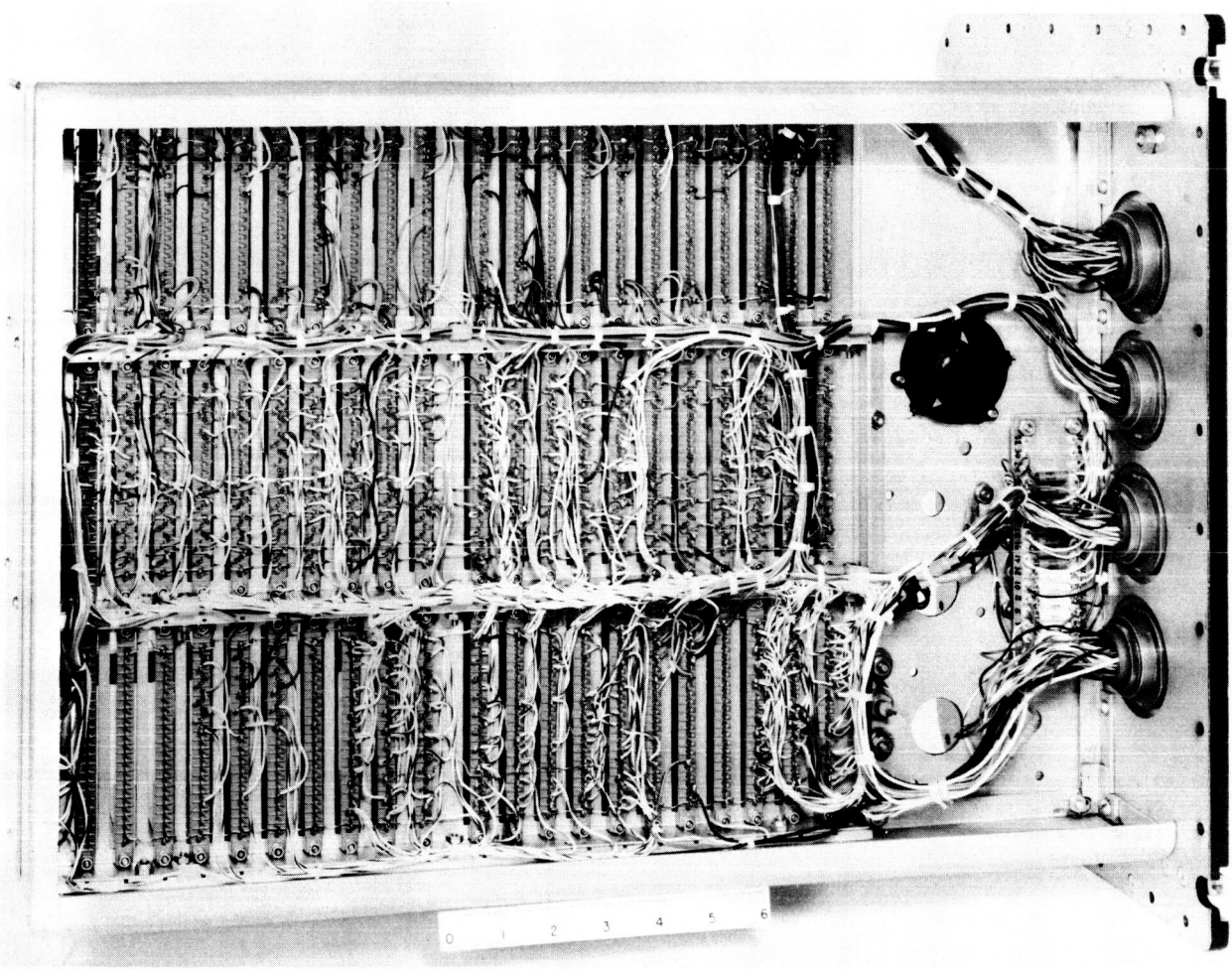


FIGURE 5-38
ELECTRONIC CHASSIS WIRING FOR EXPERIMENTAL READI, BOTTOM VIEW

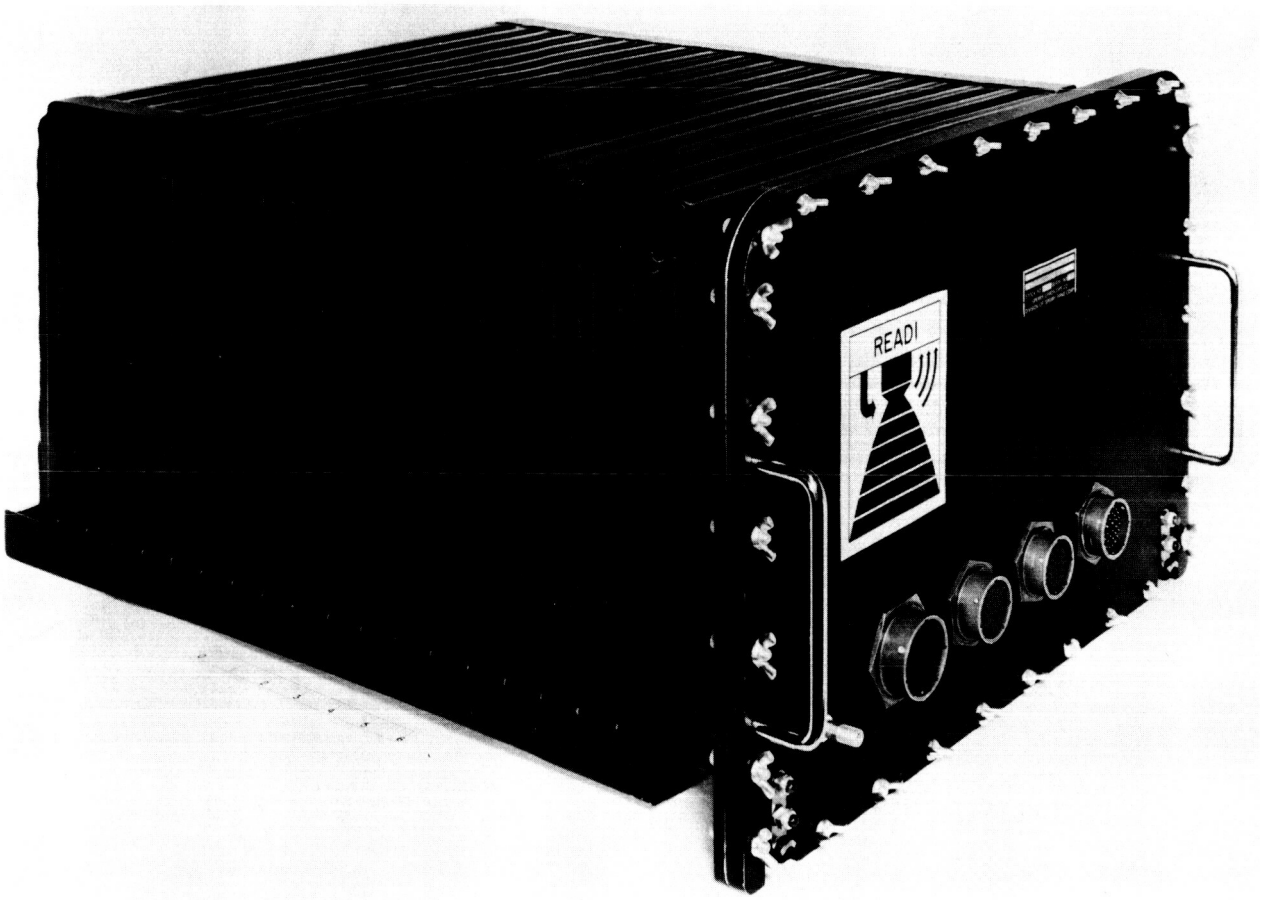


FIGURE 5-39
ELECTRONIC UNIT FOR EXPERIMENTAL READI - REINFORCED,
PRESSURIZED CASE DESIGN

natural frequency of 9 cps with a damping factor of 0.6. This rack will attenuate the higher vibration frequencies conducted by the test stand structure, and protect against sudden shock forces. The vibration isolation design is predicted on the following limits of sinusoidal excitation:

10-34 cps	0.1 inch D.A.
34-5000 cps	6 g (rms)

An acoustical field ranging up to an amplitude of 145 db between 2 and 5 kc was also assumed. This data was supplied by Marshall Test Division, based on measurements taken in an area projected for READI installation, i.e., above the thrust plate of the H-1 power plant test stand.

2. Temperature

Heat transfer analyses indicate that no special cooling provisions are required for the electronic unit. This is based in part on the following conditions of operation:

- Standard hot atmosphere (103°F)
- Power dissipation of 55 watts within the case
- All circuits qualified for satisfactory operation up to +185°F
- No exposure to solar radiation.

Under these conditions, the maximum ambient temperature inside the case under steady-state conditions, was computed to be 159°F. Additionally, the maximum surface temperatures of all components were within the respective ratings. However, as an added degree of safety, and to improve circuit reliability, a small fan has been incorporated within the unit. Based on an anticipated system pressure drop of 0.5 inch of water, the fan will deliver an air flow rate of 24 cfm, and will serve to reduce the maximum inside case temperature to 128°F.

3. Weather

The case enclosure will seal out all weather elements including rain, dust, sand, and humidity. In addition, all external connectors are of the moisture-proof type as per MIL-C-26482.

4. Explosion

The pressurized case is explosion proof in that fuel vapors cannot be entrapped within the case.

5-4. SYSTEM LABORATORY TEST

A. OBJECTIVES

This section describes a test plan for conducting a complete, methodical bench check of the experimental READI system. All procedures are completely formated (see Appendix F) and a special test set has been fabricated to simplify the testing. The test plan devised is designed to achieve three main objectives:

- Functional performance testing on the system level prior to delivery and installation on H-1 power plant test stand. This phase of testing was satisfactorily conducted at Sperry
- Visual demonstration of all functions and reliability enhancement techniques at any facility
- Periodic checkout of the experimental equipment at MSFC facilities prior to engine test runs.

All tests are conducted with the READI electronic assembly completely sealed, and are designed to enable fault isolation to the card module level. Troubleshooting of any faults, however, involves tasks which are outside the scope and purpose of system test. It should also be noted that the preliminary phases of the laboratory test fall under the general category of developmental testing and are not included in the system test procedures discussed here.

B. DESCRIPTION OF SYSTEM TEST

The system laboratory evaluation is organized for individual checkout of each malfunction detector decision logic path, and associated sensor self-check and redundant circuits where provided. Except for the accuracy evaluation of the time delay quantities, all tests are static in nature. The system tests for each malfunction detector decision logic channel and the sequence of execution are briefly described in this section. A detailed step-by-step procedure for each test has been prepared and one test section has been extracted and is included in Appendix F.

1. Basic Function Test

Suitable combinations of simulated transducer signals are manually set at prescribed values and the malfunction indicator (V) and decision (d) conditions are recorded on a 30-channel event recorder, which produces a permanent trace on recorder paper when a signal is present. All other

sensor inputs not contained in the malfunction indicator equation under examination are set at pre-established "normal" values so as not to activate other indicators. This process is repeated for each of six simulated mission phases conditions for testing the decision logic.

2. Component and Informational Redundancy Test

Where component or informational redundancy is provided, additional input signals are generated and the appropriate indicator and decision outputs are again observed.

3. Transducer Self-Check Test

Where applicable, the effectiveness of self-check provisions for validating the incoming transducer signals is also demonstrated. Since the self-check circuits of the experimental READI are designed to detect open or short conditions of the sensor pickoff elements, this test is best performed by physically disconnecting or jumping "sensor" leads directly at the system junction box. The READI events are then observed as a test of the inhibit action of the self-check circuits.

4. Time Delay Test

The various delay times (t1, t2, t3 and t4) incorporated in the experimental READI are tested by generating step functions of the appropriate sensor signals and recording, on an accurate time base, the resulting binary trace of the associated malfunction indicator.

5. Decision Priority Logic Tests

The decision logic circuits are designed to meet the priority of actions (refer to paragraph 5-3.D) established to cover the contingency of multiple engine malfunction effects. However, the logic circuits are arranged so that only a selected number of malfunction indicators (V's) need be simultaneously activated to test proper operation of the entire priority function. This test is conducted for each mission phase.

C. TEST EQUIPMENT

All equipments used in system test are interconnected through the junction box supplied for the H-1 test stand installation. This wiring arrangement was selected so that a single, compatible set of test equipment and procedures can be used for both laboratory and engine test stand checkout. A block diagram depicting the functional interconnection of the READI electronics assembly, junction box, and test equipment is shown in figure 5-40.

The oscillators and frequency counter are commercial test equipment normally available in most electronic laboratory facilities. The simulator, shown in figure 5-40, is a special test set designed for the experimental READI and is fully described in the following paragraph. The binary event recorder used in the tests at Sperry is a 30-channel Sanborn model 361, shown in figure 5-41. It is a relatively new development in measuring equipment and produces a permanent trace on recorder paper by means of fixed electric stylis, when a preselected event occurs. The recorder includes the necessary buffer switching between the low-level (1.25 volts) Fairchild microelectronic elements used in READI and the high-voltage stylus in the recorder. Both the simulator and event recorder are portable units which eases the task of setting up system tests at remote engine test facilities.

D. TRANSDUCER SIGNAL SIMULATOR

Since a total of 17 transducers of a variety of types are employed in the experimental READI, it is quite cumbersome to simulate the physical quantity which corresponds to each transducer input. Therefore, a simulator was constructed to generate signals which are identical to the range, sensitivity, and other transducer output characteristics.

Functionally, the simulator is a static device, i.e., the value of each sensed variable is manually adjusted to a desired value. For the 11 pressure and temperature transducers to be simulated, separate, independently operated circuits are provided. A potentiometer, referenced to the input variable by means of a calibrated dial, is provided in each circuit. For the variable reluctance and strain gage pressure sensors, bridge networks are used to isolate the output from ground. Bridge excitation is supplied from a 20-volt, 3-kc static inverter by way of an isolation transformer in the READI electronics unit. In the potentiometer pressure transducers ($P9_1$, $P9_2$) a simple voltage divider circuit, excited from a 5-volt dc zener regulated supply, is provided with one side connected to ground. The signals generated for the T6 and T10 thermocouples are low millivolt levels isolated from ground. Small, dry cell batteries are used as the voltage sources.

The vibration, flow, and rpm transducers (total of 6) require simulation of frequency as well as amplitude, thereby dictating the need for variable oscillators. As a practical matter, it is desirable that this bulky commercial test equipment be minimized and physically separated from

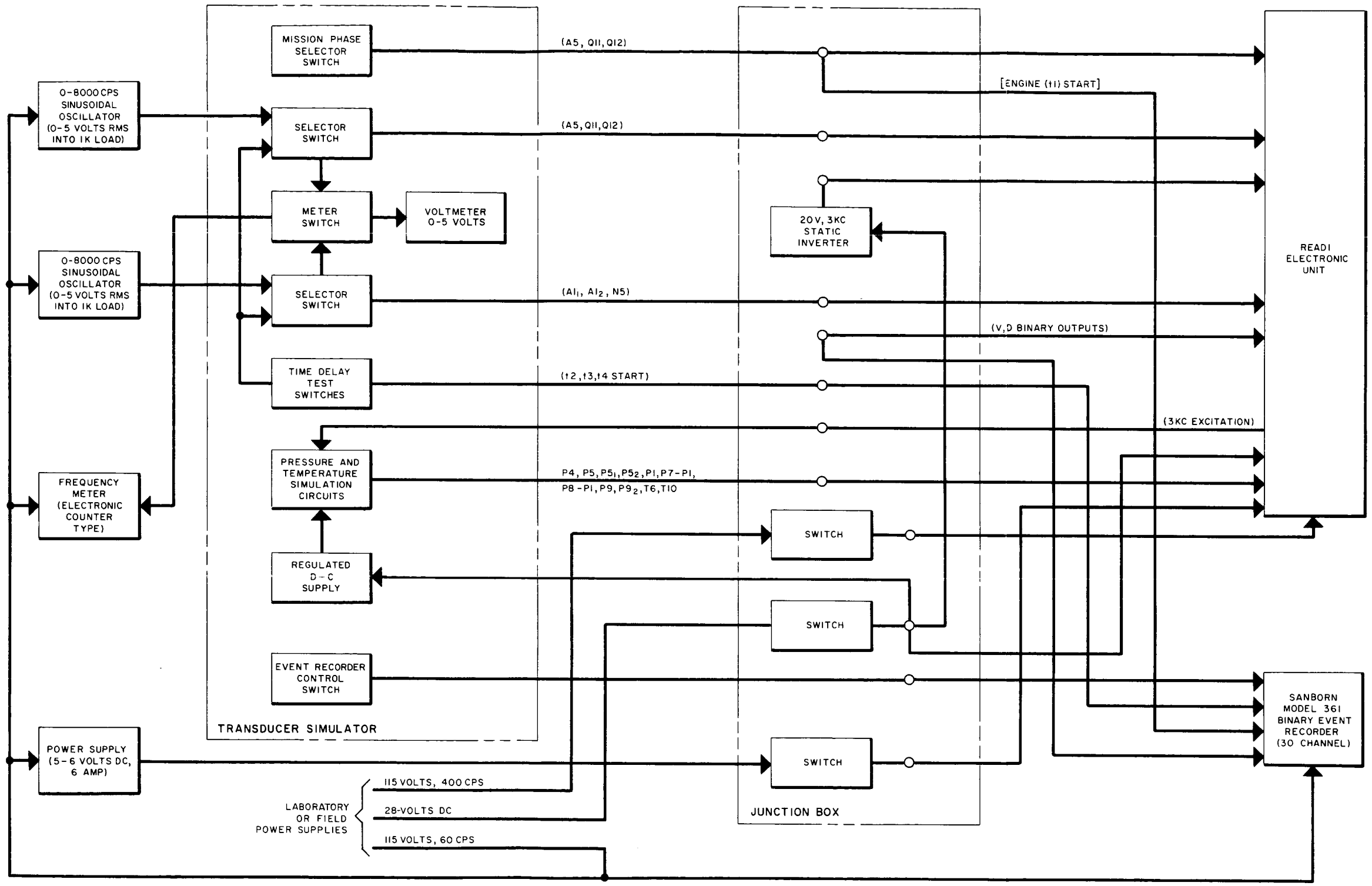


FIGURE 5-40
SYSTEM TEST BLOCK DIAGRAM

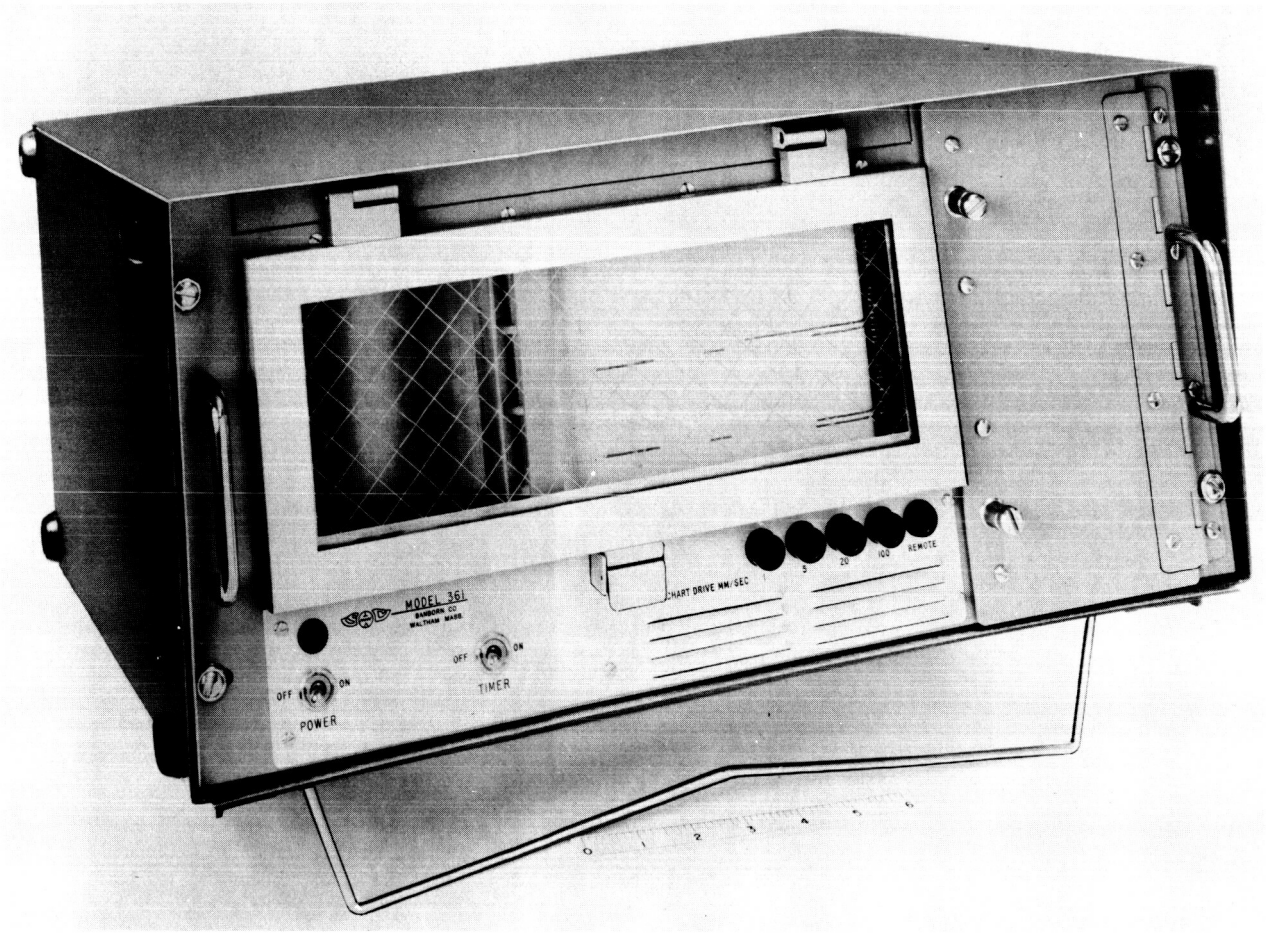


FIGURE 5-41
THIRTY-CHANNEL BINARY EVENT RECORDER, SANBORN MODEL 361

the portable simulator unit. The accomplishment of this objective is aided by the fact that an oscillator can be shared among the frequency sensitive signals, because the absence of any one such signal (i.e., zero frequency) is interpreted as a "normal" engine condition by the non-related malfunction detector channels. For the experimental READI, two oscillators are required to fulfill all the functional test requirements. These oscillators are shared over the 6 required channels by means of two selector switches as follows:

Oscillator No. 1 (0 - 8 kc range)

Main chamber vibration (A1.1-1)

Main chamber vibration (A1.1-2)

Turbine speed (N5)

Oscillator No. 2 (0-600 cps range)

Turbopump vibration (A5)

Fuel flow (Q11)

Lox flow (Q12)

The amplitude and frequency settings for all six variables are made with reference to a voltmeter installed on the simulator panel and a remote frequency meter. These meters are shared between the two oscillators, and are used in conjunction with the charts included in Appendix F which correlate the value of each variable to voltage and frequency units.

In addition to simulating transducer signals, the simulator test set includes the necessary switching to:

- Generate +2-volt dc mission phase discretes
- Provide +2-volt dc time reference signals to checkout the delay timers
- Provide remote control of event recorder.

Physically, the simulator is a portable unit measuring 19-inches wide, 14-inches high, and 8-inches deep, and weighs 10 1/2 pounds. The unit, as shown in figure 5-42, is comprised of a case enclosure and a front panel on which all potentiometer adjustment knobs, meters, switches, circuit assemblies, and connectors are mounted.

5-5. PRELIMINARY ENGINE TEST PLAN FOR EXPERIMENTAL SYSTEM

A. TEST OBJECTIVES

The objectives of evaluating the experimental READI on an operating engine may be summarized as follows:

- Demonstrate that the READI System causes no false alarms on a normally operating engine
- Demonstrate that READI leads to the correct remedial action when malfunctions occur or are simulated
- Show that transducer and cabling failures cause no false alarms
- Solve the practical problems associated with the installation of such a system and demonstrate compatibility of the engine and READI Systems.

B. TEST TECHNIQUES

The plan to test the experimental READI is directed to the attainment of the above objectives. There are a number of test techniques which can be employed in engine tests of the READI System. Three basic techniques are noted below which follows.

- Signal monitoring tests where the output engine malfunction indications, self checks, and decisions of READI are monitored during routine H-1 engine tests. This procedure shows the immunity of the equipment to false alarms, and demonstrates equipment compatibility between analyzer and engine.
- Signal modification tests where a selected group of signals associated with a malfunction are modified so that it appears to READI that, depending upon the modification, either an engine malfunction has occurred, or a transducer failure has occurred. This procedure demonstrates the correct alarm characteristics of the READI system, as well as the resistance to false alarms.
- Engine malfunction tests in which selected malfunctions of a non-destructive nature are induced in the engine.

C. TEST PROCEDURE

The approximate number of partial duration engine runs required to satisfy the objectives set forth in the previous paragraph is given below for four test phases.

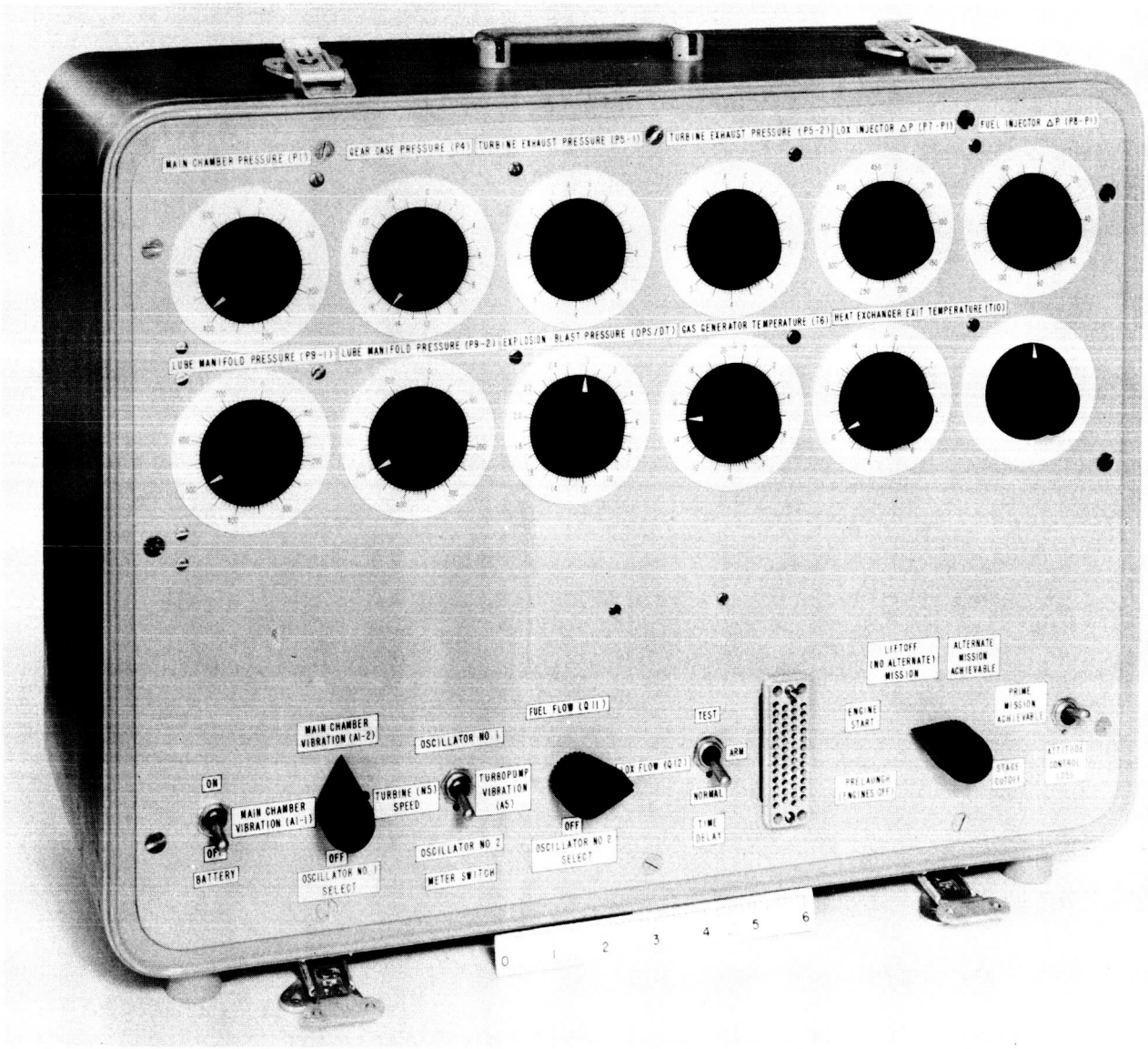


FIGURE 5-42
TRANSDUCER SIMULATOR (HINGED COVER REMOVED)

- Phase 1 - Signal Monitoring Tests - 10 runs
- Phase 2 - Signal Modification Tests - 6 runs
- Phase 3 - Engine Malfunction Tests - 10 runs
- Phase 4 - Signal Monitoring, Closed Loop - (see text)

The first three phases of test will extend over a period of approximately three months. Normal engine test schedules can be maintained during the signal monitoring and signal modification tests because it is not necessary to interfere in any way with the normal procedures. The fourth phase, signal monitoring closed loop, is reached after the equipment has satisfactorily completed the first three phases. It is planned in phase 4 to leave the READI System on the engine test stand for use as a test stand safety system for an extended period of time.

Further details of the phases in engine test are given below.

1. Phase 1, Signal Monitoring Tests

Signal monitoring tests are a necessary prelude to any of the other tests. During these tests the basic compatability of equipment and signals will be established. False alarms and other equipment shortcomings will be corrected. The normal engine start and shutdown transients will supply most of the data needed to demonstrate compatability between the input signal quantities, such as chamber pressure, and the READI transducers and circuitry. If only a short series of engine runs is monitored, the chance of an engine malfunction occurring is small, and such a test series cannot be counted upon to prove out the correct alarm characteristics of the equipment. These tests would initially be run open loop. However, after initial adjustments in the READI equipment are verified, the shutdown decision could be implemented.

2. Phase 2, Signal Modification Tests

The next step is to introduce simulated malfunctions into the test procedure by modifying the output of selected transducers on the engine. A particular malfunction is selected and the transducer outputs, which are initially affected by the malfunction, are examined. The output of the selected transducers is then modified during engine operation, by off-setting the signal or changing the scale factor of the signal, to make it appear that an engine malfunction has occurred. Thus, the normal dynamic content of the signal is preserved. All of the other signals which are initially

Table 5-6

Experimental H-I Readi System Transducers

VARIABLE	DESIGNATION AND LOCATION	FULL RANGE OF TRANSDUCER	CRITICAL RANGE	TRANSDUCER ACCURACY*	TRANSDUCER TYPE SELECTED	TRANSDUCER IMPEDANCE		EXCITATION	OUTPUT SCALE FACTOR	SELECTED VENDER	REMARKS
						INPUT	OUTPUT				
PRESSURE	P1, MAIN CHAMBER	0 TO 650 PSIA	420 TO 650 PSIA	±3%	4 ACTIVE ARM WIRE STRAIN GAUGE	350Ω	350Ω	10 VAC.	30 MV AT 650 PSIA	TABER	
	P7-P1, LOX INJECTOR ΔP	-50 TO +450 PSID	80 TO 150 PSID	±2%	4 ACTIVE ARM SEMICONDUCTOR STRAIN GAUGE	350Ω	250Ω	10 VAC.	150 MV AT 150 PSID	GULTON	
	P8-P1, FUEL INJECTOR ΔP	0 TO 170 PSID	80 TO 150 PSID	±2%	4 ACTIVE ARM SEMICONDUCTOR STRAIN GAUGE	350Ω	250Ω	10 VAC.	350 MV AT 150 PSID	GULTON	
	P9, LUBE MANIFOLD	0 TO 740 PSIA	380 TO 740 PSIA	±5%	POTENTIOMETER	2K	-	2 VDC	2V AT 740 PSIA	SERVONIC	REDUNDANT, "AND" LOGIC
	P5, TURBINE EXHAUST	0-8 PSIG	0 TO 6 PSIG	±5%	2 COIL, VARIABLE RELUCTANCE	500Ω	-	10 VAC 3 KC	750 MV AT 6 PSIG	CONSOLIDATED CONTROLS (ULTRADYNE)	REDUNDANT, "AND" LOGIC
	P4, GEAR CASE	0-25 PSIG	5 TO 20 PSIG	±5%	2 COIL, VARIABLE RELUCTANCE	500Ω	-	10 VAC 3 KC	500 MV AT 25 PSIG	WIANCKO	
	$\frac{dPS}{dT}$, EXPLOSION (BLAST PRESSURE)	±2.5 PSID	±2.5 PSID	±5%	2 COIL, VARIABLE RELUCTANCE	500Ω	-	10 VAC 3 KC	500 MV AT 2.5 PSIG	WIANCKO	
TEMPERATURE	T6, GAS GENERATOR	0 TO 2000°F	1200 TO 2000°F	±3%	CHROMEL/ALUMEL THERMOCOUPLE	-	-	NONE	44 MV AT 2000°F WITH 0°F C.J.		THERMOCOUPLES FOR T6, T10 SUPPLIED BY M-TEST
	T10, HEAT EXCHANGER EXIT	0 TO 1500°F	600 TO 1300°F	±3%	CHROMEL/ALUMEL THERMOCOUPLE	-	-	NONE	33 MV WITH 0°F C.J.		
VIBRATION	A1, MAIN CHAMBER	0 TO 200 GRMS 600 CPS TO 8 KC	80 TO 120 GRMS 900 CPS TO 6 KC	±7%	VELOCITY TYPE MAGNETIC PICKUP	-	-	NONE	60 MV/IN/SEC	SPERRY	REDUNDANT "OR" LOGIC
	A5, TURBOPUMP	0-100 GRMS 0 TO 600 CPS	30 TO 60 GRMS 60 AND 500 CPS	±7%	VELOCITY TYPE MAGNETIC PICKUP	-	-	NONE	60 MV/IN/SEC	SPERRY	
ROTARY SPEED	N5, TURBINE SPEED	0 TO 50,000 RPM	18,000 TO 50,000 RPM	-	PULSE PICKUP	-	-	NONE	3140 CPS AT 100% SPEED	(ON ENGINE)	PRESENT ENGINE MOUNTED TRANSDUCER.
PROPELLANT FLOW	Q11, FUEL FLOW	0-2200 GPM	1200 TO 2000 GPM	±0.5%	TURBINE MOTOR PULSE RATE OUTPUT	-	-	NONE	180 CPS AT 100% THRUST	(ON TEST STAND)	FLOWMETERS ARE PRESENTLY INSTALLED IN THE ENGINE TEST STAND
	Q12, LOX FLOW	0-3500 GPM	1800 TO 3200 GPM	±0.5%		-	-	NONE	240 CPS AT 100% THRUST	(ON TEST STAND)	

*% OF MAX VALUE IN CRITICAL RANGE

unaffected by the malfunction are taken from engine mounted transducers with no modification.

In a similar manner, selected transducers may be caused to fail during an engine run to demonstrate the immunity of the READI equipment to false alarms. For example, this can be accomplished by abruptly removing the excitation voltage to one of the pressure transducers while the engine is running.

Since malfunction conditions that do not exist are being simulated, the signal modification tests would be run open loop to avoid interrupting the engine run.

3. Phase 3, Engine Malfunction Tests

The best way to demonstrate the performance of the READI system is to induce or simulate malfunctions in the engine. Table 5-7 indicates some of the malfunctions which might be induced or simulated without serious hazard. Also shown is the proposed test method and the malfunction identification affected. This type of testing has the additional advantage of gaining more information on the off-design performance of the engine. It has the disadvantage of increasing the hazard to the engine and test stand. However, this hazard should be small, because of the elaborate safety monitoring provisions normally used in engine tests. Since the procedure of inducing some malfunctions in liquid rocket engines is an established developmental test technique, it may be possible to take advantage of malfunction testing already scheduled for the H-1 engine.

Table 5-7

EXPERIMENTAL READI SYSTEM EVALUATION, H-1 ENGINE TEST, ENGINE MALFUNCTION TEST PROGRAM

Engine Malfunction Induced or Simulated	Test Method	Signal Space Separation* Affected
1. Combustion instability	Discharge small explosive charge in combustion chamber	V1.1.1

*Reference table 5-6.

Table 5-7 (Cont)

EXPERIMENTAL READI SYSTEM EVALUATION, H-1 ENGINE TEST, ENGINE MALFUNCTION TEST PROGRAM

Engine Malfunction Induced or Simulated	Test Method	Signal Space Separation* Affected
2. Main propellant line rupture, pump cavitation, propellant depletion	Restrict or bypass lox and/or fuel inlet lines between engine and pre-valves	V2.2.1 followed by V2.1.1 and V2.1.2 depending on degree of bypass. V4.1.1, V5.1.1, V7.1.1, V7.1.2, V8.1.1, V8.1.2
3. High pressure propellant line rupture	Restrict or bypass lox and/or fuel flow downstream of pump	Same group of V's as group 3
4. Bootstrap line or control pressure line rupture, gas generator valve failed closed	Restrict or bypass lox and/or fuel bootstrap flow	V3.1.1 V2.2.1, 2.1.1, 2.1.2 V4.1.1

*Reference table 5-6

4. Phase 4, Closed Loop Testing

Once the preliminary phases of READI engine evaluation have been completed, the output shutdown decision can be connected through a suitable buffer to the main lox valve closing control valve on the H-1 engine. The pre-valve shutdown can also be connected by appropriate wiring to the pilot stages of the test stand mounted pre-valves. Such a closed loop arrangement would be advantageous when engine malfunctions are induced, as described previously. Also, if the READI can be left in place on the test stand for several months and transducer connections made to each engine, the chance of detecting malfunctions is quite good. In this case it would be desirable to hook up READI closed loop to demonstrate the READI capability to limit the effects of the malfunctions. However, for any closed loop tests it is necessary for the comparator limits in READI to be compatible with the "red line" limits used by test control personnel. Some READI processing channels are, for instance, setup to duplicate exactly the reaction of the ground test personnel, when an engine malfunction occurs. An example is gas generator temperature (Conisphere temperature, M-Test Measurement Number 16.01) where the red line is 1400°F steady state. A decision must be made as to whether the READI limit (V3.1.1) should be set just below, above, or right at the 1400°F level.

D. ENGINE TEST STAND INSTALLATION

One of the prime objectives in the packaging and interconnection design of the experimented READI System was to achieve a flexibility which will enable extensive changes in test arrangements and procedures without modifying the equipment. Through the use of a central junction panel, shown in figures 5-43 and 5-44, and addition of spare wires in each cable, the means are provided with a minimum of time-consuming rewiring effort, to

- adapt the experimental equipment to any rocket engine installation
- modify the experimental equipment to accomodate functional changes, such as the additon or substitution of transducers.

The use of a terminal box also reduces the number of individual cables and connectors required. In addition, a greater interconnection compatibility is provided between the simulator unit and the electronic unit under both laboratory and engine test stand conditions.

Provisions are made to record all the raw transducer data in addition to the discrete event outputs from READI. The number of signals to be recorded for a particular run will depend upon the test objectives and availability of recording channels, as well as the cabling between the test stand and the block house where the recorders are located.

A block diagram of the recommended engine test set-up is shown in figure 5-45. The binary outputs from READI will be recorded on a fixed stylus, 30-channel event recorder, as in the lab demonstration. This recorder will be supplied by Sperry. The analog transducer data will be used to correlate malfunction logic comparator settings, and troubleshoot the system after an engine run. This data will be recorded on the standard oscillographs available in the block house. The addition, approximately 7 transistor-actuated lights at the signal simulator panel are also contemplated so as to indicate more clearly the presence of anticipated malfunction and decision event outputs of READI.

The tentative engine test stand location selected for the electronic assembly unit is above the engine, on or near the thrust plate. The location of the junction box is undetermined at this time; easy accessibility should be provided, however, to enable voltage measurements and system wiring changes. Outline drawings for the electronic unit and junction box are shown in figures 5-46 and 5-47 respectively.

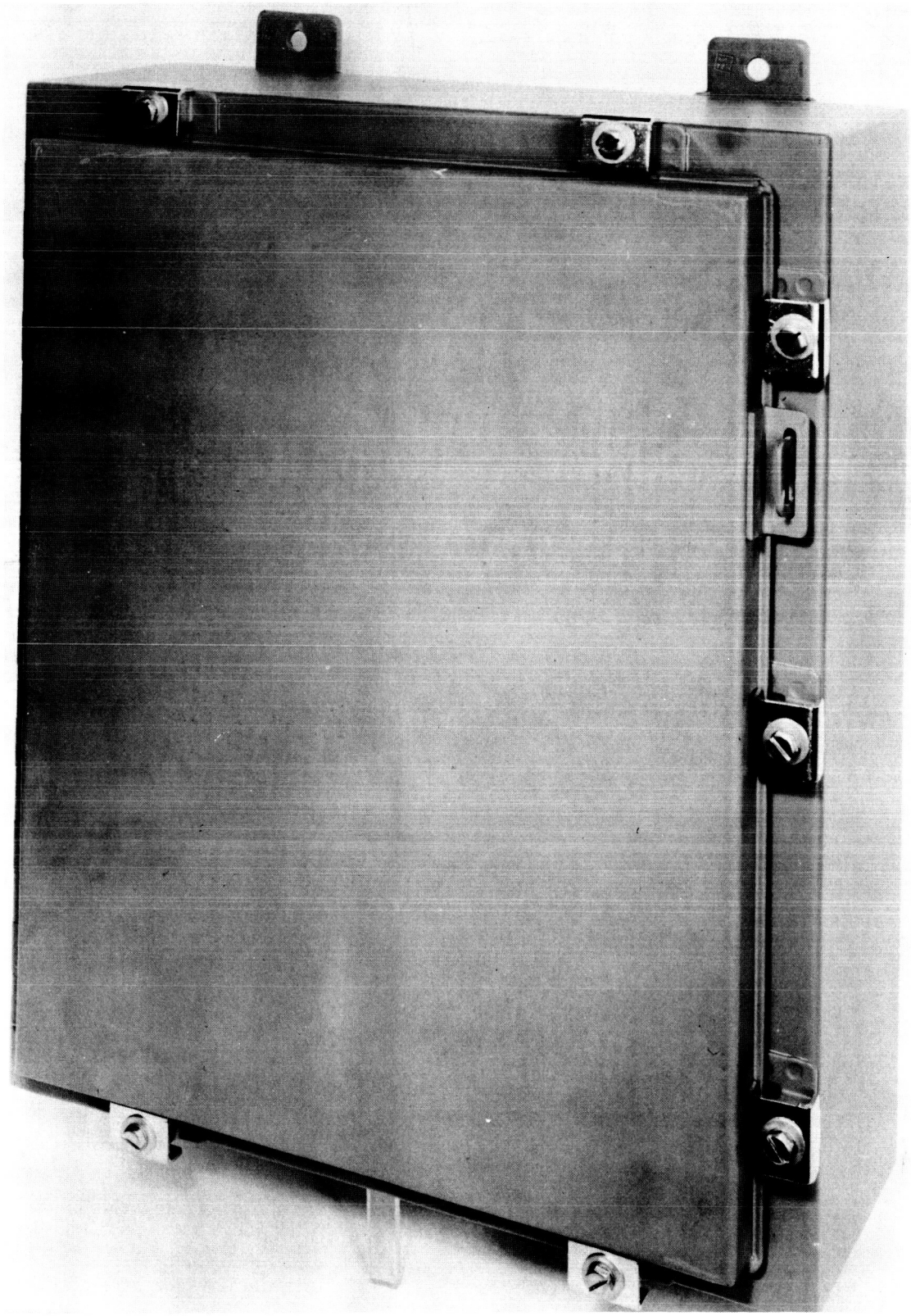


FIGURE 5-43
SYSTEM JUNCTION BOX (CLOSED)

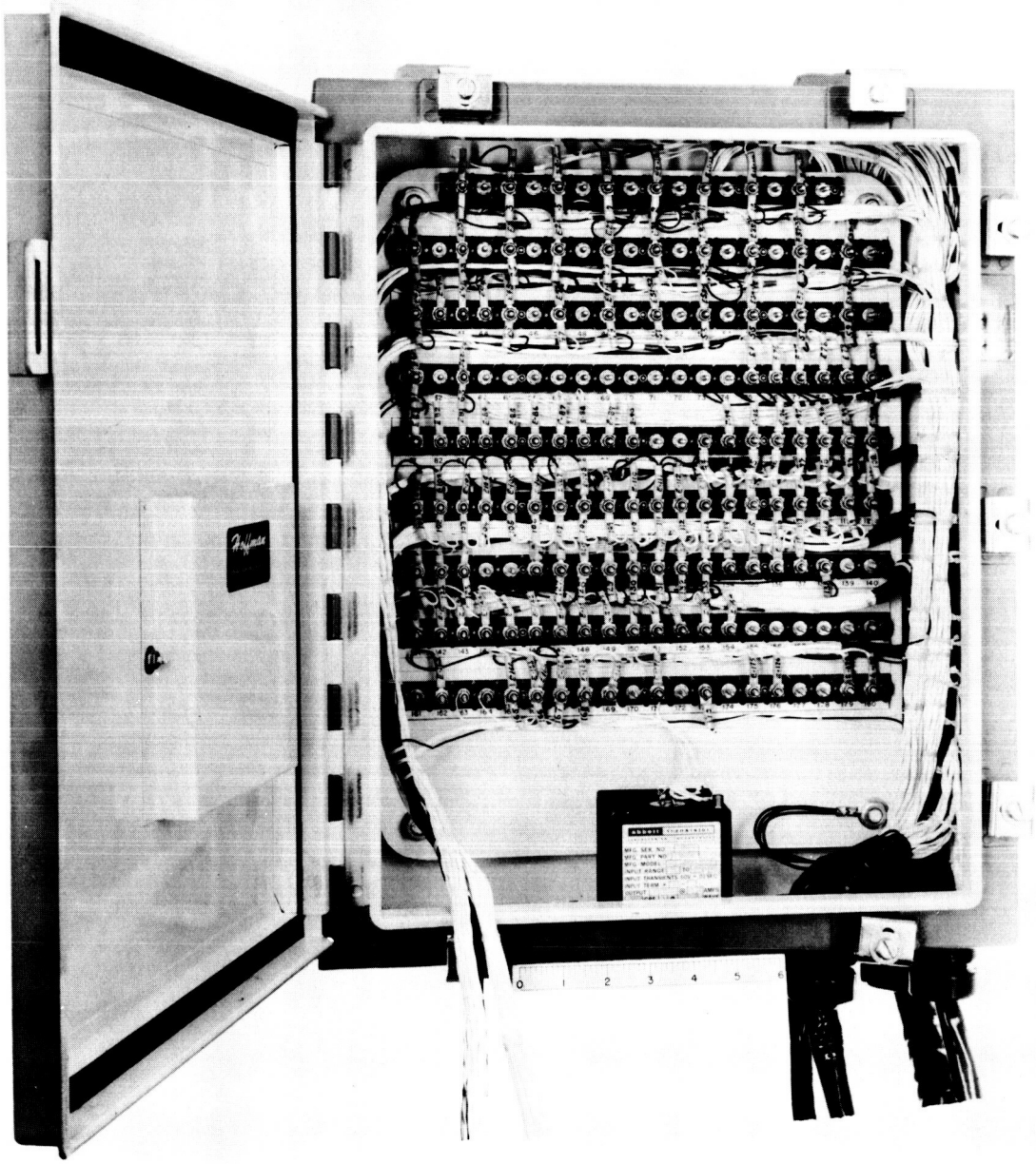


FIGURE 5-44
SYSTEM JUNCTION BOX, OPEN VIEW OF TERMINAL BOARD PANEL

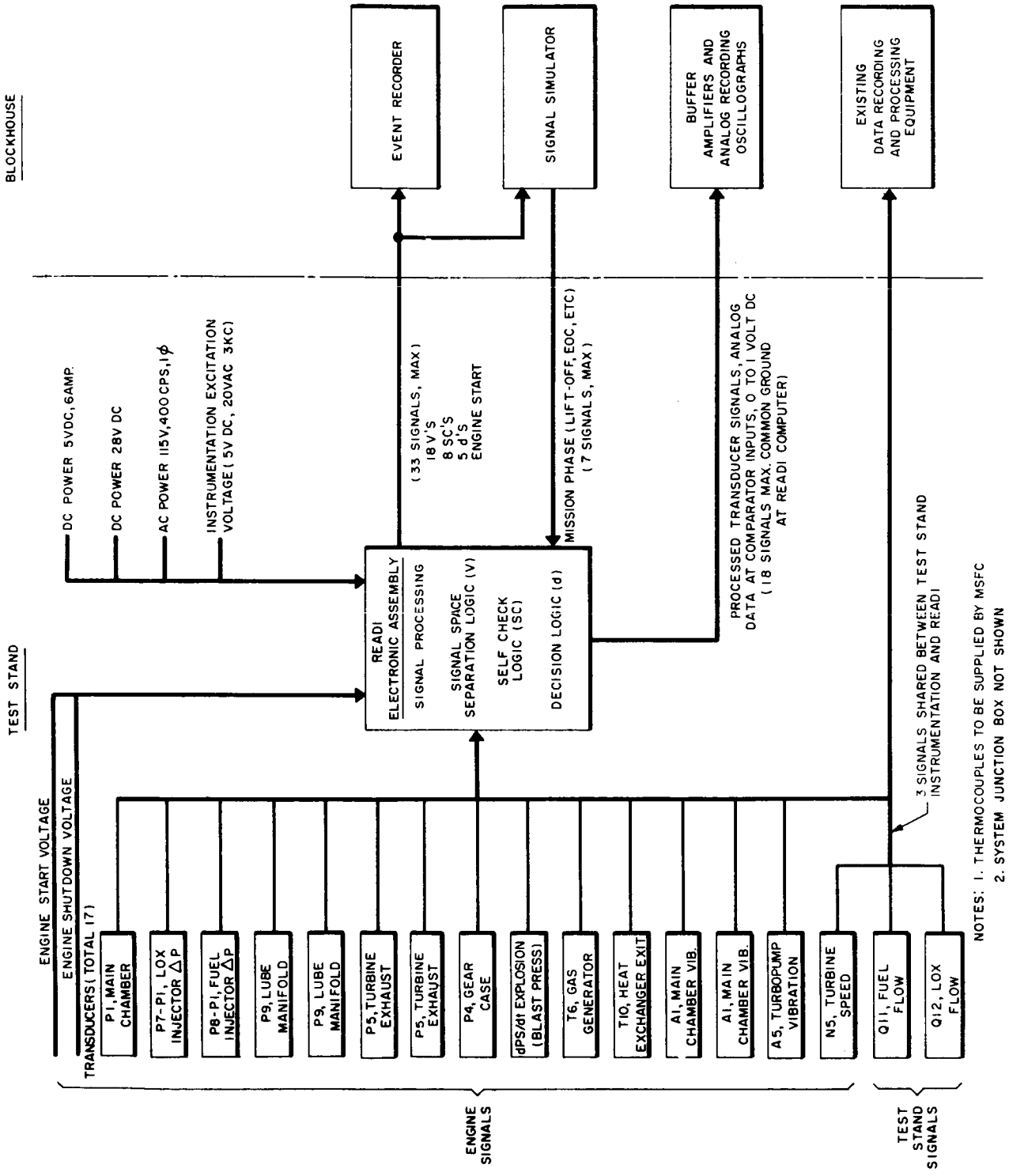


FIGURE 5-45
ENGINE TEST SET-UP FOR READI EVALUATION

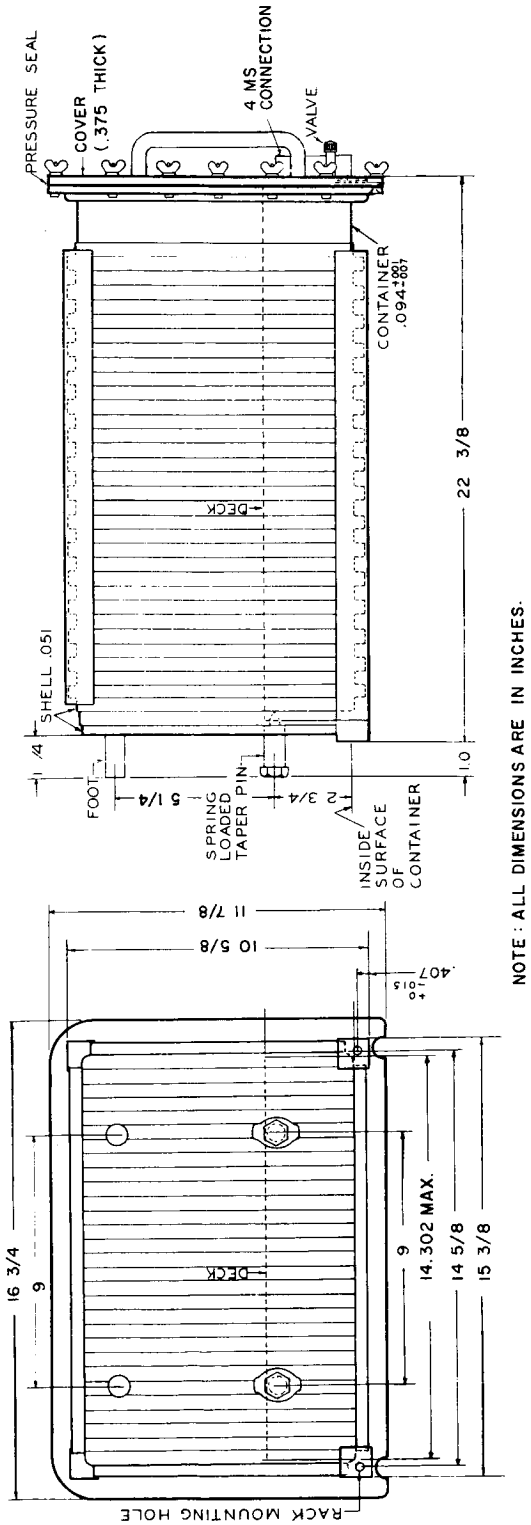


FIGURE 5-46
ELECTRONIC ASSEMBLY UNIT FOR EXPERIMENTAL READI, OUTLINE DRAWING

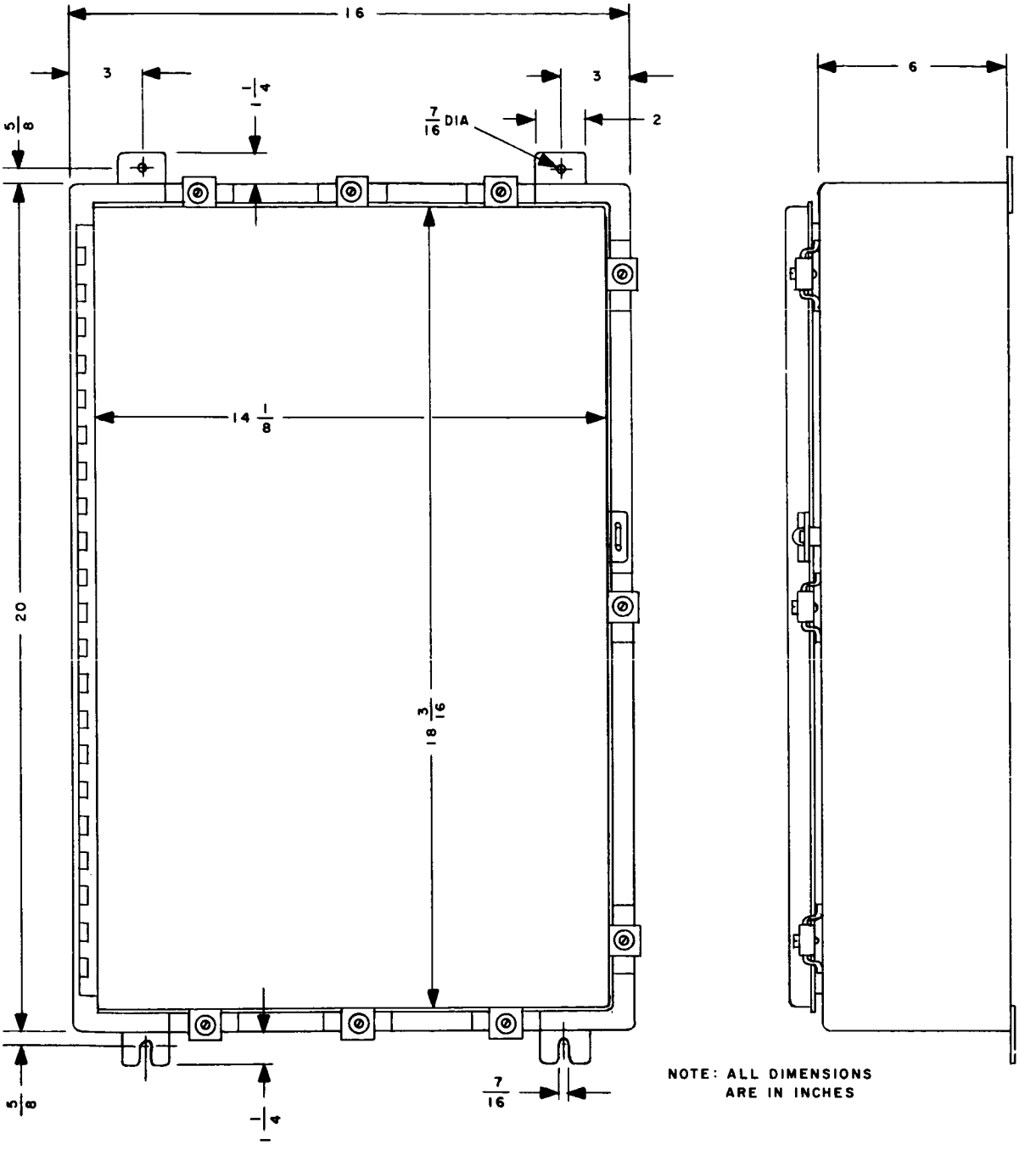


FIGURE 5-47
SYSTEM JUNCTION BOX, OUTLINE DRAWING

SECTION VI

CONCLUSIONS AND RECOMMENDATIONS

The accomplishments of the READI investigation to date can be summarized as follows:

1. The general concept of a Rocket Engine Analyzer and Decision System has been defined.
2. The physical and functional characteristics of a typical system have been determined.
3. The input data on the engine, vehicle, mission, and transducers necessary for the design and evaluation of a READI system have been identified.
4. A practical synthesis procedure for the design of the optimum system from a given set of input data has been devised.
5. Application of READI to a hypothetical but realistic engine-vehicle-mission model has demonstrated that the cost of the system is easily justified by improvement in mission safety and reliability.
6. Special information redundancy and self-check techniques that allow the system to tolerate the more likely transducer failures without false alarm have been devised.
7. Linear and digital information processing circuits suitable for construction in integrated microcircuit form have been developed.
8. An experimental system suitable for testing on the H-1 engine has been developed using the above circuits.

9. Bench tests of the experimental system have demonstrated the performance of the signal processing and logic circuits of the system and the value of the special self-check provisions.

It is recommended that the experimental system now be tested on an available H-1 engine. The objectives of this test program should be to:

1. Demonstrate that the READI system causes no false alarms on a normally operating engine.
2. Demonstrate that READI leads to the correct remedial action when malfunctions occur or are simulated.
3. Show that transducer and cabling failures cause no false alarms.
4. Solve the practical problems associated with the installation of such a system and demonstrate the compatibility of the engine and READI systems.

In addition, it is recommended that the building block signal processing and logic circuits developed in breadboard form be refined into packaged units taking full advantage of presently available microcircuitry. This will substantially reduce the lead time required to make READI available for a particular space vehicle.

APPENDIX A

RISK CALCULATION FOR STAGE END STATE

Design, evaluation, and optimization of a READI system for a particular vehicle, stage, or mission phase requires knowledge of the relative desirability of attaining each of the possible end states of that vehicle or mission stage. A quantity is defined to express this "relative desirability" and a procedure is presented to calculate the quantity.

A-1. DIMENSIONS OF RISK VECTOR

To accomplish a space mission, resources of various kinds must be allocated. When the vehicle is launched it has been determined that the scientific, political, or military value of the results are at least equal to the expected expenditure of resources. If the mission fails another vehicle must be launched to accomplish the mission objectives. The expected or average cost of the mission must include a risk component to allow for this possibility of failure.

The resources expended or risked can be of several types, and any given mission will result in different ratios of expenditure of these resources. This expenditure can be represented by an n dimensional loss vector for which each of the dimensions represents one type of resouce. A typical loss vector suitable for a manned mission, with partially recoverable booster, might have three dimensions:

$$\underline{L} = \begin{vmatrix} L_v \\ L_m \\ L_c \end{vmatrix}$$

where L_v is vehicle loss which includes various equipment and launch costs which are conveniently measurable in dollars. L_m includes mission-type losses including relative worth of alternate missions, and L_c includes crew losses and other risks to human life, if any (i.e., rescue missions, explosions near the pad, etc). Units used to express these losses can be arbitrarily selected. In the READI analysis, a value of unity has been assigned to the total vehicle and mission loss, and fractional values have been assigned to express less than total loss.

Likewise, a risk vector can be defined as the expected loss at a particular time in the mission.

$$\underline{R} = \left\{ \underline{p} \ (\underline{L}) \right\}^T \ \underline{L}$$

This vector expresses the risk or expected loss for the remaining part of the mission and, when evaluated at the start, it is, by definition, the expected or average cost of the mission in each of the n resources.

A-2. RISK SCALAR

The design criterion for a READI system has been chosen as the minimization of the average expenditure of resources. Since the minimization can only be performed on a scalar quantity, a scalar quantity, R, called the risk factor is defined as follows:

$$R = \underline{k}^T \ \underline{R}$$

$$= k_1 \ R_v + k_2 \ R_m + k_3 \ R_c \qquad \text{(A-1)}$$

This factor is the weighted sum of the components of risk.

Since the components of risk have rather diverse dimensions, some thought must be given to the assignment of the weighting factors so that the resulting READI system most nearly satisfies the overall design objectives. There are certain relationships that must be fulfilled in doing this. It can be said that the loss of the mission results is equal to the replacement value of the mission, which is equal to risk factor, R, evaluated at the start of the mission.

$$R_o = k_2 \ (\text{for } L_m = 1) \qquad \text{(A-2)}$$

The weighting value for crew risk is the most difficult factor to select, since the crew risk acceptable is somewhat a function of the nature of the mission and cannot be directly equated to the other terms in the risk expression. The best that can be done is to bracket its value based on observations of current practice and to select a value that results in similar orders of magnitude for $k_2 R_m$ and $k_3 R_c$ so that READI design considers both mission success and crew safety. It is convenient in doing this to establish the value of k_3 in terms of its ratio to k_2 by a constant, λ_c, which shall be called the crew mission value ratio.

$$k_3 = \lambda_c k_2 \qquad \text{(A-3)}$$

combining equations (A-1), (A-2), and (A-3) yields

$$R = k_1 R_v + R_o R_m + \lambda_c R_o R_c$$

Evaluating all risks at the start of the mission and substituting the cost of the vehicle in dollars for k_1, produces an expression for the average cost of the mission

$$C_{avg} = \frac{C_v \; R_v}{1 - R_m - \lambda R_c}$$

A-3. EVALUATION OF THE RISK VECTOR

The risk vector can be evaluated at any stage in the mission by the following procedure. The mission is first subdivided into a number of convenient stages or phases, and at the end of each stage a set of possible states are defined. For this purpose, regions of continuous state space that can be treated the same in all important respects are considered a discrete state.

Then, for all phases of the mission subsequent to the one under study, the probabilities are estimated for transitions from states of one stage to states of the next. These probabilities can be expressed in matrix form:

$$|T(n)| = \begin{array}{c} \\ \\ i \end{array} \begin{vmatrix} t_{11} & t_{12} & \cdot \\ t_{21} & \cdot & \cdot \\ \cdot & \cdot & t_{ij} \end{vmatrix}$$

where t_{ij} is the probability of a transition from state i at the end of stage n-1 to state j at the end of stage n.

Losses are also associated with each stage state.

$$|\underline{L}(n)| = \begin{vmatrix} \underline{l}_1 \\ \underline{l}_2 \\ \underline{l}_3 \\ \\ \underline{l}_i \end{vmatrix}$$

where $\underline{l}_i$ are the loss vectors incurred at any state j at the end of stage n.

The recursion equation for finding the risk at the end of a stage from the losses and risks of the succeeding stage is

$$\underline{R}(n) = |T(n+1)| \ \underline{R}(n+1) + \underline{L}(n)$$

and the risk at stage n of an N stage mission is

$$\underline{R}(n) = (\underline{L}(n) + (|T(n+1)| \ \underline{L}(n+1)) + \ldots$$

$$(|T(n+1)| \ |T(n+2)| \ \text{----} \ |T(n)| \ \underline{L}(N))$$

APPENDIX B

COMPUTATION OF STAGE TRANSITION PROBABILITIES

B-1. INTRODUCTION

As described in Section IV, the task of determining a set of probabilities, $P(t_j/m_i\ d_k)$, is central to the READI design concept. These probabilities relate the occurrence of a malfunction, m_i, and decision, d_k, to the jth transition, t_j. The transitions (normal, failed, etc.) connect the initial modes of a given stage with the final end states of that stage.

There are three steps in the determination of $P(t_j/m_i\ d_k)$. The first is the calculation and/or estimation of propulsion system performance parameters for each malfunction/decision pair. These parameters might include

- t^* - time of occurrence of $m_i\ d_k$
- ΔT - percent loss of stage thrust
- $\Delta \dot{m}$ - percent loss of propellant flow overboard
- ΔI_{SP} - percent loss of specific impulse
- $P(CL)$ - probability of catastrophic loss of vehicle and crew.

A tabulation of propulsion system losses is presented in table D-4.

The second step in the determination of $P(t_j/m_i\ d_k)$ is to establish the functional relationship between the propulsion system performance parameters and a set of quantities which measure vehicle performance with respect to mission accomplishment and crew survival. Appropriate quantities might include

$\Delta\bar{S}_{co}$ - decrement in stage cut-off position

$\Delta\bar{V}_{co}$ - decrement in stage cut-off velocity

Δt_{co} - increment in stage cut-off time

P(CL) - probability of catastrophic loss of vehicle and crew.

The third step in computing $P\ (t_j/m_i\ d_k)$ is the definition of acceptable limits on the above parameters for each possible end state. This involves the consideration of the flexibility in succeeding stages and the desired end condition accuracy. An error analysis performed during guidance system design studies would yield much of this data.

The purpose of this appendix is to show how a relationship between transition probabilities and propulsion system performance parameters may be obtained. The numerical results presented are not necessarily representative of a real case. For reasons of expediency, certain simplifying assumptions have been made. These assumptions do not, however, restrict the procedure used - they merely degrade the accuracy of the numerical results presented.

B-2. STAGE TRANSITION PROBABILITIES DERIVATION

The second stage of a typical large booster is considered. It is assumed that cutoff will occur when the propellant supply has been exhausted or at a predetermined time, whichever occurs first. This implies that propellant saved due to engine shutdown cannot be consumed because the mission plan does not allow for an extra burning period. Such a condition might prevail for a rendezvous mission where the guidance mode is not adaptive to an engine-out situation.

The mission plan and vehicle characteristics are assumed to be such that cutoff velocity magnitude is an adequate measure of second stage performance. In general the stage performance would be measured by a set of parameters which would also include at least cut-off time and position. For simplicity, assume that the third stage has the ability to correct for position and time errors as long as the second stage supplies the necessary velocity increment (energy) to the vehicle. This procedure may be extended to provide a multi-dimensional stage performance indicator.

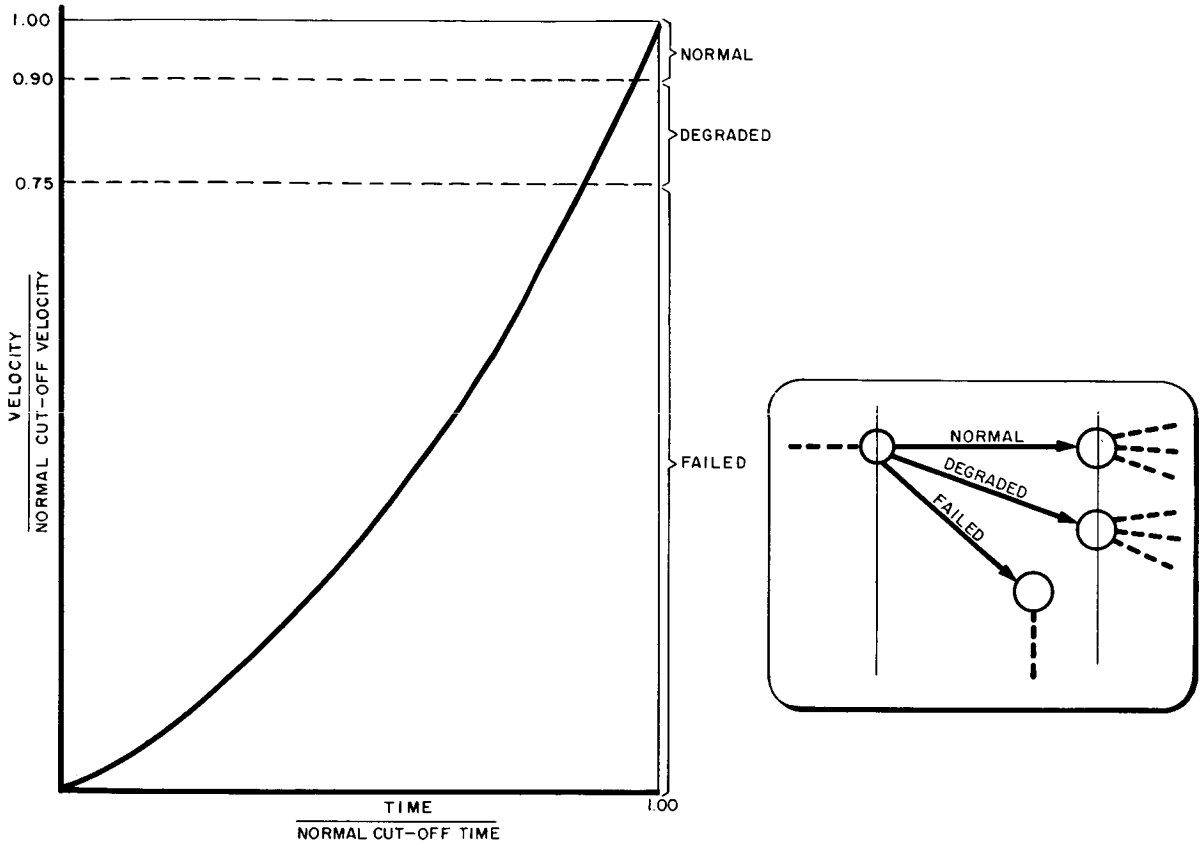


FIGURE B-1
STAGE VELOCITY CHARACTERISTICS

In this example, three transitions are considered. These are defined as shown in figure B-1. One may, in general, hypothesize as many transitional modes as are appropriate to the problem at hand. Factors which influence this selection are:

- Mission flexibility
- Availability of data
- Desired precision.

The cut-off velocity limits used in the definition of the transition were chosen to be:

- Normal - greater than $0.90V_{co_N}$
- Degraded - greater than $0.75V_{co_N}$, and
  - less than $0.90V_{co_N}$
- Failed - less than $0.75\ V_{co_N}$

Finally, it is assumed that the propulsion system failure modes are such that the only parameters which influence cut-off velocity error are ΔT, the change in stage thrust, $\Delta\dot{m}_{ox}$, the change in mass flow rate of oxidizer, and t^*, the time of occurrence of ΔT and $\Delta\dot{m}_{ox}$.

It is assumed that only one malfunction occurs and that t^* may be any time between ignition and cutoff with equal probability. The curves of figure B-2 show graphically the assumptions stated here.

The equations used to describe mathematically the example given above will now be derived. The nomenclature used in the following equations is defined in table B-1.

A. CUT-OFF TIME EQUATIONS

The cut-off time equation is given by

$$t_{co} = \text{minimum}\left[(t_{co_N}).\left[t^* + \frac{m_p - \dot{m}t^*}{\dot{m} + \Delta\dot{m}}\right]\right]$$

$$t_{co_N} = \frac{m_p}{m}$$

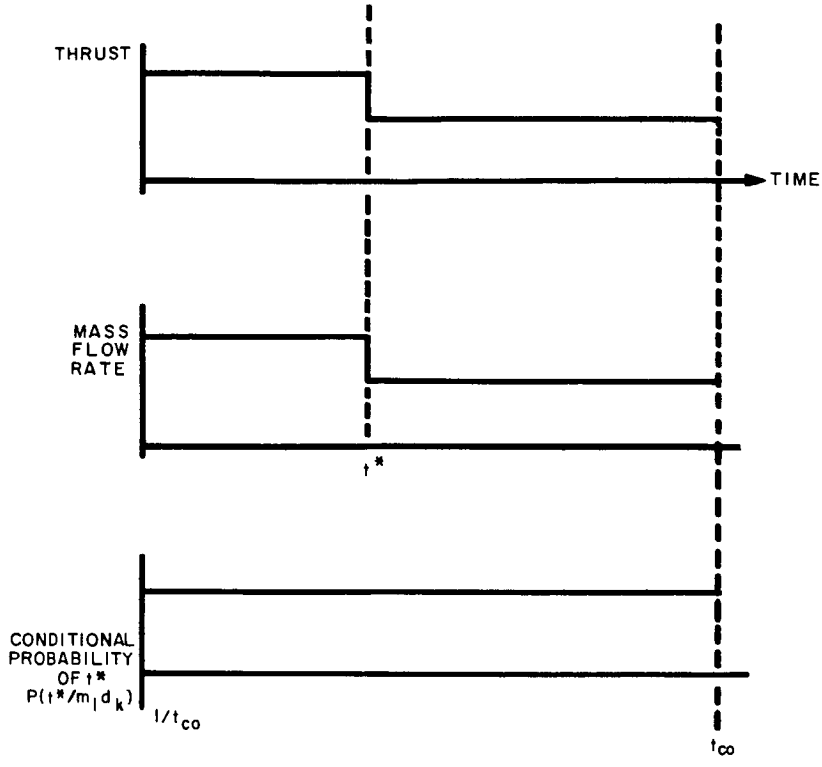


FIGURE B-2
PROPULSION SYSTEM FAILURE MODE PARAMETERS

The resulting error equation in dimensionless form is

$$\frac{\Delta t_{co}}{\Delta t_{co_N}} = 1 - \text{Minimum}\left[1, \frac{1 + \frac{t^*}{t_{co_N}} \quad \frac{\Delta \dot{m}}{m}}{1 + \frac{\Delta \dot{m}}{\dot{m}}}\right]$$

B. VELOCITY EQUATIONS

Newton's 2nd law takes the following form for this example:

$$V_{co} = V_o + \int_o^{t^*} \frac{T}{m_o - \dot{m}\,\xi}\, d\,\xi + \int_{t^*}^{t_{co}} \frac{T + \Delta T}{m_o - \dot{m}t^* - (\dot{m} + \Delta\dot{m})\,(\xi - t^*)}\, d\,\xi$$

$$- g \int_o^{t_{co}} \sin\,[\beta\,(\xi)]\, d\,\xi$$

and

$$V_{co_N} = V_o + \int_o^{t_{co_N}} \frac{T}{m_o - \dot{m}\,\xi}\, d\xi - g \int_{t_{co}}^{t_{co_N}} \sin\left[\beta(\xi)\right] \xi$$

Therefore,

$$\Delta V_{co} = \int_{t*}^{t_{co_N}} \frac{T}{m_o - \dot{m}\,\xi}\, d\xi - \int_{t*}^{t_{co}} \frac{T + \Delta T}{\dot{m} - \dot{m}\, t* - (\dot{m} + \Delta\dot{m})(\xi - t*)}\, d\xi$$

$$- g \int_{t_{co}}^{t_{co_N}} \sin\left[\beta(\xi)\right]\, d\xi$$

For typical second-stage trajectories, it is reasonable to assume that

$$\beta(t) \cong 0 \quad \text{for} \quad t_{co} < t < t_{co_N}$$

The gravity term in the cut-off velocity error equation is therefore zero, and

$$\Delta V_{co} = \int_{t*}^{t_{co_N}} \frac{T}{m_o - \dot{m}\,\xi}\, d\xi - \int_{t*}^{t_{co}} \frac{T + \Delta T}{\dot{m}_o - \dot{m}t* - (\dot{m} + \Delta\dot{m})\,(\xi - t*)}\, d\xi$$

Integrating and nondimensionalizing results in the equation:

$$\frac{\Delta V_{co}}{V_{co_N}} = 1 - \frac{\ln\left[1 - \frac{m_p}{m_o}\cdot\frac{t^*}{t_{co_N}}\right] + \left[\frac{1 + \Delta t/t}{1 + \Delta\dot{m}/\dot{m}}\right]\ln\left[\frac{1 - \frac{m_p}{m_o}\left[\left[1 + \frac{\Delta\dot{m}}{\dot{m}}\right]\left[1 - \frac{\Delta t_{co}}{t_{co_N}}\right]\right] - \frac{\Delta\dot{m}}{\dot{m}}\cdot\frac{t^*}{t_{co_N}}}{1 - \frac{m_p}{m_o}\cdot\frac{t^*}{t_{co_N}}}\right]}{\ln\left[1 - \frac{m_p}{m_o}\right]}$$

For convenience, the gravity term has been omitted in normalizing this equation. A small error results. Introducing the following nondimensional notation:

$$\rho = \frac{m_p}{m_o} \qquad \delta = \frac{\Delta V_{co}}{V_{co_N}}$$

$$\theta = \frac{t^*}{t_{co_N}} \qquad \gamma = \frac{\Delta t}{t_{co_N}}$$

$$\omega = \frac{\Delta\dot{m}}{\dot{m}} \qquad \tau = \frac{\Delta T}{T}$$

The cut-off and velocity equations become, respectively:

$$\gamma = 1 - \text{Minimum}\left[1, \frac{1 + \theta\,\omega}{1 + \omega}\right]$$

$$\delta = 1 - \frac{\ln(1 - \rho\theta) + \left[\frac{1 + \tau}{1 + \omega}\right]\ln\left[\frac{1 - \rho\,[(1 + \omega)(1 - \gamma) - \omega\theta]}{1 - \rho\theta}\right]}{\ln(1 - \rho)}$$

where

θ is the normalized time of malfunction occurrence. τ and ω are normalized thrust change and propellant change parameters, respectively. γ and δ are normalized cut-off errors in time and velocity, respectively, and ρ is the propellant mass ratio for the stage being considered. It is interesting to note that ρ is the only vehicle parameter required by the analysis.

It will be recalled that the probability of occurrence of a malfunction and decision is independent of time, i.e., P (t*) = a constant. Using this assumption, the transition probabilities are defined as follows:

$P(t_o) = 1 - \theta_o$, where ω_o is the time for which the occurrence of a given τ and ω causes a 10-percent velocity degradation

$P(t_1) = \theta_o - \theta_1$, where θ_1 is the time for which the occurrence of a given τ and ω causes a 25-percent velocity degradation

$P(t_2) = \theta_1$

$P(t_o) + P(t_1) + P(t_2) = 1$

B-3. NUMERICAL RESULTS

These foregoing equations have been solved numerically using a digital computer. Results are shown in figure B-3 for the case where the ratio of propellant mass to initial vehicle mass, ρ , equals 0.625. Three different propellant flow losses were considered: 20, 10 and 0 percent.

As expected, the general characteristics of the curves are:

- Probability of normal transition decreases with increasing thrust loss
- Probability of failed transition increases with increasing thrust loss
- Probability of degraded transitions increases and then decreases with increasing thrust loss.

For any given thrust loss and propellant flow loss, the sum of the transition probabilities is equal to one.

For large thrust loss (greater than 50-percent stage thrust), the normal transition probability approaches approximately 0.10. This can be justified through the following reasoning. If all engines are shut down after t_n, when the velocity reaches 90 percent of normal cut-off velocity, then the probability of normal transition would be one. The time between t_n and normal cut-off time is roughly 10 percent of the total stage burning period. Therefore, it would be expected that the asymptotic value of the normal transition probability would be 0.10.

Another expected result may be observed. If one engine was shut down, the thrust loss would be 0.20 and the propellant flow would decrease by 0.20. From the curves of figure B-3, the probability of normal transition equals 0.18. If, instead of terminating flow to the inoperative engine the normal propellant flow is maintained, the probability of normal transition would be 0.38. The reason that the normal situation prevails more often when propellant is "thrown away" is that the simplified cut-off law used does not allow for an extra burning period. There is no advantage to be gained by saving propellant since it can never be used.

Data such as that displayed in figure B-3 is important in designing READI. Without such information it would be impossible to relate propulsion system performance to mission reliability. Various extensions of the analytical procedure described here have been accomplished. At the present time, however, numerical solutions are not available.

Table B-1

Symbols

V_{co} = stage velocity at cutoff

V_{co_N} = stage velocity at normal cut-off time

ΔV_{co} = $V_{co_N} - V_{co}$

t_{co} = time from stage ignition to stage cutoff

t_{co_N} = time from stage ignition to normal stage cutoff

Δt_{co} = $t_{co_N} - t_{co}$

$\dot{m}_{ox}$ = normal mass flow rate of oxidizer

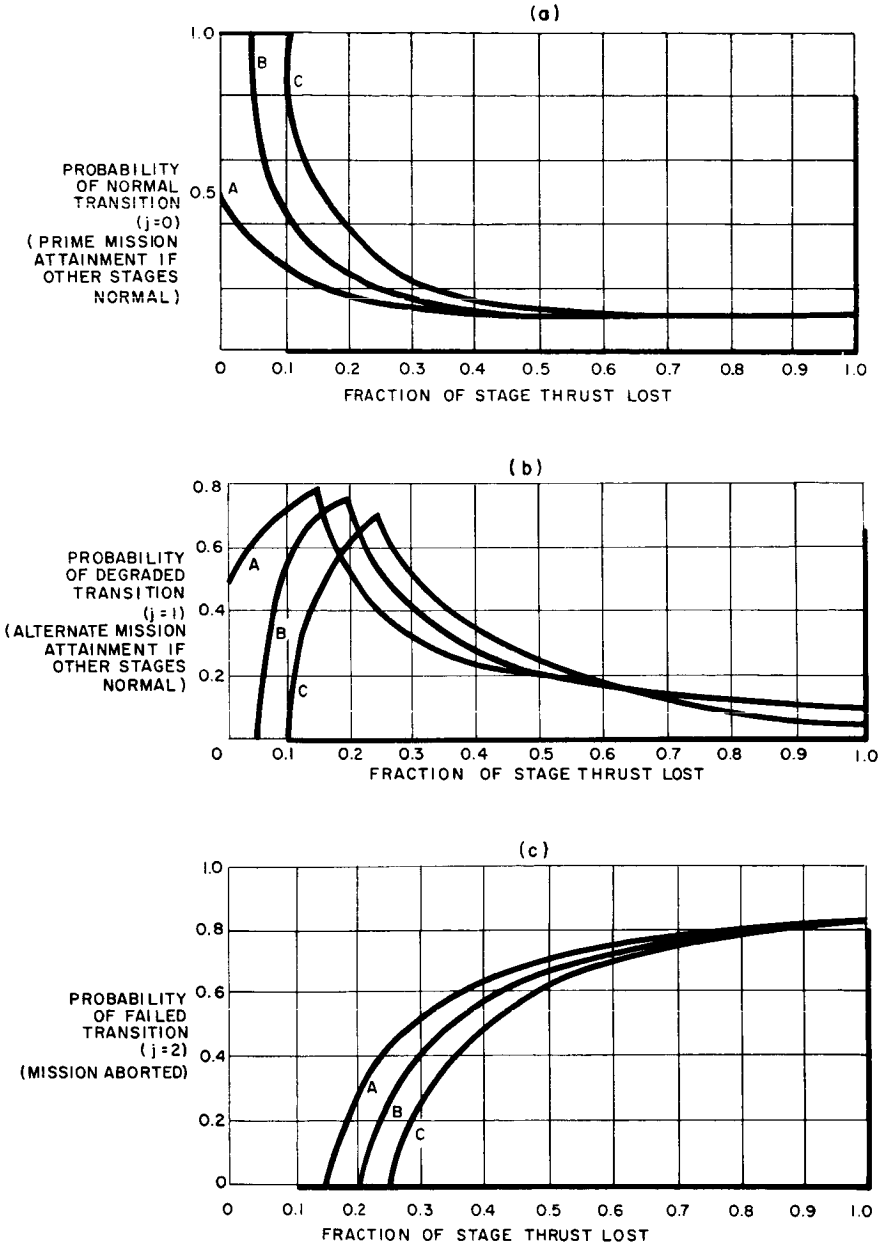
$\dot{m}_f$ = normal mass flow rate of fuel

$\dot{m}$ = $\dot{m}_{ox} + \dot{m}_f$

$\Delta\dot{m}_{ox}$ = increase in mass flow rate of oxidizer

$\Delta\dot{m}_f$ = increase in mass flow rate of fuel

$\Delta\dot{m}$ = $\Delta\dot{m}_{ox} + \Delta\dot{m}_f$



A = 20% DECREASE IN PROPELLANT FLOW
B = 10% DECREASE IN PROPELLANT FLOW
C = NO DECREASE IN PROPELLANT FLOW

FIGURE B-3

TRANSITION PROBABILITIES AS A FUNCTION OF THRUST AND PROPELLANT FLOW LOSSES

Table B-1 (Cont'd)

Symbols

T	=	normal stage thrust
ΔT	=	increase in stage thrust
g	=	acceleration of gravity
β	=	flight path angle with respect to horizontal
m_o	=	mass of vehicle at second stage ignition
m_p	=	mass of usable propellant on board at ignition
t^*	=	time of occurrence of malfunction - decision event which leads to ΔT. $\Delta \dot{m}_{ox}$, $\Delta \dot{m}_f$ and, therefore, ΔV_{co} and Δt_{co}

APPENDIX C

DIGITAL COMPUTER PROGRAMS

C-1. INTRODUCTION

As stated in Section IV, two sets of digital computer routines have been written to aid in the computation of risk. These are the READI failure enumeration routine and the risk computation routine. Paragraph C-2 covers the failure enumeration routine and paragraph C-3 covers the risk routine.

Both sets of routines were written in FORTRAN II and computed on the IBM 7094 computer using a systems tape Version 2, Mod. 25.

C-2. READI FAILURE ENUMERATION ROUTINE

This routine is referred to as TRACER. The purpose of TRACER is to compile a list which relates READI transducer failure modes, propulsion system malfunctions, and READI decisions to each other. This list encompasses the combination of circumstances in which the READI decision is not the decision programmed for the propulsion system malfunction. This list is stored on magnetic tape for use in the risk routine.

A detailed flow chart for the computer routine to accomplish this is shown in figure C-1. The symbols used in this chart are the actual FORTRAN symbols employed. The input data symbols are defined in table C-1. All other symbols are defined by the flow chart.

The basic method of accomplishing the assigned task is as follows. Each transducer is assumed to have two failure modes, very high and very low. The outputs of each transducer in each failure mode are read into the computer. Up to 59 transducers can be handled. The unfailed values of each transducer for each malfunction for a single phase are read into

the computer and written on tape. Up to 59 malfunctions can be handled. This process is repeated until all phases are covered. Up to nine phases can be handled. The tape is then rewound and the programmed decisions for the first system are read. The program then proceeds to place each transducer, in turn, in the high failed mode. A subroutine containing the definitions of the malfunction detectors in terms of transducer outputs is then called on the basis of the system number. Up to 20 systems can be handled on a single pass of the program. Then a phase indicating V is set for possible use in decision rule definition. A subroutine containing the decision rules definitions is then called and the actual decision indicated by the READI system is determined after priority is determined. The following convention on decision priority is employed:

- Decision one is no action and has the lowest priority
- Decision two has the highest priority, decision three the second highest, etc.

Up to ten decisions other than no action can be handled. The decision reached is compared to the programmed decision and if they are different a coded word indicating the corresponding triplet is stored in the high failure list.

This process is repeated for low failure of transducers. The no transducer failure condition is included on the high failure loop. When both loops have been completed, the high and low lists are written on tape and printed out for further inspection. The program proceeds to the next system, if any.

Table C-1

FORTRAN Symbols - Tracer Routine

Symbol	Definition
MKP	Maximum number of phases
MI	Maximum number of malfunctions
ML	Maximum number of transducers
MK	Maximum number of decisions
M1	Number of malfunction indicator indicating phase I
M9	Number of malfunction indicator indicating phase 9
SN(L)	High failed value of transducer L
SL(L)	Low failed value of transducer L

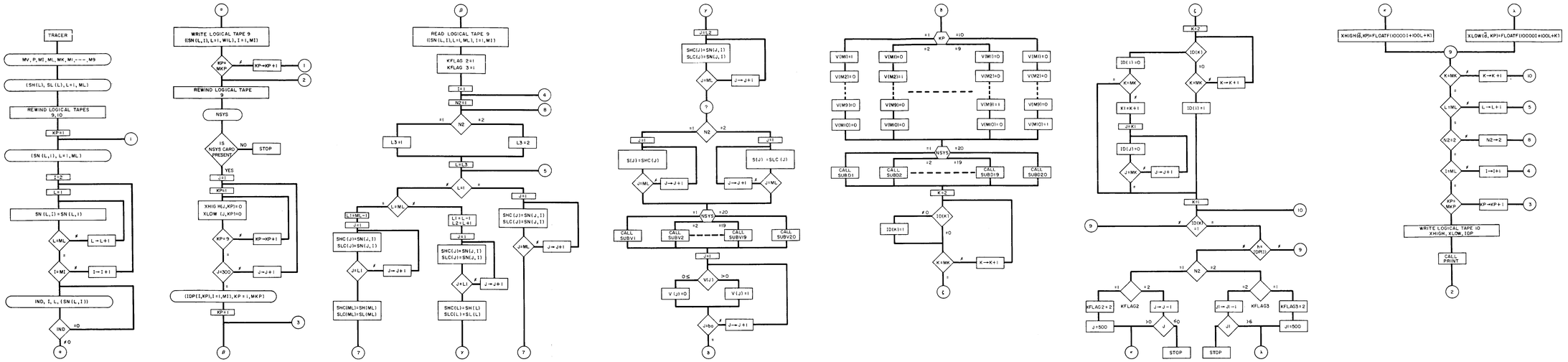


FIGURE C-1
FLOW CHART FAILURE
EVENT ROUTINE ENUMERATION

Table C-1

FORTRAN Symbols - Tracer Routine (Cont)

Symbol	Definition
SN(L,I)	Unfailed output of transducer L when malfunction I occurs. (Note: order of input deck determines phase)
IND	Zero when more SN changes are to be read in. One when end of changes for single phase
XHIGH(JFP)	J entry on high list for phase KP
XLOW (JKP)	J entry on low list for phase KP
PDP (I, KP)	Programmed decision number for malfunction I in phase KP

C-3. RISK COMPUTATION ROUTINE

The purpose of the Risk Computation Routine is to combine the output of the READI Failure Enumeration Routine (TRACER) with mission data to evaluate the overall performance of the system.

There are five subroutines plus one main routine (MAIN) in this program.

1. MAIN - The purpose of this routine is to:

- Read in the data
- Call those subroutines required for the particular run being executed. Certain indices (KFLAG 1, KFLAG 2) are read in to control the calling sequences.

The sequence of "read" and "call" orders, in flow diagram form, executed by MAIN is shown in figure C-2. The actual formats and number of cards are indicated for each group of input data.

2. ORDER - The purpose of this subroutine is to increase the efficiency of the overall program. ORDER makes it possible to arrange the input deck in such a way that data handling external to the machine is minimized. For example, if it is desired to change a certain ordered list of numbers, only the change itself need be read in. ORDER will make the insertion or deletion in such a way that the list remains ordered. ORDER need not be executed for each run.

3. COST - This subroutine computes the variable cost of each system being evaluated. The fixed cost can easily be accounted for externally.

4. LOSS - The purpose of this subroutine is to compute the losses for each malfunction/decision pair for each mission phase. The phase end state risks are multiplied by transition probabilities for each malfunction/decision pair and these products are summed. The transition probabilities may be found by using the procedure outlined in Appendix B. The end state risks are found by reflecting the mission end state losses back to the nodes of interest. This process is described in Section IV.

5. PRINT - The purpose of this subroutine is to write out the quantitative description of the particular READI/vehicle/mission complex being evaluated. System cost, component cost and component failure rates are given. The losses computed in LOSS are also written on the output tape.

6. RISK - This subroutine performs the main function in evaluating READI's performance. A detailed flow diagram is presented in figure C-3.

The risk quantity is partitioned into the following categories:

- False Actions - The occurrence of a decision when no malfunction occurs
- Missed Actions - The occurrence of no decision when a malfunction does occur
- Wrong Actions - The occurrence of a decision when a malfunction occurs, but the decision is not programmed for that malfunction
- Not Monitored Actions - The occurrence of no decision when a malfunction occurs, with no decision being programmed for that malfunction
- Correct Actions - The occurrence of a decision when a malfunction occurs, with that decision being the programmed one for the malfunction which has occurred.

The equations defining risk for each category are given in the flow diagram (see figure C-3). The variables used in this subroutine are defined in table C-2.

A sample output of the risk computation routine is shown in figure C-4. Annotations have been inserted to explain the various sections of this output.

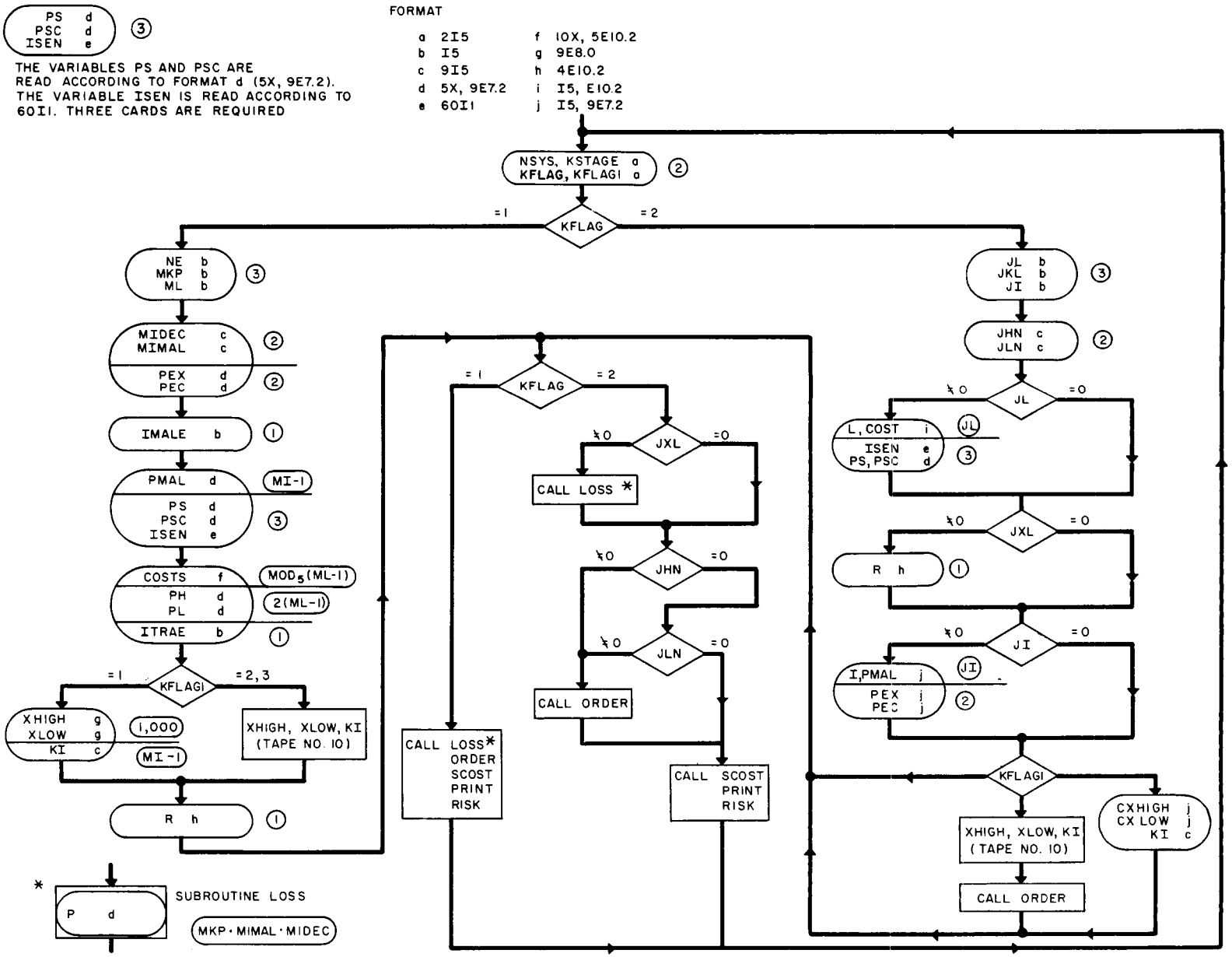


FIGURE C-2
MAIN ROUTINE

FIGURE C-3
SUBROUTINE RISK

Table C-2

Subroutine Symbols

Symbol	Definition
NSYS	System number
KSTAGE	Stage number
KFLAG	Reading sequence control index
KFLAG 1	Reading sequence control index
NE	Number of engines in stage KSTAGE
MIDEC	Maximum number of decisions
MIMAL	Maximum number of malfunctions
PEX	Engine reliability
PEC	Stage common propulsion system reliability
IMALE	Maximum number of engine malfunctions
PMAL	Probability of each malfunction, given that a malfunction has occurred
PS	Reliability of stage common transducer set
PSC	Reliability of engine transducer set
ISEN	List of transducers used in system NSYS
COSTS	List of transducer costs
PH	Probability of transducer failure (high mode)
PL	Probability of transducer failure (low mode)
ITRAE	Maximum number of transducers per engine
XHIGH	Supplied by TRACER, see table C-1
XLOW	
KI	
R	Risks for each of the phase end states
P	Transition probabilities for each malfunction/decision pair
JL	Number of changes to make in transducer data
JXL	Number of changes to make in risk data
JI	Number of changes to make in malfunction data
JHN	Number of changes to make in XHIGH
JLN	Number of changes to make in XLOW

EVALUATION OF READI SYSTEM 2 ← OPTUMUM SYSTEM

STAGE NUMBER 2

COST = 112000.00 ← TOTAL ADJUSTED COST IN DOLLARS DOES NOT INCLUDE FIXED DEVELOPMENTAL COST OF $100 K.

READI TRANSDUCER DATA

	ONE	TWO	THREE	FOUR	PHASE FIVE	SIX	SEVEN	EIGHT	NINE
SINGLE ENGINE TRANSDUCER PACKAGE RELIABILITY	9.86E-01	0.	0.	0.	0.	0.	0.	0.	0.
STAGE COMMON TRANSDUCER PACKAGE RELIABILITY	9.99E-01	0.	0.	0.	0.	0.	0.	0.	0.

TO BE READ 9.99×10^{-1}

THESE FIGURES ARE TOTAL PACKAGE RELIABILITIES THE SINGLE ENGINE TRANSDUCER PACKAGE CONSISTS OF ALL TRANSDUCERS ASSOCIATED WITH ONE ENGINE. THE STAGE COMMON TRANSDUCER PACKAGE CONSISTS OF ALL TRANSDUCERS ASSOCIATED WITH THE PORTIONS OF THE PROPULSION SYSTEM COMMON TO ALL ENGINES.

NOTE: ONLY A SINGLE *PHASE* IS TREATED *HEREIN*, BUT PROVISIONS HAVE BEEN MADE FOR UP TO 9 PHASES.

CONDITIONAL PROBABILITY OF FAILED TRANSDUCER

TRANSDUCER	FAILURE MODE	ONE	TWO	THREE	FOUR	PHASE FIVE	SIX	SEVEN	EIGHT	NINE
1	HIGH	0.	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	0.	0.	0.	0.	0.	0.	0.	0.	0.
2	HIGH	5.32E-03	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	3.46E-02	0.	0.	0.	0.	0.	0.	0.	0.
3	HIGH	1.33E-03	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	7.98E-03	0.	0.	0.	0.	0.	0.	0.	0.
4	HIGH	2.66E-03	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	4.66E-02	0.	0.	0.	0.	0.	0.	0.	0.
5	HIGH	1.40E-02	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	5.46E-02	0.	0.	0.	0.	0.	0.	0.	0.
6	HIGH	2.13E-02	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	1.08E-01	0.	0.	0.	0.	0.	0.	0.	0.
7	HIGH	5.59E-02	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	1.44E-01	0.	0.	0.	0.	0.	0.	0.	0.
8	HIGH	1.34E-01	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	1.34E-01	0.	0.	0.	0.	0.	0.	0.	0.
9	HIGH	7.05E-02	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	1.60E-01	0.	0.	0.	0.	0.	0.	0.	0.
10	HIGH	2.04E-01	0.	0.	0.	0.	0.	0.	0.	0.
	LOW	7.96E-01	0.	0.	0.	0.	0.	0.	0.	0.

INDICATES NO TRANSDUCER FAILURE

TRANSDUCERS 1 TO 9 SINGLE ENGINE TRANSDUCERS

DEFINITION OF SINGLE ENGINE TRANSDUCER PACKAGE. TRANDUCER 10 IS A STAGE COMMON TRANSDUCER PACKAGE.

THE CONDITIONING EVENT HERE IS THE FAILURE OF THE COGENT TRANSDUCER PACKAGE.

ADJUSTED TRANSDUCER COSTS

TRANSDUCER	COST	TRANSDUCER	COST	TRANSDUCER	COST
1	0.	2	3000.00	3	2000.00
4	2000.00	5	3000.00	6	-0.
7	0.	8	5000.00	9	7000.00
10	2000.00				

UNITS HERE ARE DOLLARS. COSTS OF ZERO INDICATE THAT THE TRANSDUCE IS NOT INCLUDED IN THE SYSTEM.

FIGURE C-4
SAMPLE OUTPUT OF THE RISK COMPUTATION ROUTINE
(SHEET 1 OF 5)

PROPULSION SYSTEM DATA

NUMBER OF ENGINES IN STAGE = 5

	ONE	TWO	THREE	FOUR	PHASE FIVE	SIX	SEVEN	EIGHT	NINE
SINGLE ENGINE RELIABILITY	9.96E-01	0.	0.	0.	0.	0.	0.	0.	0.
STAGE COMMON RELIABILITY	9.99E-01	0.	0.	0.	0.	0.	0.	0.	0.

THESE ARE TOTAL **RELIABILITIES.** DEFINITIONS OF THE TWO ***PACKAGES*** ARE SIMILAR TO THE TRANSDUCER PACKAGES.

CONDITIONAL PROBABILITY OF MALFUNCTION

	MALFUNCTION	ONE	TWO	THREE	FOUR	PHASE FIVE	SIX	SEVEN	EIGHT	NINE
NO PROPULSION SYSTEM MALFUNCTION	1	0.	0.	0.	0.	0.	0.	0.	0.	0.
	2	5.63E-02	0.	0.	0.	0.	0.	0.	0.	0.
	3	1.80E-02	0.	0.	0.	0.	0.	0.	0.	0.
	4	6.75E-02	0.	0.	0.	0.	0.	0.	0.	0.
	5	1.80E-02	0.	0.	0.	0.	0.	0.	0.	0.
	6	1.35E-02	0.	0.	0.	0.	0.	0.	0.	0.
	7	6.75E-03	0.	0.	0.	0.	0.	0.	0.	0.
	8	7.65E-02	0.	0.	0.	0.	0.	0.	0.	0.
	9	2.93E-02	0.	0.	0.	0.	0.	0.	0.	0.
	10	5.18E-02	0.	0.	0.	0.	0.	0.	0.	0.
	11	5.40E-02	0.	0.	0.	0.	0.	0.	0.	0.
	12	1.01E-02	0.	0.	0.	0.	0.	0.	0.	0.
	13	6.75E-03	0.	0.	0.	0.	0.	0.	0.	0.
	14	8.10E-02	0.	0.	0.	0.	0.	0.	0.	0.
	15	4.05E-03	0.	0.	0.	0.	0.	0.	0.	0.
	16	3.38E-02	0.	0.	0.	0.	0.	0.	0.	0.
	17	1.35E-02	0.	0.	0.	0.	0.	0.	0.	0.
	18	2.70E-02	0.	0.	0.	0.	0.	0.	0.	0.
	19	5.18E-02	0.	0.	0.	0.	0.	0.	0.	0.
	20	6.75E-02	0.	0.	0.	0.	0.	0.	0.	0.
	21	2.48E-02	0.	0.	0.	0.	0.	0.	0.	0.
	22	3.38E-02	0.	0.	0.	0.	0.	0.	0.	0.
	23	1.80E-02	0.	0.	0.	0.	0.	0.	0.	0.
	24	1.35E-01	0.	0.	0.	0.	0.	0.	0.	0.
	25	1.01E-01	0.	0.	0.	0.	0.	0.	0.	0.

MALFUNCTIONS 1 TO 24 ARE SINGLE ENGINE MALFUNCTIONS

THE CONDITIONING EVENT IS THE FAILURE OF THE COGENT *SET* OF MALFUNCTIONS (I.E., SINGLE ENGINE MALFUNCTIONS AND STAGE COMMON MALFUNCTIONS)

FIGURE C-4
SAMPLE OUTPUT OF THE RISK COMPUTATION ROUTINE
(SHEET 2 OF 5)

LOSS DATA

DECISION	MALFUNCTION	ONE	TWO	THREE	FOUR	PHASE FIVE	SIX	SEVEN	EIGHT	NINE
1	1	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	2	3.44E 00	0.	0.	0.	0.	0.	0.	0.	0.
1	3	3.10E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	4	7.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	5	5.10E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	6	3.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	7	7.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	8	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.
1	9	5.73E 00	0.	0.	0.	0.	0.	0.	0.	0.
1	10	7.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
1	11	3.44E 00	0.	0.	0.	0.	0.	0.	0.	0.
		1.30E 00	0.	0.	0.	0.	0.	0.	0.	0.
		7.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
		5E 00	0.	0.	0.	0.	0.	0.	0.	0.
		00	0.	0.	0.	0.	0.	0.	0.	0.
			0.	0.	0.	0.	0.	0.	0.	0.
4				0.	0.	0.	0.	0.	0.	0.
4						0.	0.	0.	0.	0.
4	6					0.	0.	0.	0.	0.
4	7	4.					0.	0.	0.	0.
4	8	1.31E					0.	0.	0.	0.
4	9	4.40E-01					0.	0.	0.	0.
4	10	3.30E-01	0.					0.	0.	0.
4	11	4.40E-01	0.	0.				0.	0.	0.
4	12	1.31E 00	0.	0.	0.			0.	0.	0.
4	13	4.40E-01	0.	0.	0.	0.			0.	0.
4	14	5.50E-01	0.	0.	0.	0.				
4	15	3.30E-01	0.	0.	0.	0.				
4	16	6.75E 00	0.	0.	0.	0.	0.			
4	17	6.75E 00	0.	0.	0.	0.	0.			
4	18	4.40E-01	0.	0.	0.	0.	0.			
4	19	4.40E-01	0.	0.	0.	0.	0.	0.		
4	20	5.50E-01	0.	0.	0.	0.	0.	0.	0.	
4	21	3.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
4	22	3.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
4	23	3.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
4	24	5.50E-01	0.	0.	0.	0.	0.	0.	0.	0.
4	25	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.
5	1	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	2	7.76E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	3	3.00E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	4	2.36E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	5	5.10E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	6	2.20E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	7	7.20E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	8	8.30E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	9	7.76E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	10	7.20E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	11	7.76E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	12	2.20E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	13	7.20E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	14	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.
5	15	2.36E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	16	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	17	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	18	7.78E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	19	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.
5	20	7.79E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	21	7.76E 00	0.	0.	0.	0.	0.	0.	0.	0.
5	22	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	23	1.90E-01	0.	0.	0.	0.	0.	0.	0.	0.
5	24	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.
5	25	1.10E 01	0.	0.	0.	0.	0.	0.	0.	0.

LOSS DATA IS GIVEN FOR EACH m/s PAIR. UNITS ARE MISSION REPLACEMENT VALUE = 1
λ = 10

FIGURE C-4
SAMPLE OUTPUT OF THE RISK COMPUTATION ROUTINE
(SHEET 3 OF 5)

THIS LIST FOR HIGH TRANSDUCER FAILURES

RISK COMPONENT TABULATION
REACI SYSTEM 2
STAGE 2

PHASE	MALFUNCTION	DECISION	TRANSDUCER FAILED	FUNCT MONITORED	CORRECT ALARM	RISK COMPONENT FALSE ALARM	MISSED ALARM	WRONG ALARM	DESIGN ERROR
1	1	3	2			7.59E-05			
1	1	4	4			5.69E-05			
1	2	3	2					6.19E-08	
1	2	4	1		7.73E-04				
1	2	1	9				3.76E-06		
1	2	4	3		7.09E-08				
1		4	4		1.42E-07				
1	2	4	5		7.44E-07				
1	[illegible]	4	8		7.13E-06				
[illegible]	[illegible]	3	2					5.81E-09	
			10		1.67E-07				
			1		7.26E-05				
			9				1.08E-07		
1	20		3		2.04E-09				
1	2	[illegible]	4		4.09E-09				
1	20	4	5		2.15E-08				
1	20	4			2.05E-07				
1	21	4						2.18E-08	
1	21	1			[illegible]7E-08				
1	21	4			[illegible]04				
1	21	4	4				9.58E-07		
1	22	3	2						
1	21	4	8		2.[illegible]				
1	21	4	9		1.06E[illegible]				
1	21	4	10		2.16E-0[illegible]				
1	22	1	1	1.18E-04				1.63E-09	
1	22	4	3						
1	22	4	4						
1	23	3	2						
1	22	1	5	2.47E-08					
1	22	1	8	2.36E-07					
1	22	1	9	1.25E-07					
1	22	1	10	2.54E-08					
1	23	1	1	6.27E-05					
1	23	4	3					2.18E-09	
1	23	4	4					4.36E-09	
1	24	3	2					1.49E-07	
1	23	1	5	1.32E-08					
1	23	1	8	1.26E-07					
1	23	1	9	6.64E-08					
1	23	1	10	1.35E-08					
1	24	4	1		1.86E-03				
1	24	1	3				2.78E-07		
1	25	1	10				2.27E-07		
1	2	4	4		5.56E-07				
1	24	4	5		2.92E-06				
1	24	4	8		2.79E-05				
1	24	4	9		1.47E-05				
1	24	4	10		3.00E-06				
1	25	2	1		4.15E-03				
1	25	2	2		3.32E-07				
1	25	2	3		8.29E-08				
1	25	2	4		1.66E-07				
1	2	2	5		8.71E-07				
1	2	2	8		8.34E-06				
1	25	2	9		4.40E-06				
TOTAL RISK FOR PHASE 1				2.71E-04	1.28E-02	1.33E-04	2.11E-05	5.35E-06	.
TOTAL PROBABILITY FOR PHASE 1				1.08E-03	1.58E-02	5.17E-04	5.48E-06	1.84E-06	.

THE DECISION IS INDICATED FOR EACH MALFUNCTION TRANSDUCER FAILURE PAIR. THE RESULT IS CLASSIFIED AND THE RISK COMPONENT IS GIVEN IN UNITS OF LOSS.

FOR THE DEFINITION OF RISK COMPONENTS USED HERE SEE TABLE 4-7.

FIGURE C-4
SAMPLE OUTPUT OF THE RISK COMPUTATION ROUTINE
(SHEET 4 OF 5)

NOTE: THIS LIST FOR LOW TRANSDUCER FAILURES

PHASE	MALFUNCTION	DECISION	TRANSDUCER FAILED (LO)	RISK COMPONENT NOT MONITORED	CORRECT ALARM	FALSE ALARM	MISSED ALARM	WRONG ALARM	DESIGN ERROR
1	1	4	3			1.71E-04			
1		1	9				8.52E-06		
1		4	2		1.84E-06				
1		4	3		4.25E-07				
1	2	4	4		2.48E-06				
1	2	4	5		2.91E-06				
		4	8		7.16E-06				
		1	9				2.46E-07		
		4	10		2.99E-06				
1		4	2		5.32E-08				
1	2	4	3		1.23E-08				
1	21	4	4		7.16E-08				
1	21	4	5		8.38E-08				
1	22		8		2.07E-07				
1	23		9				2.17E-06		
1	22		10		8.62E-08				
1	22		2		4.69E-07				
1	22	1			1.08E-07				
1	22	1			6.32E-07				
1	22	1			7.40E-07				
1	23	1	2	[illegible]	[illegible]				
1	25	1	10					9.80E-09	
1	23	1	4	4.39E-08					
1	23	1	5	5.14E-08					
1	23	1	8	1.27E-07					
1	23	1	9	1.50E-07					
1	23	1	10	5.29E-08					
1	24	4	2		7.23E-06				
1	24	4	3		1.67E-06				
1	24	4	4		9.73E-06				
1	24	4	5		1.14E-05				
1	24	4	8		2.81E-05			6.54E-09	
1	24	4	9		3.34E-05				
1	24	4	10		1.17E-05				
1	25	2	2		2.16E-06				
1	25	2	3		4.98E-07				
1	2	2	4		2.90E-06				
1	25	2	5		3.40E-06				
1	25	2	8		8.38E-06				
1	25	2	9		9.95E-06				
TOTAL RISK FOR PHASE 1				2.73E-04	1.32E-02	3.03E-04	7.14E-05	8.92E-06	0.
TOTAL PROBABILITY FOR PHASE 1				1.08E-03	1.59E-02	1.03E-03	1.81E-05	5.24E-06	0.

FIGURE C-4
SAMPLE OUTPUT OF THE
RISK COMPUTATION ROUTINE
(SHEET 5 OF 5)

TOTAL RISK COMPONENT TABULATION
READI SYSTEM 2
STAGE 2

TOTAL RISK COMPONENT DUE TO UNMONITORED MALFUNCTIONS = 2.73E-04 (PROBABILITY = 1.08E-03)

TOTAL RISK COMPONENT DUE TO CORRECT READI ACTIONS = 1.32E-02 (PROBABILITY = 1.59E-02)

TOTAL RISK COMPONENT DUE TO FALSE READI ACTIONS = 3.03E-04 (PROBABILITY =1.03E-03)

TOTAL RISK COMPONENT DUE TO MISSED ACTIONS = 7.14E-05 (PROBABILITY = 1.81E-05)

TOTAL RISK COMPONENT DUE TO WRONG READI ACTIONS = 8.92E-06 (PROBABILITY = 5.24E-06)

TOTAL RISK COMPONENT DUE TO READI DESIGN ERRORS = 0. (PROBABILITY = 0.)

APPENDIX D

DESIGN DATA USED IN READI OPTIMIZATION STUDY

D-1. ENGINE DESCRIPTION

A. GENERAL

An engine configuration has been hypothesized to serve as a model on which the various READI concepts and configurations can be tried. Because of limitations of security and proprietary data, it was considered preferable to design a representative configuration rather than work with a real engine. The engine is a second and third stage 200,000-pound thrust LO_2-LH_2 engine. The essential features of the engine are given below. Fluid and electrical schematics appear in figures D-1 and D-2, respectively.

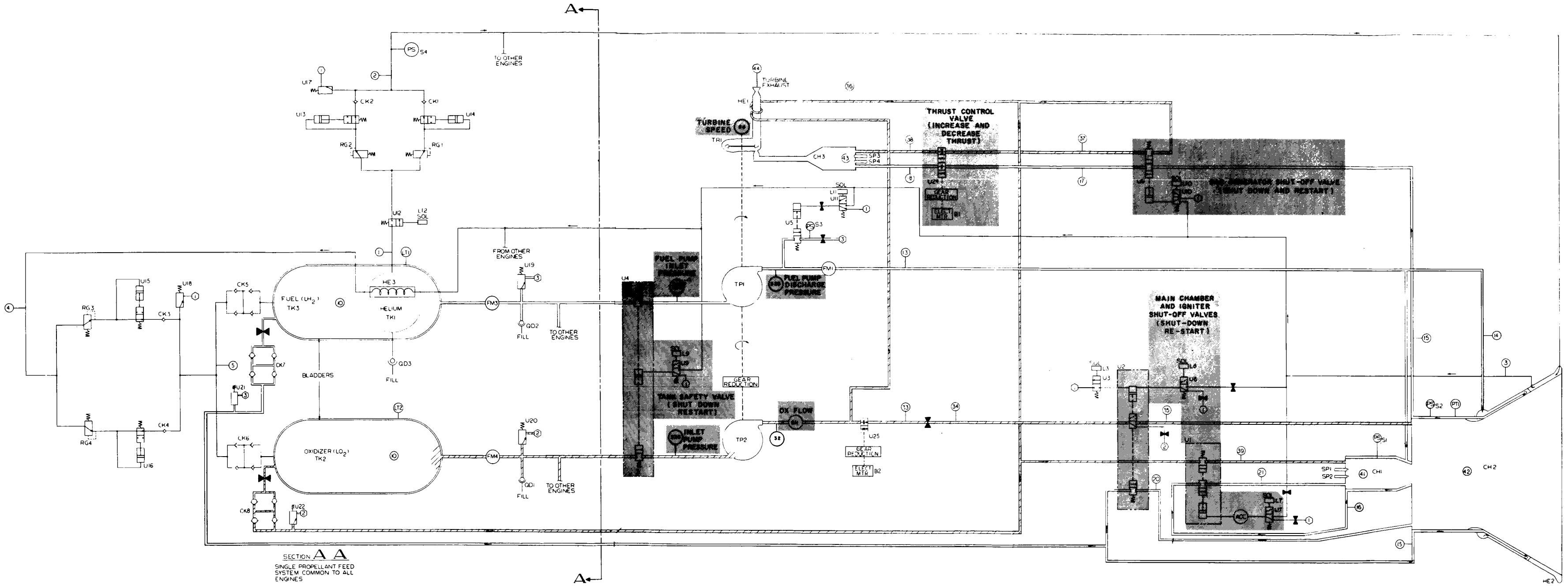
Thrust	200,000 pounds at altitude
Specific Impulse	420
Propellants	LO_2, LH_2
Cooling	Regenerative
Pumping	Turbopump with gas generator
Expansion Area Ratio	25:1
Mixture Ratio, Main Chamber	5:1
Mixture Ratio, Gas Generator	1:1
Rated Duration of Operation	400 sec
Chamber Pressure	600 psi
Pressurization	Helium start plus autogenous.

Note that in figure D-1 the whole propulsion system for a second stage is shown, since the READI model engine includes tankage, fuel and oxidizer pressurization systems, and control gas source, in addition to the liquid rocket engine. Table D-1 lists the pressure budget for a READI model engine at 100 percent thrust.

Table D-1

Pressure Budget Model Engine at 100 Percent Thrust

Station No.	Fluid Flowing	Location	Pressure (psia)
1	Helium Gas	Helium Tank Exit	5000-750
2	Helium Gas	Exit 1st Stage Regulation	650
3	Helium Gas	Exit Helium Heat Exchanger (HE2)	600
4	Helium Gas	Exit TK1 Heat Exchanger (HE3)	550
5	Helium Gas	Exit 2nd Stage Regulation	55
10	- - - - -	Propellant Tankage	50
11	Liquid Fuel	Fuel Pump Inlet	35
12	Liquid Fuel	Fuel Pump Exit	920
13	Liquid Fuel	Exit Fuel Flow Meter (FM1)	910
14	Liquid Fuel	Cooling Jacket Inlets	900
15	Gaseous Fuel	Main Cooling Jacket Exits	750
16	Gaseous Fuel	Igniter Cooling Jacket Exit	810
17	Gaseous Fuel	Turbopump Control Valve Inlet	730
18	Gaseous Fuel	Turbopump Control Valve Exit	550
20	Gaseous Fuel	Main Prop Valve Exit	730
21	Gaseous Fuel	Igniter Prop Valve Exit	790
31	Liquid Oxidizer	Oxidizer Pump Inlet	35
32	Liquid Oxidizer	Oxidizer Pump Exit	990
33	Liquid Oxidizer	Oxidizer O/F Control Valve Exit	840
34	Liquid Oxidizer	Main Oxidizer Trim Orifice Exit	750
35	Liquid Oxidizer	Main Prop Valve Exit	730
36	Gaseous Oxidizer	Heat Exchanger (HE1) Exit	810
37	Gaseous Oxidizer	Turbopump Control Valve Inlet	790
38	Gaseous Oxidizer	Turbopump Control Valve Exit	550
39	Gaseous Oxidizer	Igniter Prop Valve Exit	790
41	Combustion Products	Igniter Chamber	660
42	Combustion Products	Main Thrust Chamber	600
43	Combustion Products	Turbine Gas Generator	460
44	Combustion Products	Turbine Exhaust	Ambient



LEGEND

1. HELIUM OVERBOARD DRAIN
2. OXIDIZER OVERBOARD DRAIN
3. FUEL OVERBOARD DRAIN
- (ACC) ACCUMULATOR
- MECHANICAL LINK
- FIXED ORIFICE
- PRESSURE BUDGET STATION NO

LT	OXIDIZER TANK LEVEL TRANSDUCER
LT1	FUEL TANK LEVEL TRANSDUCER
PT1	MAIN THRUST CHAMBER PRESSURE TRANSDUCER
SS	TURBOPUMP SPEED SENSOR
SP1 SP4	GAS GENERATOR IGNITER PLUG
SP1, SP2	IGNITER SPARK PLUG
CH3	TURBINE GAS GENERATOR
CH2	MAIN THRUST CHAMBER
CH1	MAIN THRUST CHAMBER IGNITER
FM1	OXIDIZER FLOW METER-TOTAL
FM2	FUEL FLOW METER-TOTAL
FM3	OXIDIZER FLOW METER-ENGINE
FM4	FUEL FLOW METER-ENGINE
TB1	TURBINE
TP2	OXIDIZER PUMP
TP1	FUEL PUMP
S4	CONTROL GAS PRESSURE SWITCH
S3	FUEL PUMP INPUT PRESSURE SWITCH
S2	MAIN CHAMBER PRESSURE SWITCH
S1	IGNITER CHAMBER PRESSURE SWITCH
QD3	HELIUM TANK QUICK DISCONNECT
QD2	FUEL TANK QUICK DISCONNECT
QD1	OXIDIZER TANK QUICK DISCONNECT
CK5-CK8	QUADRUPLE CHECK VALVE
CK1-CK4	CHECK VALVE
HE3	HELIUM TANK HEAT EXCHANGER
HE2	OXIDIZER HEAT EXCHANGER
HE1	FUEL HEAT EXCHANGER
TK3	FUEL TANK
TK2	OXIDIZER TANK
TK1	HELIUM TANK
RG4	SECOND STAGE HELIUM PRESSURE REGULATOR
RG3	SECOND STAGE HELIUM PRESSURE REGULATOR
RG2	FIRST STAGE HELIUM PRESSURE REGULATOR
RG1	FIRST STAGE HELIUM PRESSURE REGULATOR
MV	ELECTRIC MOTOR OMNIDIRECTOR CONTROL VALVE
U1	ELECTRIC MOTOR TURBOPUMP CONTROL VALVE
U25	OXIDIZER SHUT CONTROL VALVE (ELECTRIC MTR OPERATING)
U24	TURBOPUMP CONTROL VALVE (ELECT MTR OPERATING)
U7	INSTRUMENTATION SHUT-VALVE-OXIDIZER
U13	INSTRUMENTATION SHUT-VALVE-FUEL
U12	OXIDIZER TANK RELIEF VALVE
U11	FUEL TANK RELIEF VALVE
U18	SECOND STAGE REGULATOR PRESSURE RELIEF VALVE
U15	FIRST STAGE REGULATOR PRESSURE RELIEF VALVE
U14	FIRST STAGE REGULATOR MAIN VENT VALVE (PNEUMATIC OPERATING)
U16	FIRST STAGE REGULATOR MAIN VENT VALVE (PNEUMATIC OPERATING)
U3	FIRST STAGE REGULATOR MAIN VENT VALVE (PNEUMATIC OPERATING)
U4	FUEL TANK REGULATOR PRESSURIZATION VALVE (PNEUMATIC OPERATING)
U2	OXIDIZER TANK REGULATOR PRESSURIZATION VALVE (PNEUMATIC OPERATING)
U6	HELIUM TANK SHUT-OFF VALVE (ELECTRIC MOTOR OPERATING)
U8	HELIUM TANK SHUT-OFF VALVE (ELECTRIC MOTOR OPERATING)
U9	TURBOPUMP SHUT-OFF VALVE (ELECTRIC MOTOR OPERATING)
U10	TURBOPUMP SHUT-OFF VALVE (ELECTRIC MOTOR OPERATING)
U5	ENGINE SAFETY VALVE (BLEED VALVE-ELECTRIC OPERATING)
U19	OXIDIZER FILL VALVE (ELECTRIC MOTOR OPERATING)
U20	OXIDIZER FILL VALVE (ELECTRIC MOTOR OPERATING)
U21	FUEL PUMP PRIME VALVE (ELECTRIC MOTOR OPERATING)
U22	FUEL PUMP PRIME VALVE (ELECTRIC MOTOR OPERATING)
U23	ENGINE SAFETY VALVE (PNEUMATIC OPERATING)
U17	FAST SHUTDOWN VALVE (ELECTRIC OPERATING)
U12	MAIN TRIP VALVE (PNEUMATIC OPERATING)
U11	MAIN TRIP VALVE (PNEUMATIC OPERATING)
SYMBOL	DESCRIPTION

FIGURE D-1
READI MODEL ENGINE, FLUID SCHEMATIC

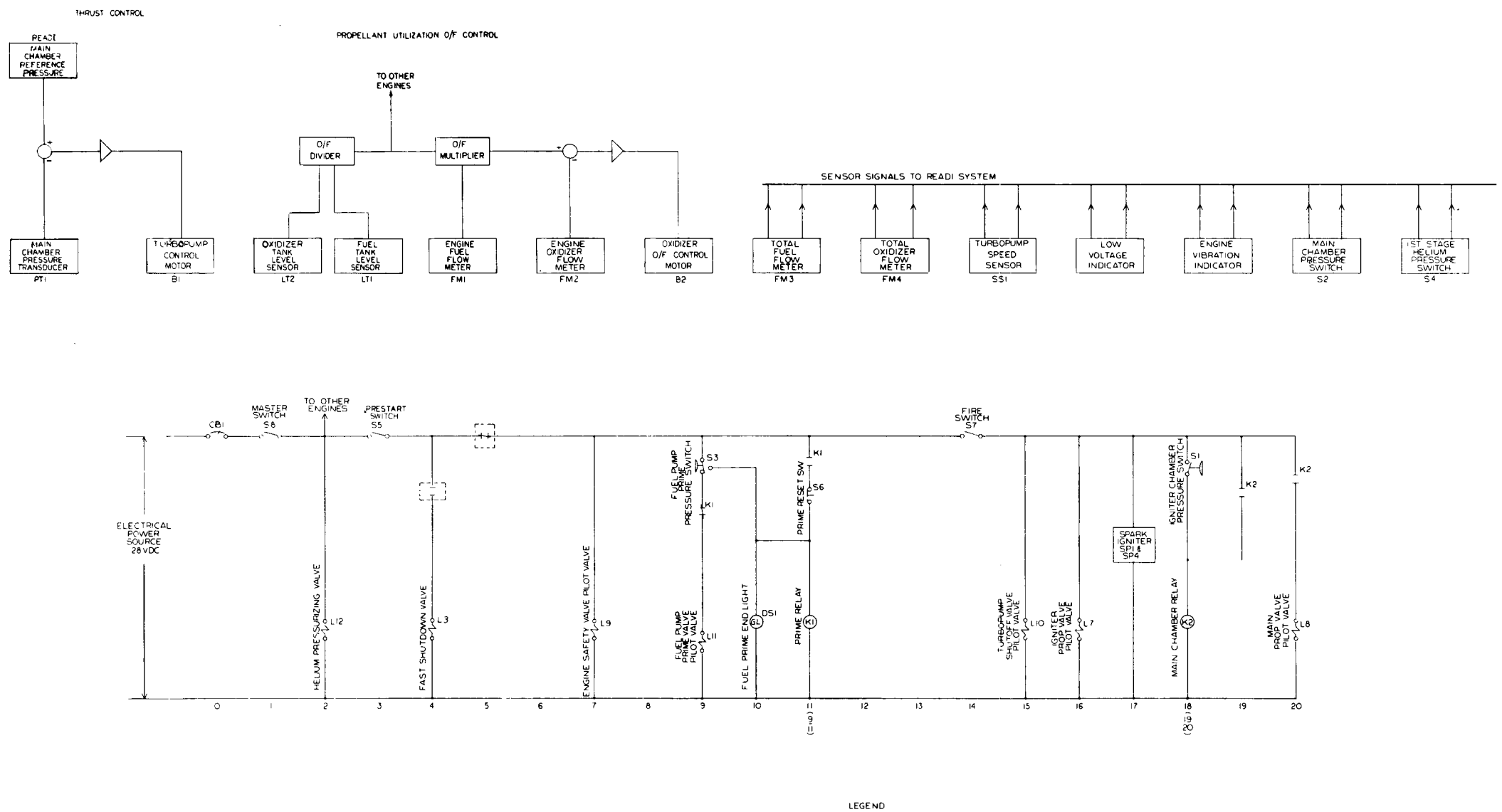


FIGURE D-2
READI MODEL ENGINE-ELECTRICAL SCHEMATIC

Figure D-1 shows a thrust control valve (U24) and a fast shut down valve (U7) which were originally hypothesized, during the Phase I investigation, to increase the alternative capability of the engine. These valves and their corresponding functions were not used in the Phase II Optimization Study. Other provisions, such as redundancy in the pressurization systems and the igniter chamber interlock arrangement, were retained since they make the overall propulsion system more reliable and safe, with or without a READI system.

B. MALFUNCTION CHARACTERISTICS

To be of maximum usefulness, the READI model engine must have malfunction characteristics which parallel those of real engines. This means that both the magnitude of failure probabilities and the distribution with respect to major components must be representative of near future engines. All of the available failure data for current production and developmental engines were therefore collected and compared.

There is surprisingly good agreement in major subsystem failure rates from different sources, as can be noted in table D-2 where five different data sources are compared. The "used in analysis" column is not the average of high and low limits because consideration had to be given to the difference between the data source engines and the representative engine configuration. The component failure rates were all normalized to give an engine which has a failure rate of 0.01 per full duration run, or a reliability of 0.99. This figure is consistent with the current state-of-the-art for engines which have undergone extensive development effort. The list of final states given below covers all situations which can occur in the READI model engine for second stage operation.

- Failure to start 0.001
- Premature, safe shut down 0.002
- Explosion 0.004
- Severe off-design operation 0.003

For a stage requiring restart, two more states are defined:

- Abnormal and/or dangerous condition after shutdown
- Failure to restart.

In order to include all of the failures in only four categories, some arbitrary classifications of real situations are necessary. For instance, explosions are implied to be severe enough to lead eventually to vehicle destruction.

A more detailed table, which is divided by major malfunction areas, m's, is shown in table D-3. This table shows the breakdown of assigned failure probabilities by m and by mission phase.

One condition which is troublesome from the standpoint of statistical independence is combustion instability. Combustion instability is really a failure effect, not a primary failure. However, the cause in each instance of combustion instability is difficult to trace and measure in real engines. Therefore, most analyses of rocket engines list instability as an independent failure and, therefore, it is listed in that way for the model engine.

Table D-2

Failure Probability Data by Major Subsystem

Major Subsystem	Low Limit of Data		Hi Limit of Data		Used in Analysis Procedure	
	% of Total Engine Failures	Failure Rate	% of Total Engine Failures	Failure Rate	%	λ
Turbopump Assembly	22	0.0022*	32	0.0052	22	0.0022
Thrust Chamber	14	0.0014*	32	0.0065	28	0.0028
Gas Generator	10	0.0016	17.1	0.00171*	12	0.0012
Valves	5.7	0 0014	31.7	0.00317*	24	0.0024
Line (Large and Small)	4.5	0.00045*	21	0.0034	9	0.0009
Regulators	-	0.0002	13.2	0.0030	3	0.0003
Starting System	1.9	0.00038	3.6	0.00036*	2	0.0002
Total for Engine					100%	0.0100

All failure rates are based on per cycle or per firing data

*Normalized total engine failure rate of 0.01

Table D-3

READI Model Engine Malfunction Summary

Malfunctions		Malfunction Probabilities X 10^4				
No	Engine Malfunctions	P1* Prestart (20 Sec)	P2 Start (2 Sec)	P3 Start to Prime EOC* (100 Sec)	P4 Prime EOC to CO (400 Sec)	P5 Stage CO (2 Sec)
2	Engine fuel leak (5%)	0.4	0.9	0.8	2.50	0
3	Fuel injector eroded - main chamber	0	0	0.3	0.80	0
4	Chamber burnout	0	0	1.0	3.00	0
5	G.G. injectors: clogged - fuel; eroded - lox	0	0.5	0.3	0.80	0
6	Pre-valve closed (fuel and lox)	1.8	0.7	0.2	0.60	0.7
7	G.G. fuel leak (including bootstrap line)	0	0.3	0.1	0.30	0
8	Combustion instability	0	13.5	1.1	3.40	0
9	Engine fuel leak (30%)	0.20	0.45	0.35	1.30	0
10	Lox injector eroded - main chamber	0	0	0.8	2.30	0
11	Engine lox leak (5%)	0.20	0.4	0.8	2.40	0
12	Main propulsion valve closed	0	3.15	0.15	0.45	0
13	G.G. lox leak (including bootstrap line)	0	0.30	0.1	0.30	0
14	T.P. structural failure	0.40	0.80	1.2	3.60	0
15	Clogged fuel injector - main chamber	0.3	0.03	0.06	0.18	0
16	Fuel pump cavitation	0	3.2	0.50	1.50	0
17	Lox pump cavitation	0	1.3	0.2	0.60	0
18	Engine lox leak (30%)	0.1	0.2	0.4	1.20	0

*EOC - Single engine engine-out capability, i.e., prime mission velocity required for stage can be achieved and attitude control retained.

Table D-3 (Cont)

READI Model Engine Malfunction Summary

Malfunction		Malfunction Probabilities X 10^4				
No	Engine Malfunctions	P1* Prestart (20 Sec)	P2 Start (2 Sec)	P3 Start to Prime EOC* (100 Sec)	P4 Prime EOC to CO (400 Sec)	P5 Stage CO (2 Sec)
19	T.P. gear bearing failure	0.3	0.3	0.8	2.30	0
20	Turbine exhaust failure	0	0	1.0	3.00	0
21	Clogged lox injector - main chamber	0.2	0.5	0.3	1.10	0
22	Turbine nozzle erosion	0.3	0.6	0.5	1.50	0
23	G.G. injector: eroded - fuel; clogged - lox	0.1	0.1	0.3	0.80	0
24	G.G. structural failure	0.7	1.4	2.0	6.00	0
	Stage Malfunctions					
25	Loss of tank pressurization	0.3	0.03	1.5	4.50	0.03

*EOC - Single engine engine-out capability, i.e., prime mission velocity required for stage can be achieved and attitude control retained.

C. PROPULSION SYSTEM PERFORMANCE LOSSES

The previous paragraphs in this appendix established the failure characteristics and the remedial action capability of the model propulsion system. The next step is to generate data which reflects the effect of all possible malfunction/decision pairs on propulsion system performance. The parameters chosen to describe this performance are:

- Loss of thrust from normal
- Loss of specific impulse from normal
- Loss of propellant overboard
- Probability of catastrophic loss of mission and crew.

The losses have been calculated or estimated for all malfunction areas and programmed decisions. Table D-4 shows the losses for phase 4, the interval of 2nd stage burning time from 100 to 400 seconds.

D-2. READI DESCRIPTION

A. GENERAL

For the purpose of evaluating READI, data are needed to describe transducers, malfunction detection techniques and programmed decisions for each system. The following paragraphs describe the data used in optimizing READI for that part of stage 2 operation during which engine-out capability exists.

B. TRANSDUCERS

The set of transducers hypothesized for the optimization study are listed in table D-5 according to the measurements being made. The estimated cost of making each measurement and the adjusted transducer failure rates are also given in table D-5. Cost is taken here in the broad sense - it includes penalties for installation, checkout and maintenance as well as the dollar cost of equipment.

C. MALFUNCTION DETECTION

Each transducer output is processed* and compared to one or more reference levels to produce discrete signals which indicate the occurrence of a malfunction group. For instance, the main chamber vibration signal is compared to two levels. Above the first level and below the second is called "high main chamber vibration." Any one of four malfunctions (numbers 9, 10, 15 and 16 of table D-3) can cause an indication of high main chamber vibration. Above the second reference level is an indication of "very high main chamber vibration." This indication will result when only one malfunction (number 8 of table D-3) occurs.

- - - - - - -

*The transducer signal processing includes electronic operations such as amplification, modulation, demodulation, filtering, frequency-to-analog conversion, and mathematical operations such as addition, subtraction, differentiation, integration, etc.

Table D-4

Propulsion System Loss Data For Mission Phase 4
(Prime Mission Engine-out Capability to Cut Off)

	D1 (No Action)				D2 (Abort)				D3 (Shut Down One Engine)				D4 (Pre-valve Shut Down)				D5 (Shut Down and Restart)			
m	ΔTH	ΔI_{SP}	ΔW_P***	P_{CL}	ΔTH	ΔI_{SP}	ΔW_P	P_{CL}	ΔTH	ΔI_{SP}	ΔW_P	P_{CL}	ΔTH	ΔI_{SP}	ΔW_P	P_{CL}	ΔTH	ΔI_{SP}	ΔW_P	P_{CL}
1*	0	0	0	0	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.998)**	0	0	0
2	0.02	0.02	0.002(f)	0.30	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.02	0(0.998)	0	0.002(f)	0.70
3	0.006	0.03	0	0.01	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0.03(0.990)	0.03	0	0.01
4	0	0	0.006(f)	0.05	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.990)	0	0.006(f)	0.20
5	0.01	0	0	0.03	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0.01(0.990)	0	0	0.03
6	0.20	0	0	0.01	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0)	0	0	0
7	0.01	0	0.002(f)	0.05	1.00	0	0	0	0.20	0	0	0.04	0.20	0	0	0.02	0.01(0.990)	0	0.002(f)	0.05
8	0.20	0	0.04(f, o)	0.99	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.10	0(0.600)	0	0	0.06
9	0.02	0.12	0.01(f)	0.50	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.02	0.2(0.998)	0	0.01(f)	0.70
10	0.03	0.03	0	0.05	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0.03(0.990)	0.03	0	0.05
11	0.04	0.02	0.01(o)	0.30	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.02	0.2(0.998)	0	0.01(o)	0.70
12	0.20	0	0	0.10	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.10	0.2(0)	0	0	0
13	0.05	0	0.002(o)	0.05	1.00	0	0	0	0.20	0	0	0.04	0.20	0	0	0.02	0.05(0.990)	0	0.002(o)	0.05
14	0.20	0	0.04(f, o)	0.50	1.00	0	0	0	0.20	0	0	0.03	0.20	0	0	0.03	0(0)	0	0.04(f, o)	1.00
15	0.02	0.04	0	0.10	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.998)	0	0	0.20
16	0.20	0	0	0.50	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.60	0(0.300)	0	0	0
17	0.20	0	0	0.50	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.60	0(0.300)	0	0	0
18	0.04	0.12	0.30(o)	0.50	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.02	0(0.998)	0	0.30(o)	0.70
19	0.20	0	0	0.20	1.00	0	0	0	0.20	0	0	0.01	0.20	0	0	0.02	0(0)	0	0	1.00
20	0.20	0	0	0.50	1.00	0	0	0	0.20	0	0	0.04	0.20	0	0	0.03	0(0)	0	0	0.70
21	0.04	0.02	0	0.50	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.998)	0	0	0.70
22	0.04	0	0	0	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.998)	0	0	0
23	0.04	0	0	0	1.00	0	0	0	0.20	0	0	0	0.20	0	0	0.01	0(0.998)	0	0	0
24	0.20	0	0	0.50	1.00	0	0	0	0.20	0	0	0.05	0.20	0	0	0.03	0(0)	0	0	1.00
25	1.00	0	0	1.00	1.00	0	0	0	1.00	0	0	1.00	1.00	0	0	1.00	1.00	0	0	1.00

*m1 represents the no malfunction condition.

**(.XXX) is the probability of successful restart

***The letter in parenthesis indicates whether lox (o) or fuel (f) or both, is being lost

ΔTH Fractional loss of Stage Thrust

ΔI_{SP} Fractional loss of Propulsion System I_{SP}

ΔW_P Fractional overboard loss of Stage Propellent Flow. The letters f and o indicate fuel and lox flow, respectively.

P_{CL} Probability of incurring catastrophic loss of vehicle. Implies loss of crew.

Table D-5

Transducer Characteristics

Transducer Measurement	Cost (dollars)	Failure Rate X 10^4	
		High	Low
2. Main Chamber Vibration	3,000	0.80	5.20
3. Turbine Speed	2,000	0.20	1.20
4. Lox Flow Discrepancy	2,000	0.40	7.00
5. Main Chamber Pressure	3,000	2.10	8.20
6. Lox Injector Pressure Drop	3,000	4.10	16.20
7. Engine Lox Flow	7,000	8.40	21.60
8. Fire Detector	5,000	20.10	20.20
9. Engine Fuel Flow	7,000	10.60	24.00
10. Propellent Tank Pressure	2,000	2.10	8.20

It is convenient to use a Venn diagram representation of the malfunction indicators described above. Figure D-3 shows how each transducer output is affected by the occurrence of propulsion system malfunctions. A table indicating the transducer content of each of the 10 systems evaluated is also shown in this figure. This table shows, for example, that system number 6 contains all transducers except numbers 6 and 7.

D. PROGRAMMED DECISIONS

To complete the description of the READI designs considered in the optimization study, it is necessary to present the decision rules which were programmed for each malfunction.

During the synthesis procedure (refer to Section III), the total set of possible READI's was reduced from over a million systems to 10 systems. The simplest systems under consideration, for instance those containing only one transducer, were capable of only one decision. The most elaborate systems were capable of executing the optimum decision for nearly all engine malfunctions. During the reduction process the programming of decisions became well defined. For the particular case considered, the programmed decisions for all 10 final systems were the same. This neither simplified nor complicated the digital computer evaluation of these systems, since provision was made for a variation in decisions from system to system in the program.

The programmed decisions for all systems are shown in figure D-4. The topological technique used in figure D-3 is again employed.

D-3. MISSION DESCRIPTION

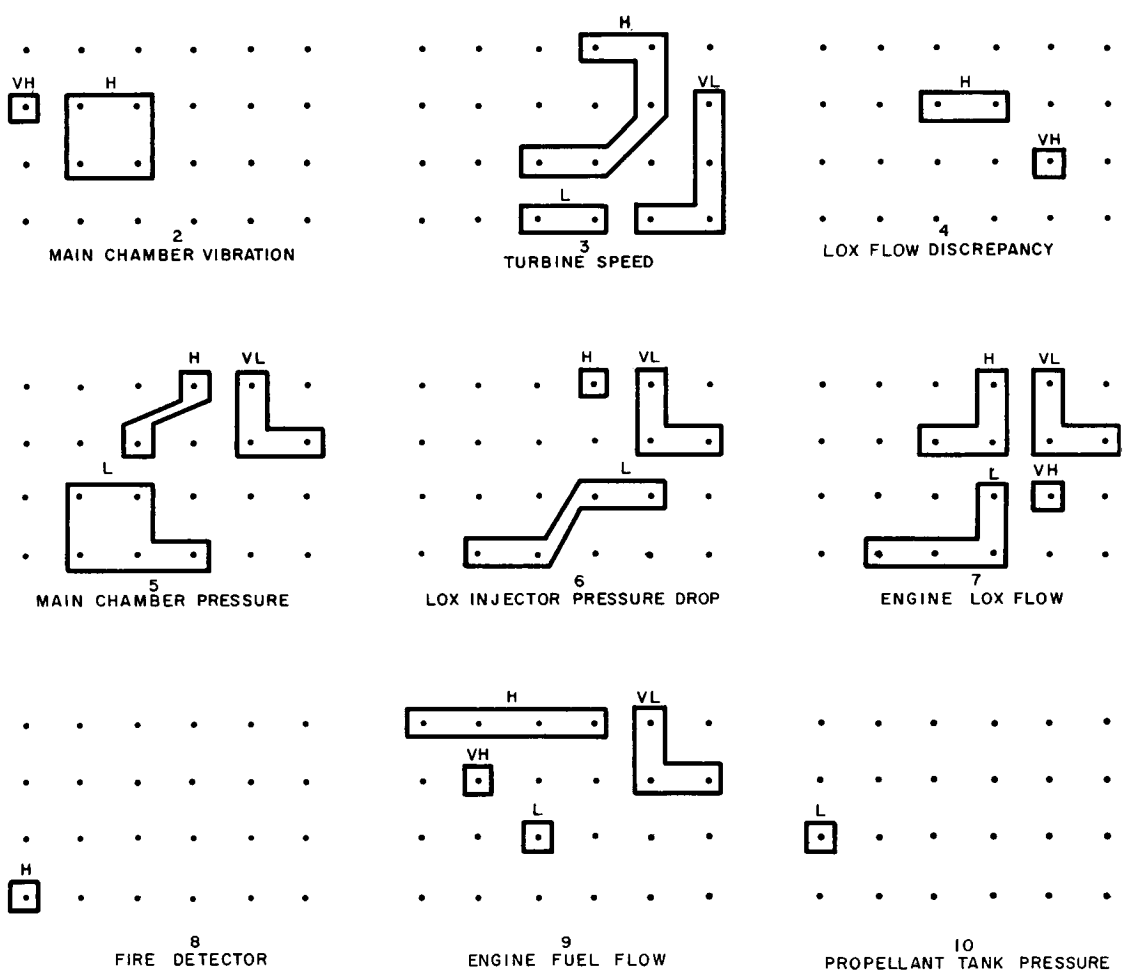
A. GENERAL

It was recognized early in the READI investigation that the value of READI would be a strong function of the mission plan being considered. Indeed, the ability of READI to capitalize on the flexibility present in advanced vehicle/mission concepts is the underlying reason for the high return in increased reliability and safety attributed to READI. The evolution of adaptive guidance concepts gives further evidence of awareness that vehicle flexibility (engine-out capability, etc.) can be used effectively to enhance mission performance.

B. MATHEMATICAL MODEL

It follows logically that some kind of model describing the many possible chains of events leading to the various desired mission objectives could be usefully employed. Such a model has been developed and is shown in figure D-5. The concepts implicit in this model are described in detail in paragraph 4-2.

This model was used in the evaluation of READI for a particular class of missions (manned lunar exploration) in the following manner. First, the values of the various mission end states were assigned. Prime mission attainment was arbitrarily assigned a value of 1 (refer to paragraph 2-6). Secondly, the probabilities governing transitions between all nodes (mission states) were obtained. The procedure used here was to compute the transitions for one phase of stage 2. This information was used to design an optimum READI configuration. The transition probabilities for the first and third stages were obtained by an extrapolation of stage 2 based on engineering judgement. The results are shown in table D-6. The reliabilities shown in table D-7 were obtained from this data.



KEY:

2	3	4	5	6	7
8	9	10	11	12	13
25	15	16	17	18	19
20	21	22	23	24	14

MALFUNCTION NUMBERS
(SEE TABLE D-3)

SYSTEM NUMBER	TRANSDUCER NUMBER 2	3	4	5	6	7	8	9	10
1	X	X				X	X	X	X
2	X	X		X		X	X	X	X
3	X	X			X	X	X	X	X
4	X	X		X	X	X	X	X	X
5	X	X	X			X	X	X	X
6	X	X	X	X			X	X	X
7	X	X	X	X		X	X	X	X
8	X	X	X		X	X	X	X	X
9	X	X	X	X	X		X	X	X
10	X	X	X	X	X	X	X	X	X

TRANSDUCER CONTENT OF SYSTEMS

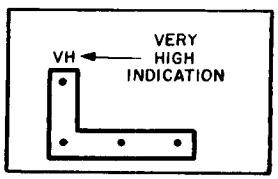
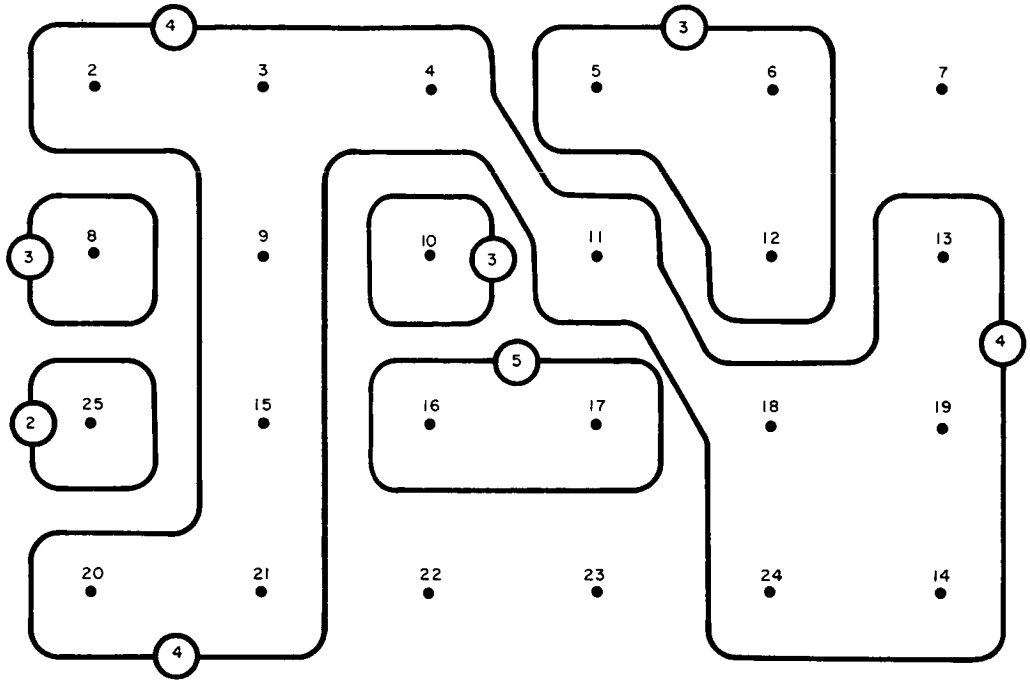


FIGURE D-3
MALFUNCTION DETECTION CHART



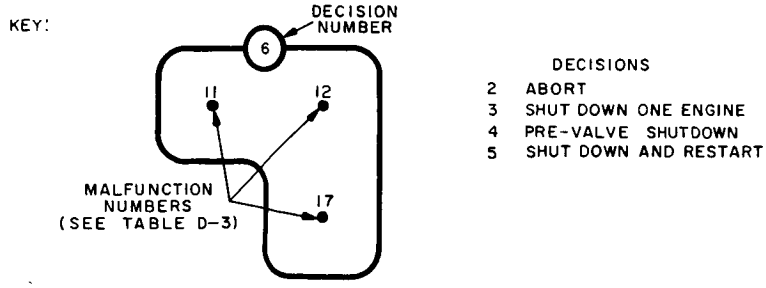


FIGURE D-4

PROGRAMMED DECISIONS – ALL SYSTEMS

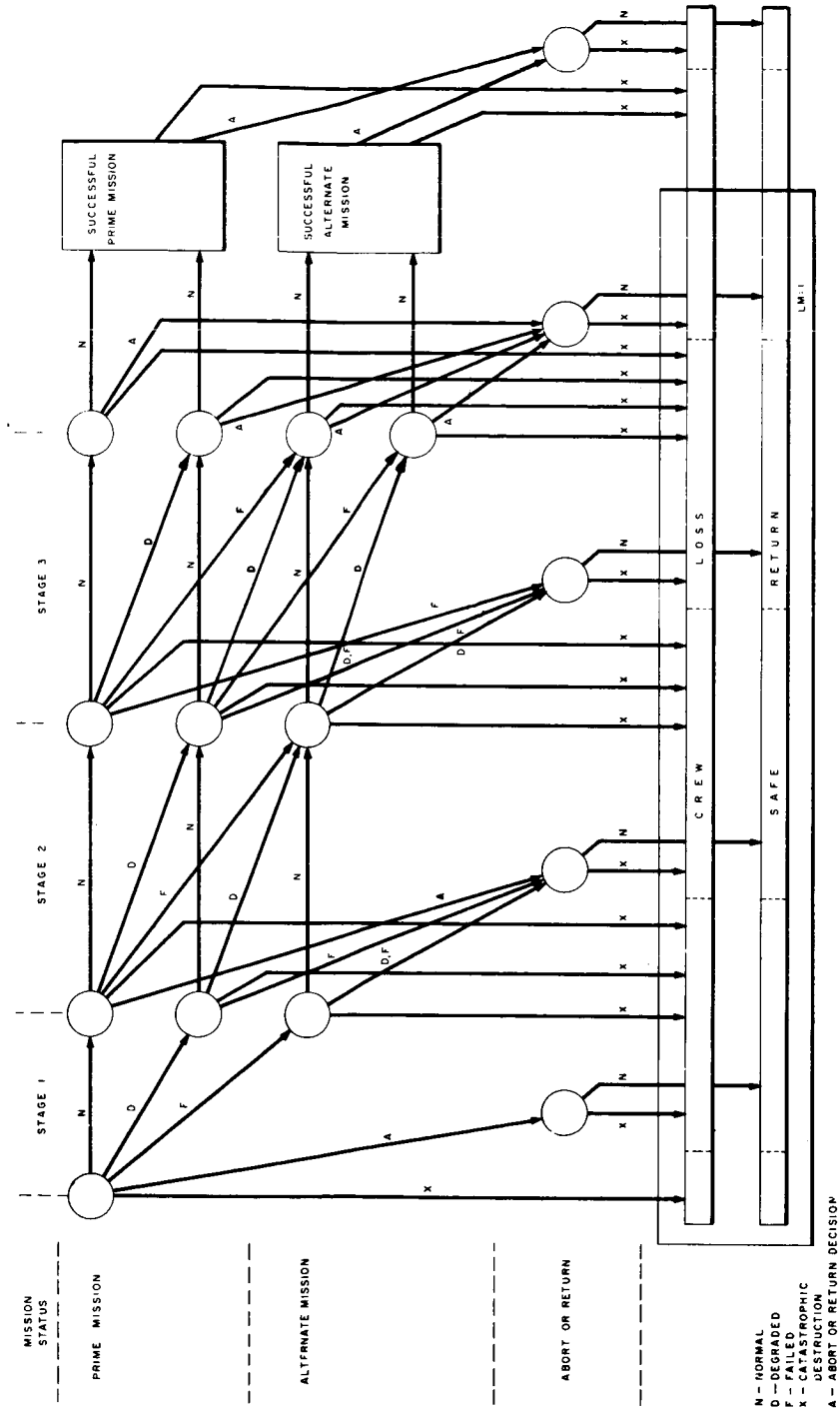


FIGURE D-5

OVERALL MISSION MODEL

Table D-6

Transition Probabilities

	Stage 1	Stage 2	Stage 3	Post Boost
Transition Probabilities - No READI				
Normal	0.965	0.960	0.990	0.950
Degraded	0.000	0.015	0.000	0.000
Failed	0.000	0.000	0.000	0.000
Abort	0.015	0.010	0.008	0.050
Catastrophic	0.020	0.015	0.002	0.000
Transition Probabilities - READI in Stages 1, 2 and 3				
Normal	0.985	0.989	0.992	0.950
Degraded	0.003	0.002	0.001	0.000
Failed	0.001	0.003	0.005	0.000
Abort	0.010	0.007	0.002	0.050
Catastrophic	0.001	0.001	0.000	0.000
Abort Reliabilities - Probability of Safe Abort				
	0.95	0.90	0.90	0.80

Table D-7

Mission and Crew Survival Reliabilities

	No READI	With READI
Probabilities		
Normal Mission	0.865	0.914
Degraded Mission	0.015	0.006
Prime Mission Attainment	0.880	0.920
Failed Mission	0.000	0.009
Prime or Alternate Mission Attainment	0.880	0.929
Aborted Mission/Crew Safe	0.070	0.058
Aborted Mission/Crew Lost	0.013	0.011
Catastrophic Loss of Mission and Crew	0.037	0.002
	1.000	1.000

Table D-7 (Cont)

Mission and Crew Survival Reliabilities

	No READI	With READI
Approximate Mission Loss Probabilities		
Stage 1	0.035	0.012
Stage 2	0.025	0.011
Stage 3	0.010	0.007
Post Boost	0.050	0.050
Total	0.120	0.080
Approximate Crew Loss Probabilities		
Stage 1	0.021	0.002
Stage 2	0.016	0.002
Stage 3	0.003	0.000
Post Boost	0.010	0.010
Total	0.050	0.014

APPENDIX E

CATALOG OF SIGNAL SPACE SEPARATIONS FOR H-1 ENGINE

The following table summarizes the set of malfunction detection techniques, or signal space separations, which have been incorporated in the Experimental READI System.

SIGNAL SPACE SEPARATION V 1.1.1

MAIN CHAMBER ROUGH COMBUSTION

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
A1	A1.1 > 100 grms 960 to 6000 cps	3 grms*				0 - 150 grms 200 to 8 KC	80 - 120 grms 600 to 6 KC
t2	t2.1 > 100 m sec	-	-	-	-	-	-

Definition of V = 1

(A1.1) (t2.1)

Malfunction(s) which cause V = 1

ROUGH COMBUSTION

Optimum Corrective Action

SHUT DOWN OR FAST SHUTDOWN IF FEASIBLE

* MAINSTAGE OPERATION ONLY
NOTE: BAND PASS FILTER REQ. 3 db DOWN @ 960 and 6K, 12 db/ ACTIVE ATTENUATION

SIGNAL SPACE SEPARATION V 2.1.1

LOW TURBINE SPEED AND LOW CHAMBER PRESSURE

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
N5	18,000 < N5.1 < 25,000	-	-			0-40,000	18-40K RPM
t1	t1.1 > 1.0 SEC	-	-	-	-	-	-
P1	P1.1 < 420 PSIA					0-650 PSIA	420-650 PSIA

Definition of V = 1

(N5.1)(t1.1)(P1.1)

Malfunction(s) which cause V = 1

LOW GG°/F RATIO, OR LOW TOTAL GG FLOW DUE TO PLUGGED GG INJECTORS OR PARTIAL GG VALVE OPENING, HOT GAS LEAK

Optimum Corrective Action

SHUTDOWN ENGINE WHEN PRIME MISSION EOC IS ATTAINED

NOTE: SHARE N5 PULSE PICKUP WITH RECORDER

SIGNAL SPACE SEPARATION V 2.1.2

LOSS TURBINE SPEED AND LOW CHAMBER PRESSURE

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
N5	N5.2 < 18,000	-	-			0-40,000 RPM	18-40K RPM
t1	t1.1 > 1.0 SEC	-	-				
P1	P1.1 < 420 PSIA					0-650 PSIA	420-650 PSIA

Definition of V = 1

(N5.2)(t1.1)(P1.1)

Malfunction(s) which cause V = 1

SEE 2.1.1 - ALSO, BROKEN BOOT STRAP LINE OR CHAMBER PRESSURE LINE, ALL FAILURES WHICH CAUSE LOSS OF OR NO CHAMBER PRESSURE

Optimum Corrective Action

SHUTDOWN ENGINE

NOTE: 6 PULSE/REV ON 31,460 RPM SHAFT

SIGNAL SPACE SEPARATION V 2.2.1

HIGH TURBINE SPEED

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
N5	40,000 < N5.3 > 35,000 RPM	-	-		N5 200,000 RPM/SEC	0-40,000 RPM	18-40K RPM

Definition of V = 1

N5.3

Malfunction(s) which cause V = 1

HIGH GG°/F CAUSED BY FUEL INJECTOR PLUGGING OR OX INJECTOR EROSION PARTIAL OPENING OF FUEL POPPET IN GG, OVERLAP OF SPGG AND LPGG, LOSS PUMP LOAD CAUSED BY LOSS OF PROPELLANT SUPPLY, CLOSURE OF PRE-VALVE

Optimum Corrective Action

SHUTDOWN

NOTE:

SIGNAL SPACE SEPARATION V 2.2.2.

HIGH TURBINE SPEED

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
N5.4	N5.4 > 40,000 RPM	-	-		N5' 200,000 RPM/sec	0-40,000 RPM	18-40K RPM

Definition of V = 1

N5.4

Malfunction(s) which cause V = 1

HIGH GG°F CAUSED BY FUEL INJECTOR PLUGGING OR OX INJECTOR EROSION, PARTIAL OPENING OF FUEL POPPET IN GG OVERLAP OF SPGG AND LPGG, LOSS PUMP LOAD CAUSED BY LOSS OF PROPELLANT SUPPLY CLOSURE OF PRE-VALVE

Optimum Corrective Action

SHUTDOWN

NOTE:

SIGNAL SPACE SEPARATION V 3.1.1

HIGH GG TEMPERATURE

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
T6	2000°F > T6.1 > 1500°F	-	-	-	120,000°F/SEC	0 - 2000 °F	1000 - 2000 °F

Definition of V = 1

T6.1

Malfunction(s) which cause V = 1

SEE V2.2.1 - ALL GAS GENERATOR FAILURES NOTED FOR V.2.2.1

Optimum Corrective Action

SHUTDOWN WHEN EOC IS ATTAINED

NOTE: CHROMEL/ALUMEL THERMOCOUPLE IN LPGG

SIGNAL SPACE SEPARATION V 3.1.2

HIGH GG TEMPERATURE

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
T6	T6.2 > 2000°F	-	-	-	120,000 °F/SEC	0 - 2000 °F	1000 - 2000 °F

Definition of V = 1

T6.2

Malfunction(s) which cause V = 1

SEE V3.1.1

Optimum Corrective Action

SHUTDOWN

NOTE: CHROMEL / ALUMEL THERMOCOUPLE IN LPGG

SIGNAL SPACE SEPARATION V 5.1.1

LOSS OF FUEL FLOW WITHOUT LOSS OF OX FLOW

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
(LOX) P7-P1	P7-P1 > 90 PSID = ΔP7.1	–	–		16,000 PSI/SEC	0-150	90-150
(FUEL) P8-P1	P8-P1 < 60 PSID = ΔP8.1			4000 PSI/SEC		0-130	80-130
t1	t1.1 > 1.0 SEC	–	–	–	–	–	–

Definition of V = 1

(ΔP7.1)(ΔP8.1)(t1.1)

Malfunction(s) which cause V = 1

LOSS OF FUEL TANK PRESSURE, FUEL LINE RUPTURE, FUEL PRE-VALVE CLOSURE, MFV CLOSURE

Optimum Corrective Action

SHUTDOWN

SIGNAL SPACE SEPARATION V 7.1.1

FLOW DISCREPANCY, LOX (FLOWMETER TO INJECTOR)

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
Q12	(0.0793)(Q12) − 121 = ΔPC1			—		0-3500 gpm	1800 - 3200 gpm
P7-P1	(P7-P1) = ΔPA	—	—	2400 PSI/SEC		0-150 PSID	90-150 PSID
t1	t1.1 > 1.0 SEC						
	X1 = 1 for ΔPC1 −	ΔPA >	0				
t3*	t3.1 > 1.0 SEC						

Definition of V = 1

V = 1 for (X1)(t3.1)(T1.1)($\overline{V2.2.1}$)

Malfunction(s) which cause V = 1

LOX LEAKS BETWEEN FLOWMETER AND LOX INJECTOR

Optimum Corrective Action

PRE-VALVE SHUTDOWN WHEN EOC IS ATTAINED

NOTE: LOX AND FUEL FLOW METERS IN TEST STAND

* t3 IS A TIME INTERVAL REFERENCE STARTING WHEN X OCCURS

SIGNAL SPACE SEPARATION V 7.1.2

FLOW DISCREPANCY, LOX (FLOWMETER TO INJECTOR)

Stage FIRST, & ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
Q12	(0.0740)(Q12) − 121 = ΔPC2	—		—		0 - 3500 gpm	1800 - 3200
t1	t1.1 > 1.0 SEC	—	—	—	—	—	—
P7-P1	(P7-P1) = ΔPA	—	—	2400 PSID/SEC		0 - 150 PSID	90 - 150 PSID
	χ_2 = 1 FOR ΔPC2 − ΔPA > 0						

Definition of V = 1

V = 1 FOR (χ_2) (V7.1.1)

Malfunction(s) which cause V = 1

SAME AS 7.1.1

Optimum Corrective Action

PRE-VALVE SHUTDOWN

SIGNAL SPACE SEPARATION V 8.1.1

FLOW DISCREPANCY, FUEL FLOWMETER TO INJECTOR

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
Q 11	(0.118)(Q 11) -113 = ΔPC	—		—		0-2200 gpm	1200 - 3000 gpm
t1	t1.1 > 1.0 SEC	—	—	—	—	—	—
P8-P1	(P8-P1) = ΔPA			4000 PSID/SEC		0 - 130 PSID	80-130 PSID
	Y1 = 1 for ΔPC1 - ΔPCA > 0						
t4*	t4.1 > 1.0 SEC						

Definition of V = 1

V=1 for (Y1)(t4.1)(t1.1)(V2.2.1) > 0

Malfunction(s) which cause V = 1

FUEL LEAKS BETWEEN FLOWMETER AND FUEL INJECTOR

Optimum Corrective Action

PRE-VALVE SHUTDOWN WHEN EOC IS ATTAINED

* SEE 7.1.1

SIGNAL SPACE SEPARATION V 8.1.2

FLOW DISCREPANCY, FUEL (FLOWMETER TO INJECTOR)

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
Q11	(0.110)(Q11) − 112 = ΔPC2	—	—	—		0-2200 gpm	1200-2000
t1	t1.1 > 1.0 SEC	—	—	—	—	—	—
P8-P1	(P8-P1)(t1.1) = ΔPA	-	—	4000 PSI/SEC		0-130	80-130
	Y2 = ΔPC2 − ΔPA > 0						

Definition of V = 1

V = 1 for (Y2)($\overline{V8.1.1}$)

Malfunction(s) which cause V = 1

SAME AS 8.1.1

Optimum Corrective Action

PRE-VALVE SHUTDOWN

SIGNAL SPACE SEPARATION V 9.1.1

TURBOPUMP VIBRATION

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
A5	A5.1 > 30 grms	3 grms M ONLY	* -	—	—	0-100 grms 60+600 cps	10-50 grms 60-600 cps

Definition of V = 1

(A5.1)($\overline{V1.1.1}$)

Malfunction(s) which cause V = 1

LUBE SYSTEM, BEARING FAILURES

Optimum Corrective Action

SHUTDOWN WHEN EOC IS ATTAINED

NOTE: BAND PASS FILTER - 3 db DOWN AT 60 AND 500 cps, 12 db/OCTIVE ATTENUATION

* MAINSTAGE OPERATION ONLY

SIGNAL SPACE SEPARATION V 9.1.2

TURBOPUMP VIBRATION

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
A5	A5.2 > 50 grms	3 grms M ONLY	* –	–	–	0 - 1000 grms 60-6000 cps	10-50 grms 60 - 600 cps

Definition of V = 1

(A5.2)($\overline{V1.1.1}$)

Malfunction(s) which cause V = 1

SEE 9.1.1

Optimum Corrective Action

SHUTDOWN WHEN EOC IS ATTAINED

NOTE: BAND PASS FILTER REQ 3 db DOWN AT 60 AND 600 CPS, 12 db/OCTIVE ATTENUATION

* MAINSTAGE OPERATION ONLY

SIGNAL SPACE SEPARATION V 11.1.1

LOSS OF LUBE PRESSURE

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
P9	P9 < 400 PSIA	–	–	–	–	0 - 740 PSIA	350 - 450 PSIA
t1	t1.2 > 1.5 SEC						

Definition of V = 1

(P9)(t1.2)

Malfunction(s) which cause V = 1

LUBE LINE BREAKAGE, FABU FAILURE (CLOGGING, FAIL TO OPEN)

Optimum Corrective Action

SHUTDOWN WHEN EOC IS ATTAINED

SIGNAL SPACE SEPARATION V 13.1.1

EXPLOSION ENGINE AREA

Stage _____

Engine _____

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
PS	$X = \frac{dP_S}{dt} - 100\ PSI/SEC > 0$	—	—	—	—	±2.5 PSID	±2.5 PSID

Definition of V = 1

V = 1 FOR X > 0

Malfunction(s) which cause V = 1

ROUGH COMBUSTION, PROPELLANT ACCUMULATION DUE TO LEAKS, TURBOPUMP RUNAWAY

Optimum Corrective Action

ABORT

NOTE: ΔP SENSOR WITH PNEUMATIC HI PASS NETWORK

SIGNAL SPACE SEPARATION V 15.1.1

HIGH GEARCASE PRESSURE

Stage FIRST, 8 ENGINE

Engine _____

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
P4	P4.1 > 15 psig	–	–	–	50,000 PSI/SEC	0-25 PSIG	4-15 PSIG

Definition of V = 1

P4.1

Malfunction(s) which cause V = 1

LUBE DRAIN FAILURE

Optimum Corrective Action

SHUTDOWN WHEN EOC IS ATTAINED

APPENDIX F

EXPERIMENTAL SYSTEM LAB TEST PROCEDURE

Section V of this report describes a system laboratory test plan, setup, and equipment designed to demonstrate and check out the operation of the experimental READI. To facilitate a rapid, systematic test of the system, a test specification has been prepared. The system test established by this specification is logically divided into sections related to the 18 malfunction detection channels in the H-1 experimental system.

All tests are for demonstrating functional performance; no environmental performance tests are specified. The format of each section of the specification consists of three main parts, namely:

- Catalog of malfunction detection requirements
- Test procedure
- Test results (required and measured).

The test procedure is comprised of four groupings:

- Basic channel test
- Component and information redundancy test
- Transducer self-check test
- Time delay test.

To illustrate the content of the test specification, the V7.1.1 section (Flow Discrepancy, Lox) is reproduced in this Appendix.

The pressure and temperature dials of the transducer simulator described in Section V are graduated directly in the associated physical units, i.e., psi and °F. The frequency sensitive signals generated by the two oscillators, however, are related to the physical quantities by means of curves. These curves are shown in figures F-1, F-2, and F-3 for vibration, speed, and flow variables, respectively. It should be noted that the vibration curves account for the variation in amplitude sensitivity with frequency characteristic of the velocity type pickups selected for the experimental READI.

Reference is made in the test procedure which follows to a "non-alarm" state of simulated signals - both analog and discrete. The input signals must be set at certain values to isolate the malfunction detection channel under test from the other channels to prevent the unwarranted activation of these other channels. For this purpose, non-alarm values are not necessarily those that would exist during engine operation. For example, zero rpm has been selected as the value for turbine speed; however, the system will initiate no action because the main chamber pressure is set at a normal value greater than 420 psia (see catalog malfunction detector V2.1.1 and V2.1.2). The non-alarm simulator settings are shown in table F-1.

TABLE F-1

NON-ALARM SIMULATOR SETTINGS

Transducer Signal	Value
A1 (Both redundant signals)	0 g's, 0 cps
A5	0 g's, 0 cps
N5	0 rpm
Q11	0 gpm
Q12	0 gpm
P1	645 psia
P7-P1	145 psid
P8-P1	100 psid
Transducer Signal	**Value**
P9 (Both redundant signals)	500 psia
P5 (Both redundant signals)	4.5 psig
P4	10 psig

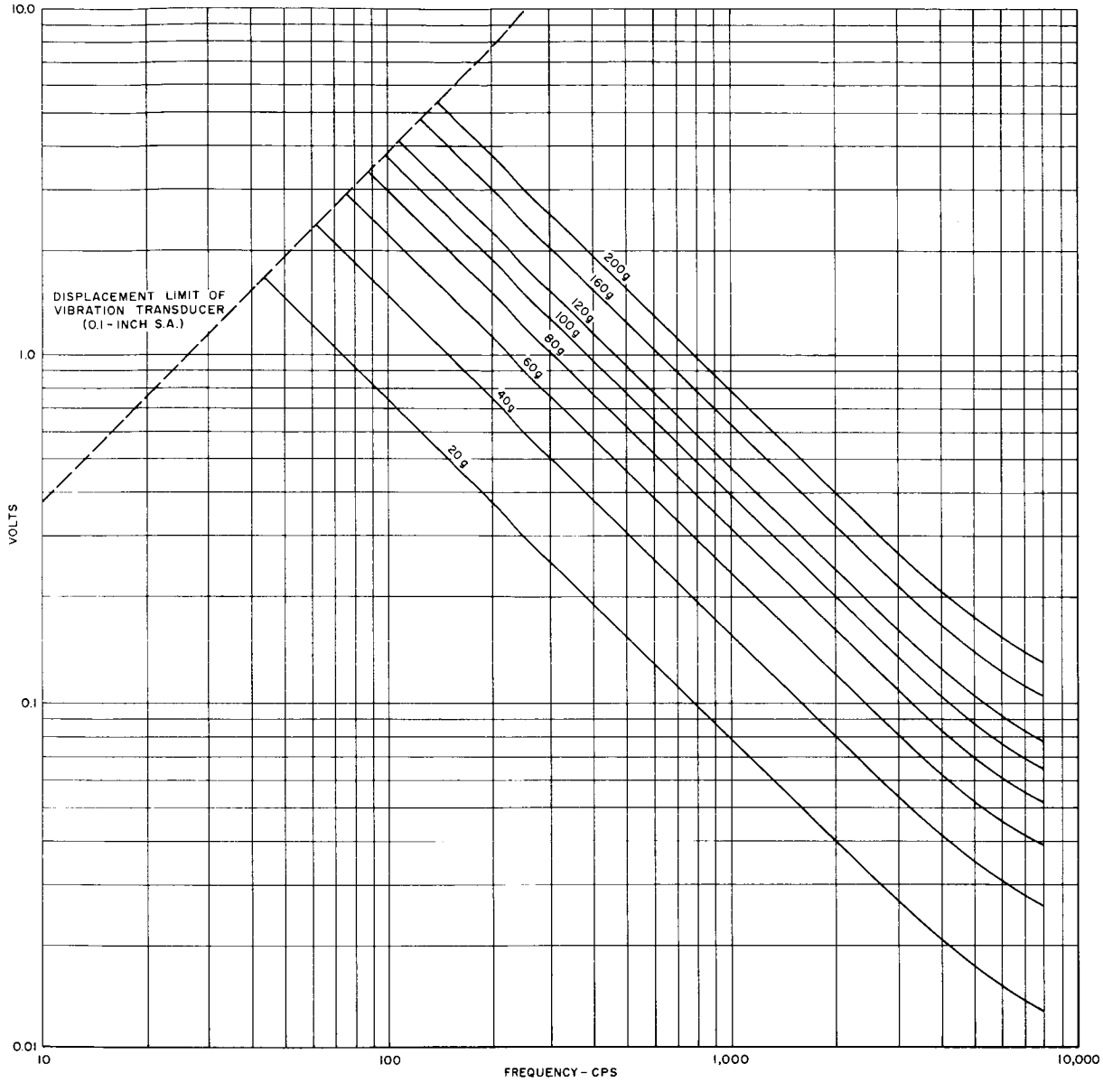


FIGURE F-1

SIGNAL SENSITIVITY OF VIBRATION TRANSDUCER
(VELOCITY PICKUP TYPE)

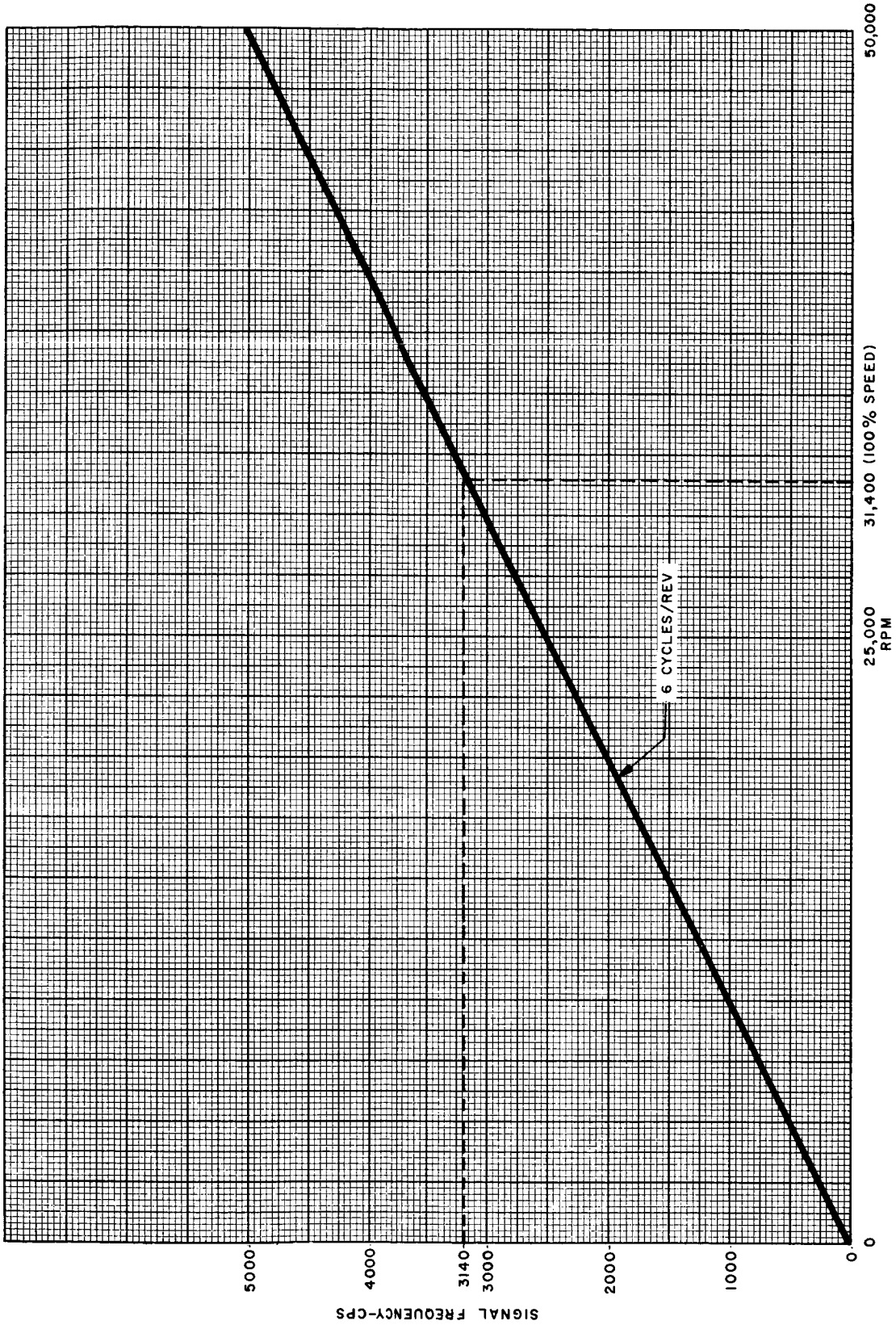


FIGURE F-2
SIGNAL SENSITIVITY FOR TURBINE SPEED (N5)

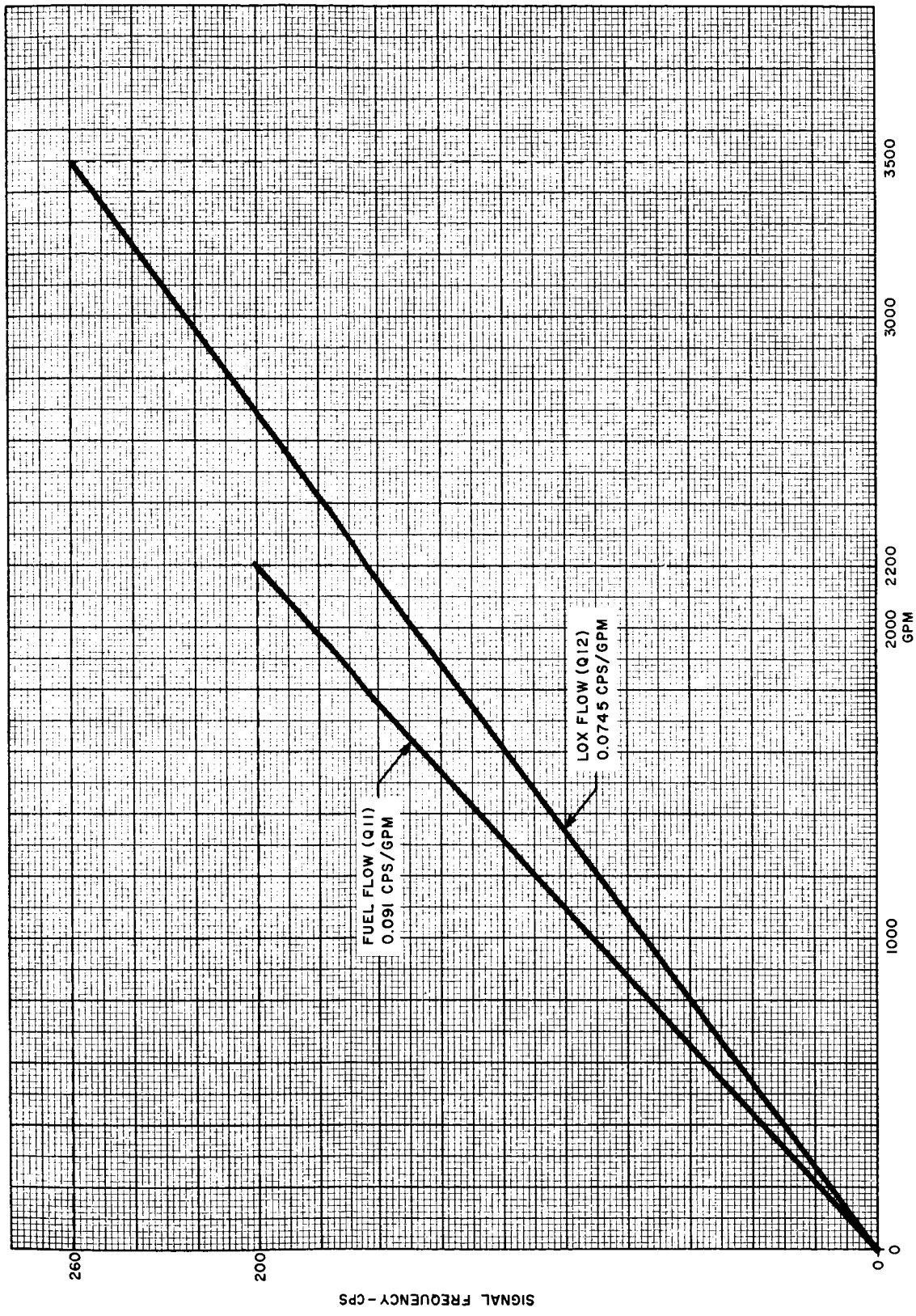


FIGURE F-3

SIGNAL SENSITIVITIES FOR LOX AND FUEL FLOW

TABLE F-1 (Cont)

NON-ALARM SIMULATOR SETTING

Transducer Signal	Value
$Ps-Ps_{Ref.}$ (Blast Press)	0 psid
To	1200°F
T10	1000°F

Switch Signals	Position
Mission Phase Selection	Engine off
Oscillator #1 Selector	Off
Oscillator #2 Selector	Off
Timer test (t2)	Normal
Timer test (t3)	Normal
Event Recorder	Off

(SAMPLE)

SECTION 9 - MALFUNCTION DETECTOR FLOW DISCREPANCY, LOX FLOWMETER TO INJECTOR

PART I - FUNCTIONAL SPECIFICATION

SIGNAL SPACE SEPARATION V 7.1.1

FLOW DISCREPANCY, LOW (FLOWMETER TO INJECTOR)

Stage FIRST, 8 ENGINE

Engine H-1 (188K)

Input Signals	Signal Processing	Signal Self-test Limits: Level Min	Level Max	Rate of Change Max Neg	Rate of Change Max Pos	Signal Range Full	Signal Range Critical
Q12	(0.0793)(Q12) − 121 = ΔPC,			—		0 − 3500 gpm	1800 − 3200 gpm
P7 − P1	(P7 − P1) = ΔPA	—	—	2400 PSI/SEC		0 − 150 PSID	90 − 150 PSID
t1	t1.1 > 1.0 SEC						
	X, = 1 FOR ΔPC, − ΔPA > 0						
t3*	t3.1 > 1.0 SEC						

Definition of V = 1

V = 1 FOR (X,)(t3.1)(t1.1)($\overline{V2.2.1}$)

Malfunction(s) which cause V = 1

LOX LEAKS BETWEEN FLOWMETER AND LOX INJECTOR

Optimum Corrective Action

PRE-VALVE SHUTDOWN WHEN EOC ATTAINED

NOTE: LOX AND FUEL FLOW METERS IN TEST STAND

* t3 IS A TIME INTERVAL REFERENCE STARTING WHEN X OCCURS.

(SAMPLE)

(SAMPLE)

PART II - TEST PROCEDURE

BASIC FUNCTION TEST

1.	Set system to non-alarm condition values.	Normal Conditions
2.	Set oscillator No. 1 selector switch to turbine speed (N5) position.	
3.	Set oscillator No. 2 selector switch to lox flow (Q12) position.	
4.	Set meter switch to oscillator No. 1 position.	
5.	Adjust turbine speed to 33000 rpm at 500 mv.	
6.	Set meter switch to oscillator No. 2 position.	
7.	Adjust Q12 (oscillator No. 2) to 3220 gpm at 500 mv.	
8.	Rotate box injector pressure drop (P7-P1) dial to 145 psid.	
9.	Start event recorder at 5 mm/sec chart speed.	
10.	Rotate mission phase selector switches to all positions and record all V and D traces (channels 1 through 29) on event recorder.	
11.	Set mission phase selector switches to engine off position.	Low injector ΔP due to leak
12.	Stop event recorder.	
13.	Decrease P7-P1 to 125 psid.	
14.	Repeat steps 9 through 12.	
15.	Adjust P7-P1 dial to 145 psid.	High Lox Flow due to leak
16.	Adjust Q12 to 3450 gpm at 500 mv.	
17.	Repeat steps 9 through 12.	
18.	Set Q12 to 3220 gpm at 500 mv.	Large leak, very low injector ΔP
19.	Set P7-P1 dial to 110 psid.	
20.	Repeat steps 9 through 12.	
21.	Adjust N5 to 37,000 rpm at 500 mv.	High turbine speed (V2.2.1)
22.	Repeat steps 9 through 12.	

(SAMPLE)

TRANSDUCER SELF-CHECK

1. Reset N5 to 33,000 rpm at 500 mv, Q12 to 3220 and P7-P1 to 145 psig.
2. Rotate mission phase selector switch to start position.
3. Start event recorder at 5 mm/sec chart speed.
4. Manually connect terminals 49 and 51 of system junction box with jumper wire. (Short output of P7-P1 press. trans.)
5. Repeat Step 10; leave mission phase sw in prime EOC position.

Check maximum negative ΔP rate

6. Remove jumper wire.
7. Lower P7-P1 to 125.
8. Note recorder.
9. Set P7-P1 to 145.
10. Set mission selector sw. to off pos. and stop recorder.

Self check locks out V7.1.1

TIME DELAY TEST

1. Start event recorder at 20 mm/sec chart speed.
2. After 2 seconds, set mission phase selector switch to engine start position.
3. Stop event recorder when channel 9 trace (V7.1.1) appears on event recorder.
4. Record elapsed time between start of channel 30 trace and start of channel 9 trace.

T1.1 and T3 occur in series

5. Set t3 timer switch to "ARM" position
6. Start event recorder at 20 mm/sec chart speed.
7. Set t3 timer switch to test position.
8. Repeat step 3.
9. Record elapsed time between start of channel 29 trace and start of channel 9 trace.

T3 delay verification

(SAMPLE)

COMPONENT REDUNDANCY TEST

1. Reset Q12 to 3220 gpm. 2. Start event recorder at 5 mm/sec speed. 3. Lower P9.1 to 350 psia. 4. Observe recorder for all settings of mission phase SW.	One lube oil pressure transducer indicates low pressure
5. Increase P9.1 to 500 psia and lower P9.2 to 350 psia. 6. Observe recorder for all settings of mission phase SW.	The second transducer indicates low pressure
7. Lower P9.1 to 350 psia. 8. Observe recorder for all settings of mission phase SW.	Both transducers indicate low pressure
9. Increase P9.1 and P9.2 to 500 psia.	
10. Stop Recorder.	

DECISION PRIORITY TEST

1. Start event recorder at 5 mm/sec speed. 2. Lower P7-P1 to 125 psid. 3. Note V and D indication (should be same as step 14) 4. Lower P9.1 and P9.2 to 350 psia. 5. Record V and D indication for all setting of mission phase switch.	D1 (shutdown) has priority over D3 (prevalve shutdown)

(SAMPLE)

PART III - TEST RESULTS

(Numbers indicate channels activated on event recorder)

Basic Function Test

Mission Phase	Step 10		Step 14		Step 17		Step 20		Step 22	
	Req.	Meas.	Req.	Meas.	Req.	Meas.	Req.	Meas.	Req.	Meas.
A Start to Lift-off	none		9		9		9, 27, 28		4	
B L.O. to Alt. EOC	none		9		9		10		4	
C Alt. EOC	none		9		9		10, 27		4	
D Prime EOC	none		9, 27		9, 27		10, 27		4, 25	
E Loss Att. Control	none		9		9		10		4	
F Stage Cut-off	none		9, 27		9, 27		10, 27		4, 25	

Transducer Self-Check Test

	Step 5		Step 8	
	Req.	Meas.	Req.	Meas.
A Start to Lift-off	22			
B LO to Alt. EOC	22			
C Alt EOC	22			
D Prime EOC	22		22	
E Loss Att. Control	22			
F Storage Cut-off	22			

Time Delay Test

Delay	Step	Req'd	Meas.
T1.1 + T3	4	1.8-2.3	
T3	9	1.0-1.3	

(SAMPLE)

PART III - TEST RESULTS (Cont)

	Component Redundancy						Decision Priority	
	Step 4		Step 6		Step 8		Step 5	
	Req.	Meas.	Req.	Meas.	Req.	Meas.	Req.	Meas.
A Start to Lift-off	none		none		15, 28		9,15,28	
B LO to Alt. EOC	none		none		15		9,15	
C Alt EOC	none		none		15, 25		9,15,25	
D Prime EOC	none		none		15, 25		9,15,25	
E Loss Att. Control	none		none		15, 25		9,15	
F Storage Cut-off	none		none		15, 25		9,15,25	

DISTRIBUTION LIST

No. of Copies	
1	Office of Technical Information (Code M-MS-IPC) NASA Marshall Space Flight Center Huntsville, Alabama 35812
1	Contracting Officer (Code MP&C-C) NASA Marshall Space Flight Center Huntsville, Alabama 35812
1	Patent Office (Code M-PAT) NASA Marshall Space Flight Center Huntsville, Alabama 35812
4	Mr. Henry Burlage, Jr. Chief, Liquid Propulsion Systems, RPL
1	Mr. Vernon E. Jaramillo Advanced Manned Mission, MTA
25	Scientific and Technical Information Facility NASA Representative, Code CRT P.O. Box 5700 Bethesda, Maryland 20014
1	(Technical Manager) Mr. Donald Pryor (M-P&VE-PA) NASA Marshall Space Flight Center Huntsville, Alabama 35812
2	Ames Research Center Moffett Field, California 94035 Harold Hornby, Mission Analysis Division
2	Goddard Space Flight Center Greenbelt, Maryland 20771 Merland L. Moseson, Code 623

DISTRIBUTION LIST

No. of Copies	
2	Jet Propulsion Laboratory California Institute of Technology 4800 Oak Grove Drive Pasadena, California 91103 Robert F. Rose, Propulsion Div., 38
2	Langley Research Center Langley Station Hampton, Virginia 23365 Floyd L. Thompson, Director
2	Lewis Research Center 21000 Brookpark Road Cleveland, Ohio 44135 Dr. Abe Silverstein, Director
2	Marshall Space Flight Center Huntsville, Alabama 35812 Hermann K. Weidner, Code M-P&VED
2	Manned Spacecraft Center Houston, Texas 77001 Robert R. Gilruth, Director
1	Advanced Research Projects Agency Washington 25, D.C. D. E. Mock
1	Aeronautical Systems Division Air Force Systems Command Wright-Patterson Air Force Base Dayton, Ohio D. L. Schmidt, Code ASRCNC-2
1	Air Force Missile Development Center Holloman Air Force Base, New Mexico Maj. R. E. Bracken, Code MDGRT
1	Air Force Missile Test Center Patrick Air Force Base, Florida L. J. Ullian
1	Air Force Systems Command, Dyna-Soar Air Force Unit Post Office Los Angeles 45, California Col. Clark, Technical Data Center

DISTRIBUTION LIST

No. of Copies	
1	Arnold Engineering Development Center Arnold Air Force Station Tullahoma, Tennessee Dr. H. K. Doetsch
1	Bureau of Naval Weapons Department of the Navy Washington 25, D. C. J. Kay, Code RTMS-41
1	Central Intelligence Agency 2430 E Street, N. W. Washington 25, D. C. Attn: Miss Elizabeth F. Kernan
1	Defense Documentation Center Headquarters Cameron Station, Building 5 5010 Duke Street Alexandria, Virginia 22314 Attn: TISIA
1	Headquarters, U. S. Air Force Washington 25, D. C. Col. C. K. Stambaugh, Code AFRST
1	Picatinny Arsenal Dover, New Jersey I. Forsten, Chief Liquid Propulsion Laboratory
1	Rocket Research Laboratories Edwards Air Force Base Edwards, California Col. H. W. Norton
1	U. S. Atomic Energy Commission Technical Information Services Box 62 Oak Ridge, Tennessee
1	U. S. Army Missile Command Redstone Arsenal, Alabama 35809 Dr. Walter Wharton
1	U. S. Naval Ordnance Test Station China Lake, California 93557 E. Yim, Jr., Code 451 Chief, Missile Propulsion Division

DISTRIBUTION LIST

No. of Copies	
1	Chemical Propulsion Information Agency Johns Hopkins University Applied Physics Laboratory 8621 Georgia Avenue Silver Springs, Maryland Neil Safeer
1	Aerojet-General Corporation P. O. Box 296 Azusa, California L. F. Kohrs
1	Aerojet-General Corporation P. O. Box 1947 Technical Library, Bldg 2015, Dept. 2410 Sacramento 9, California R. Stiff
1	Aeronutronic A Division of Ford Motor Company Ford Road Newport Beach, California D. A. Carrison
1	Aerospace Corporation 2400 East El Segundo Boulevard P. O. Box 95085 Los Angeles, California 90045 John G. Wilder, MS-2293 Propulsion Dept.
1	Arthur D. Little, Inc. Acorn Park Cambridge 40, Massachusetts A. C. Tobey
1	Astropower, Inc., Subsidiary of Douglas Aircraft Company 2968 Randolph Avenue Costa Mesa, California Dr. George Moc Director, Research
1	Astrosystems, Inc. 1275 Bloomfield Avenue Caldwell Township, New Jersey A. Mendenhall

DISTRIBUTION LIST

No. of Copies	
1	Atlantic Research Corporation Edsall Road and Shirley Highway Alexandria, Virginia A. Scurlock
1	Beech Aircraft Corporation Boulder Facility Box 631 Boulder, Colorado J. H. Rodgers
1	Bell Aerosystems Company P. O. Box 1 Buffalo 5, New York W. M. Smith
1	Bendix Systems Division Bendix Corporation Ann Arbor, Michigan John M. Brueger
1	Boeing Company P. O. Box 3707 Seattle 24, Washington J. D. Alexander
1	Chrysler Corporation Missile Division Warren, Michigan John Gates
1	Curtiss-Wright Corporation Wright Aeronautical Division Wood-Ridge, New Jersey G. Kelley
1	Douglas Aircraft Company, Inc. Missile and Space Systems Division 3000 Ocean Park Boulevard Santa Monica, California 90406 R. W. Hallet, Chief Engineer Advanced Space Tech.
1	Fairchild Stratos Corporation Aircraft Missiles Division Hagerstown, Maryland J. S. Kerr

DISTRIBUTION LIST

No. of Copies	
1	General Dynamics/Astronautics Library & Information Services (128-00) P.O. Box 1128 San Diego, California 92212 Frank Dore
1	General Electric Company Missile and Space Vehicle Department 3198 Chestnut Street, Box 8555 Philadelphia 1, Pennsylvania L. S. Beers
1	General Electric Company Flight Propulsion Lab Department Cincinnati 15, Ohio D. Suichu
1	Grumman Aircraft Engineering Corp. Bethpage, Long Island, New York Joseph Gavin
1	Kidde Aero-Space Division Walter Kidde and Company, Inc. 675 Main Street Belleville 9, New Jersey R. J. Hanville Director of Research Engineering
1	Lockheed California Company 10445 Glen Oaks Boulevard Pacoima, California G. D. Brewer
1	Lockheed Missiles and Space Company Attn: Technical Information Center P.O. Box 504 Sunnyvale. California Y. C. Lee Power Systems R&D
1	Lockheed Propulsion Company P.O. Box 111 Redlands, California H. L. Thackwell
1	The Marquardt Corporation 16555 Saticoy Street Box 2013 - South Annex Van Nuys, California D. L. Walter

DISTRIBUTION LIST

No. of Copies	
1	Martin Division Martin Marietta Corporation Baltimore 3, Maryland John Calathes (3214)
1	Martin Denver Division Martin Marietta Corporation Denver, Colorado J. D. Goodlette Mail A-241
1	McDonnell Aircraft Corporation P. O. Box 6101 Lambert Field, Missouri R. A. Herzmark
1	North American Aviation, Inc. Space & Information Systems Division Downey, California H. Storms
1	Northrop Corporation 1001 East Broadway Hawthorne, California W. E. Gasich
1	Pratt & Whitney Aircraft Corp. Florida Research and Development Center P. O. Box 2691 West Palm Beach, Florida R. J. Coar
1	Radio Corporation of America Astro-Electronics Division Defense Electronic Products Princeton, New Jersey S. Fairweather
1	Reaction Motors Division Thiokol Chemical Corporation Denville, New Jersey 07832 Arthur Sherman
1	Republic Aviation Corporation Farmingdale, Long Island, New York Dr. William O'Donnell

DISTRIBUTION LIST

No. of Copies	
1	Rocketdyne (Library Dept. 586-306) Division of North American Aviation 6633 Canoga Avenue Canoga Park, California 91304 E. B. Monteath
1	Space General Corporation 9200 Flair Avenue El Monte, California C. E. Roth
1	Space Technology Laboratories Subsidiary of Thompson-Ramo-Wooldridge P. O. Box 95001 Los Angeles 45, California G. W. Elverum
1	Stanford Research Institute 333 Ravenswood Avenue Menlo Park, California Thor Smith
1	TAPCO Division Thompson-Ramo-Wooldridge, Inc. 23555 Euclid Avenue Cleveland 17, Ohio P. T. Angell
1	Thiokol Chemical Corporation Redstone Division Huntsville, Alabama W. L. Berry
1	United Aircraft Corporation Research Laboratories 400 Main Street East Hartford 8, Connecticut Erle Martin
1	United Technology Center 587 Methilda Avenue P. O. Box 358 Sunnyvale, California B. Abelman
1	Vought Astronautics Box 5907 Dallas 22, Texas Warren C. Trent