General Disclaimer

One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.

- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.

- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.

- This document is paginated as submitted by the original source.

- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

Produced by the NASA Center for Aerospace Information (CASI)

CR-

~~NAS10-7072~~
TR-1087

STUDY OF TECHINQUES FOR REDUNDANCY VERIFICATION WITHOUT DISRUPTING SYSTEMS

Radiation Incorporated
Systems Division
Melbourne, Florida 32901

September 1970

Summary Report, Phases I, II and III

Contract No. NAS10-7072

Prepared for

JOHN F. KENNEDY SPACE CENTER, NASA
Kennedy Space Center, Florida 32899

ERRATA

for

SUMMARY REPORT, PHASES I, II, and III

STUDY OF TECHNIQUES FOR REDUNDANCY VERIFICATION WITHOUT DISRUPTING SYSTEMS

Above Report Published

September 1970

FACILITY FORM 602

N71-13900
(ACCESSION NUMBER)

275
(PAGES)

CR-111765
(NASA CR OR TMX OR AD NUMBER)

(THRU)

G3
(CODE)

10
(CATEGORY)

The following corrections should be made to the report named on the cover of these errata:

1.	page 2-11	On the line fifth from the bottom of the page, insert the word "be" between "not" and "feasible".
2.	page 3-3	Replace Figure 3.0-1 with Figure 3.0-1 hereto attached.
3.	page 5-93	Replace Figure 5.3.1-5 with Figure 5.3.1-5 hereto attached.
4.	page 5-95	Replace Figure 5.3.1-7 with Figure 5.3.1-7 hereto attached.

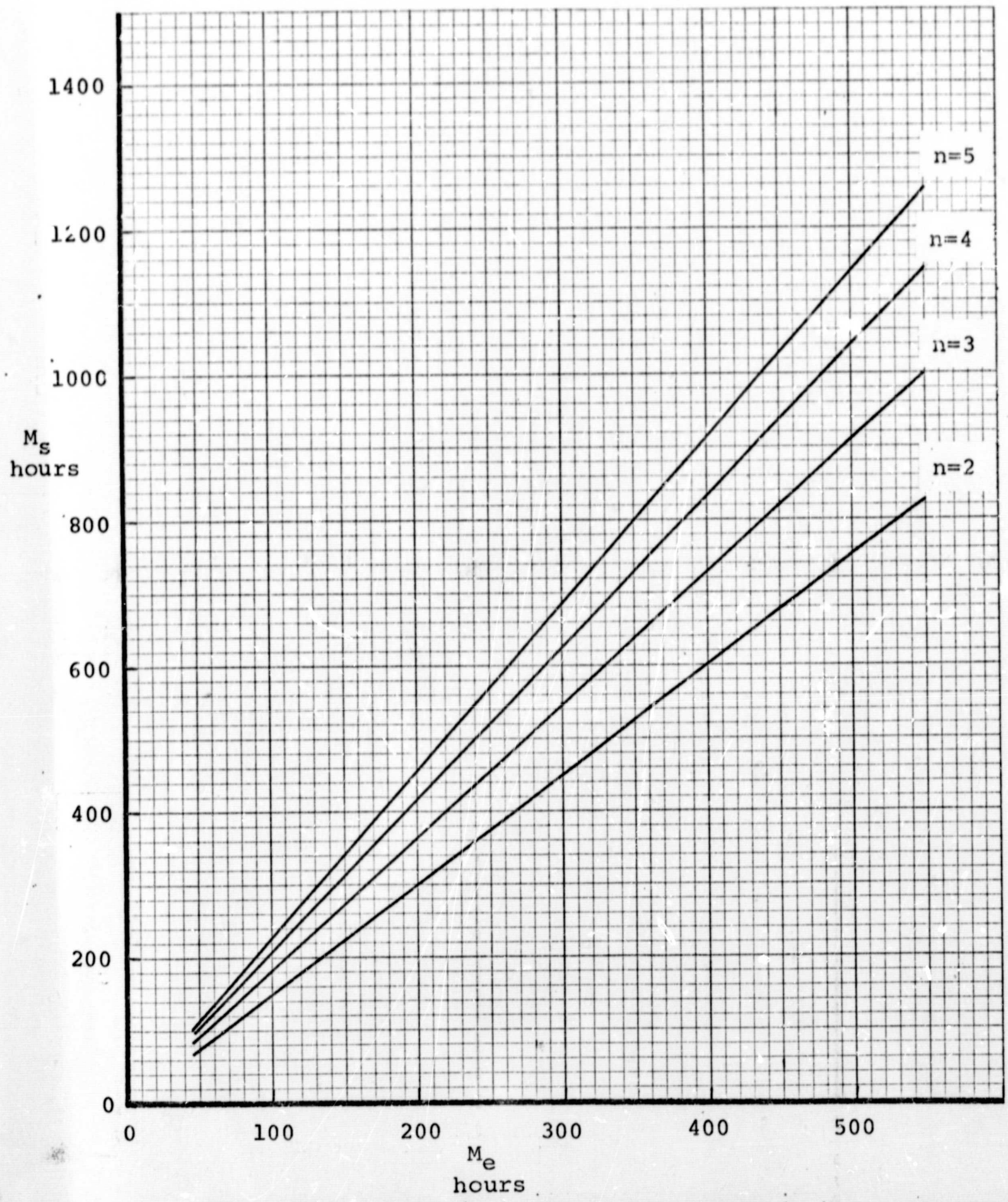


Figure 3.0-1. Plot of Set MTBF (M_s) vs. Element MTBF (M_e) For the Number Of Elements (n) Ranging From Two To Five - Unmaintained Redundancy

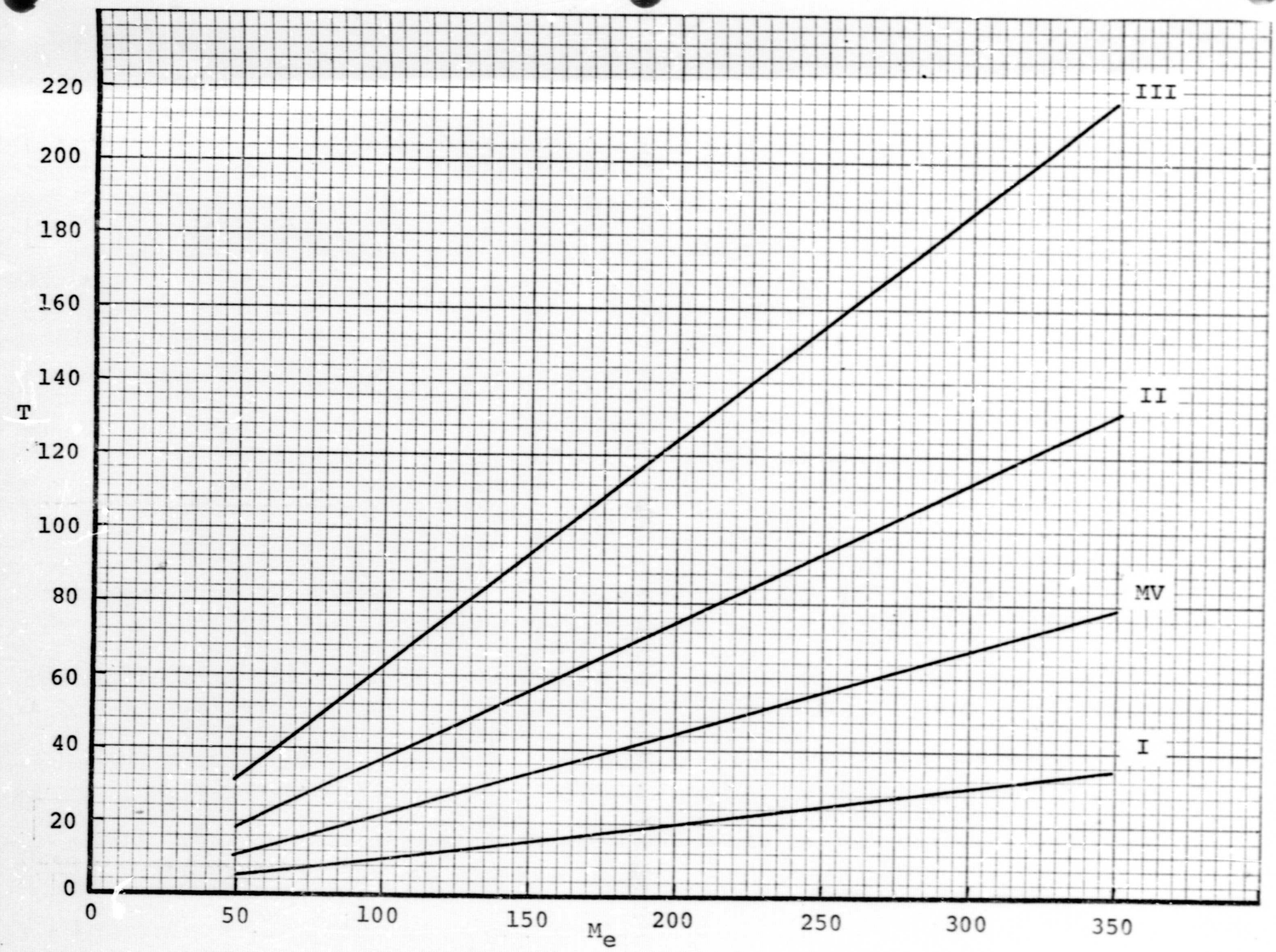


Figure 5.3.1-5. Comparison of Simple Sets; Two Success Criteria
Lines of Equal Probability $1-\alpha = 0.90$

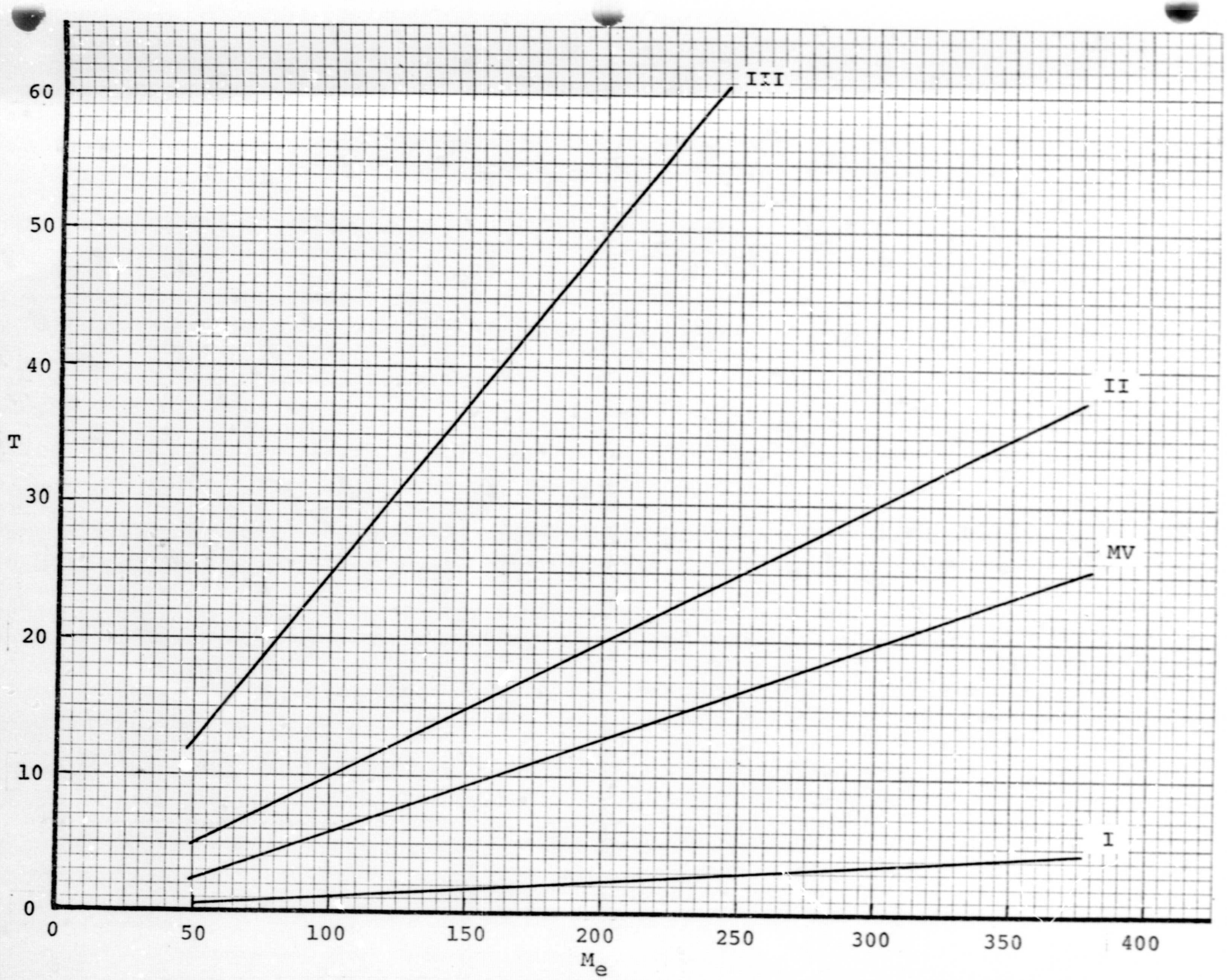


Figure 5.3.1-7. Comparison of Simple Sets; Two Success Criteria
Lines of Equal Probability $1-\alpha = 0.99$

NOTICE

This report was prepared as an account of Government-sponsored work. Neither the United States, nor the National Aeronautics and Space Administration (NASA), nor any person acting on behalf of NASA.

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately-owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method or process disclosed in this report.

As used above, "person acting on behalf of NASA" includes any employee or contractor of NASA, or employee of such contractor, to the extent that such employee or contractor of NASA or employee of such contractor prepares, disseminates, or provides access to any information pursuant to his employment or contract with NASA, or his employment with such contractor.

TECHNICAL REPORT STANDARD TITLE PAGE

1. Report No. NAS10-7072	2. Government Accession No. Blank	3. Recipient's Catalog No.
4. Title and Subtitle: Study of Techniques for Redundancy Verification without Disrupting Systems		5. Report Date: September 1970 6. Performing Organization Code: Blank
7. Author(s): Radiation Inc.		8. Performing Organization Report No.: TR-1087
9. Performing Organization Name and Address: Radiation Incorporated, Systems Division, Melbourne, Florida 32901		10. Work Unit No.: 908-62-15-26-00 11. Contract or Grant No.: NAS10-7072
12. Sponsoring Agency Name and Address: John F. Kennedy Space Center, NASA, Kennedy Space Center, Florida 32899		13. Type of Report and Period Covered: Summary Report, Phases I, II and III 14. Sponsoring Agency Code: Blank

15. Supplementary Notes: None

16. Abstract: This work addresses the problem of verifying the operational integrity of redundant equipments and the impact of a requirement for verification on such equipments.

Redundant circuits are examined and the characteristics which determine adaptability to verification are identified. Mutually exclusive and exhaustive categories for verification approaches are established. The range of applicability of these techniques is defined in terms of signal characteristics and redundancy features. Verification approaches are discussed and a methodology for the design of redundancy verification is developed.

The new methodology is exercised through a case study which involves the design of a verification system for a hypothetical communications system.

Design criteria for redundant equipments are presented. These criteria assure adaptability of these equipments to automated verification. Recommendations for the development of technological areas pertinent to the goal of increased verification capabilities are given.

17. Key Words (Selected by Author(s))	18. Distribution Statement		
Redundancy Verification Status Resolution Automatic Checkout Equipment Reliability of Redundant Systems	Unclassified - Unlimited		
19. Security Classif. (of this report): Unclassified	20. Security Classif. (of this page): U	21. No. of Pages: 274	22. Price

TABLE OF CONTENTS

Section/Paragraph	Title	Page
1.0	INTRODUCTION	1-1
2.0	REDUNDANCY CLASSIFICATIONS AND THE STATUS IDENTIFICATION PROBLEM	2-1
2.1	Classifications of Redundancy	2-1
2.2	A General Look at Status Identification	2-8
2.3	Conclusions	2-13
3.0	WHY REDUNDANCY VERIFICATION	3-1
4.0	SOME GENERAL CONCEPTS	4-1
4.1	The Implications of Redundancy Verification	4-1
4.2	Functional Descriptions of Signals	4-2
4.3	The Notions of Groups and Sets	4-2
4.4	The Implications of Time	4-4
4.5	The Relationship of Verification to On-Line and Off-Line Elements	4-7
4.6	Some Additional Points About Status of Redundant Sets	4-8
5.0	DESIGNING REDUNDANCY VERIFICATION - A DESIGN PROCESS AND CONSIDERATIONS	5-1
5.1	Design Inputs	5-1
5.1.1	Design Confidence	5-2
5.1.2	Properties Indicative of Operation and Their Status Relationships	5-3
5.1.3	Time Profiles and System Partitioning	5-6
5.1.4	The Group Policy	5-7
5.2	The Design Process	5-8
5.2.1	The Higher Level Group Problem	5-12
5.2.1.1	Isolation/Independence Plan	5-12
5.2.1.2	Policy for Treating Off-Line Elements	5-12
5.2.1.3	Determination of Status Resolution and Status Reporting	5-13
5.2.1.4	Relationship to a Central Processor	5-14
5.2.2	The Set Problem	5-14
5.2.2.1	Functions to be Performed	5-15
5.2.2.2	Coincidence Development	5-18
5.2.2.3	Parameter Estimation and Status Variables	5-31
5.2.2.4	Mapping into Conditional Status	5-35
5.2.2.5	Sample Coincidence Development Implementations	5-35

TABLE OF CONTENTS (Continued)

Section/Paragraph	Title	Page
5.2.2.5.1	Output/Output Comparisons	5-37
5.2.2.5.2	Output to Reference Comparisons	5-41
5.2.2.5.3	Output to Input Comparisons	5-71
5.2.3	The Group Problem	5-78
5.2.3.1	Exhaustive Deduction	5-80
5.2.3.2	Iterative Deduction	5-81
5.2.3.3	Logical Deduction	5-83
5.3	Other Design Considerations	5-86
5.3.1	Continuous Verification and the Dedication of Equipment to Verification	5-86
5.3.2	Implications of Sharing Verification Devices	5-102
5.4	Relationships to a Central Processor and Existing Ace Techniques	5-104
5.4.1	Automation Considerations	5-104
5.4.2	Digital Processing Applicability	5-105
5.4.3	Redundancy Verification Functional Flow	5-106
5.4.4	Central Processing Options	5-106
5.4.4.1	Case I	5-110
5.4.4.2	Case II	5-110
5.4.4.3	Case III	5-110
5.4.4.4	Case IV	5-111
5.4.5	Programming Considerations	5-111
5.4.6	Existing ACE Techniques	5-112
5.5	Summary of the Process	5-114
5.5.1	Establishing the Framework.	5-114
5.5.2	The General Group Problem	5-115
5.5.3	The Set Problem	5-115
5.5.4	Design Outputs	5-116
6.0	DEVELOPMENT OF DESIGN CRITERIA AND IDENTIFICATION OF NEW TECHNOLOGY	6-1
6.1	Verifiability	6-1
6.2	Design Criteria	6-3
6.3	New Technology	6-6
6.4	Technology Development Plan	6-9
6.4.1	Current Sensors and "No-Touch" Sensing	6-10
6.4.2	Devices for Combining Element Outputs	6-12
6.4.3	Multiplexing Techniques	6-13
6.4.4	Sampling Spectrum Analyzers	6-13

TABLE OF CONTENTS (Continued)

Section/Paragraph	Title	Page
7.0	A CASE STUDY	7-1
7.1	The Hypothetical System	7-1
7.2	Redundancy Verification Design	7-2
8.0	CONCLUSIONS AND RECOMMENDATIONS	8-1
8.1	Conclusions	8-1
8.2	Recommendations	8-3
	APPENDICES	
A	DISCUSSIONS OF COINCIDENCE DEVELOPMENT TECHNIQUES	A-1
B	TECHNICAL DESCRIPTION HCDL-ERS	B-1
C	CASE STUDY DESIGN DESCRIPTION AND SOLUTION	C-1
D	PERFORMANCE AND DESIGN REQUIREMENTS SPECIFICATION FOR REDUNDANT EQUIPMENTS	D-1
	GLOSSARY	1

LIST OF ILLUSTRATIONS

Figure	Title	Page
2.1-1.	Redundancy Design Flow Chart	2-2
2.1-2.	Redundancy Classification, Exhaustive Enumeration	2-7
2.2.	Status Identification Process Flow Chart	2-9
2.3	Classification of Redundancy Features for Simple Sets with Regard to Verification	2-14
3.0-1.	Plot of Set MTBF (M_s) vs. Element MTBF (M_e) for the Number of Elements (n) Ranging from Two to Five - Unmaintained Redundancy	3-3
3.0-2.	Plot of Set MTBF (M_s) vs. Element MTBF (M_e) for Average Element Down Time (D) = 1/2,1,2 - Redundancy with Immediate Repair.	3-5
3.0-3.	Plot of Set MTBF (M_s) vs. Element MTBF (M_e) for Three Durations Between Verification (T) - Redundancy with Deferred Maintenance	3-7
4.2.	Signal Relationships	4-3
4.3-1.	Examples of Two Redundancy Configurations	4-5
4.3-2.	The Relationship of Redundancy Verification to Redundancy.	4-6
4.6.	The Relationship of the Status Variable and Conditional Status.	4-9
5.1.3.	Sample System Showing Identification of Groups and Sets, Functional Diagram	5-9
5.2.	The Redundancy Verification Design Process	5-11
5.2.2.1-1.	Verification Functions - Set Problem	5-16
5.2.2.1-2.	Example of Verification Functions	5-17
5.2.2.2-1.	Approaches to Coincidence Development	5-19
5.2.2.2-2.	Examples of Coincidence Development Techniques	5-21
5.2.2.2-3.	Examples of Coincidence Development Techniques	5-23
5.2.2.2-4.	Examples of Coincidence Development Techniques	5-24
5.2.2.2-5.	Applicability Matrix	5-27
5.2.2.2-6.	Selection Process for Coincidence Development Techniques.	5-30
5.2.2.3-1.	Illustration of Parameter Estimation	5-32
5.2.2.3-2.	Derived and Stored Impulse Responses	5-34
5.2.2.4.	Status Mapping Truth Table	5-36
5.2.2.5.1-1.	Compare Two - Digital	5-38
5.2.2.5.1-2.	Compare Two - Analog	5-39
5.2.2.5.1-3.	Voting	5-40
5.2.2.5.1-4.	Threshold Voter, Schematic Diagram	5-42
5.2.2.5.1-4.	Disagreement Detector Circuit	5-43

LIST OF ILLUSTRATIONS (Continued)

Figure	Title	Page
5.2.2.5.1-6.	Switchable Voter, Schematic	5-44
5.2.2.5.2-1.	Valve Check Sequential	5-46
5.2.2.5.2-2.	Valve Check Sequential	5-47
5.2.2.5.2-3.	Valve Checks Nonsequential	5-48
5.2.2.5.2-4.	Coding Parity Checks	5-50
5.2.2.5.2-5.	1-Bit Parity Check System	5-51
5.2.2.5.2-6.	Coding	5-53
5.2.2.5.2-7.	Pseudorandom Sequence Generator	5-54
5.2.2.5.2-8.	Signal Form Analysis.	5-56
5.2.2.5.2-9.	Mean Machine I	5-57
5.2.2.5.2-10.	Mean Machine II	5-58
5.2.2.5.2-11.	Integrator and Interval Timer	5-59
5.2.2.5.2-12.	Peak Machine	5-61
5.2.2.5.2-13.	MS Machine	5-62
5.2.2.5.2-14.	Instantaneous Frequency Machine	5-64
5.2.2.5.2-15.	Complete Spectrum Analysis	5-65
5.2.2.5.2-16.	Partial Spectrum Analysis	5-67
5.2.2.5.2-17.	Acknowledgment	5-68
5.2.2.5.2-18.	Acknowledgment	5-69
5.2.2.5.3-1.	Inverse Transform	5-72
5.2.2.5.3-2.	Inverse Transform	5-75
5.2.2.5.3-3.	Cross Correlation	5-76
5.2.2.5.3-4.	Time Domain Reflectometry	5-77
5.2.3.3.	Logical Deduction - An Illustrative Example	5-84
5.4.3.	Redundancy Verification Functional Flow	5-107
5.4.4.	Central Processing Configuration	5-108
5.4.6.	Automatic Testing Functional Flow	5-113
6.4.1-1.	Development Plan - Current and "No Touch" Sensing Devices	6-11
A3.	Voting Techniques - Some Sample Implementations	A-8
B2.0.	ERS Operations Profile - Site A	B-4
B2.2.	Channel Utilization Profiles	B-5
B4.2.	Downlink Spectra and Bandpass	B-8
B4.3.	Link Budget	B-10
B4.4.	TLM Format	B-11
B4.6.	ERS Functional Block Diagram	B-13
B4.6.4.	Frequency Spectrum at Output of Voice Channel Demodulator	B-17

LIST OF ILLUSTRATIONS (Continued)

Figure	Title	Page
C2.1-1.	ERS Block Diagram	C-3
C2.2-1.	Typical Isolation Schemes for Tap Points	C-6
C2.4-1.		C-7
C2.5-1.		C-9
C4.1-1.	Typical Power Spectrum for Conversational English	C-14
C4.1-2.	ERS Functional Block Diagram with Verification Equipment in Place	C-17

LIST OF TABLES

Number	Title	Page
2.2	Reasons for an Approach Not Being Feasible	2-12
5.3.1	Probability of Being Down to Exactly One Element for the Two and Three Element Sets	5-97
B4.2	Modulation Summary	B-9

1.0 INTRODUCTION

This report presents the unified results of Phases I, II, and III of the above-named study.

The study effort was divided into three phases. Phase I concerned itself with the achievement of redundancy w th emphasis on the special requirements placed on redundancy by a need for automated verification. The investigations of the first phase resulted in the identification of those features of redundancy which are important to the purpose of verification and the establishment of classes into which redundant situations may be placed.

While Phase I of the study developed characteristics which a redundancy design must possess to be amenable to automated redundancy verification, Phase II developed techniques for achieving this verification. There are two fundamental approaches which can be taken in the attack of this problem: (a) specify in detail some relatively small number of specific (and presumable typical) cases and develop detailed solutions to each, or (b) address the general problem and exploit the methodology for achieving solutions. The former attack has the advantage of achieving immediate results for those cases selected. But what about other cases which may be important in the future or under different circumstances? A casual examination of the problem reveals the wide variety of conditions which can arise and which a specific design must satisfy. How do the few selected, detailed solutions relate to solutions under other circumstances? What problems are "typical?" What is typical today may not be typical five years from now under the advancing state-of-the-art.

The above questions are quite pertinent and the inference which can be drawn when attempting to answer them is equally pertinent--unless a redundancy verification methodology is developed, each problem which arises will be an isolated case to be solved from the very beginning with only isolated (and usually intuitively) related experience gained from proceeding problems. Under these circumstances, it is difficult at best to forecast the impact of redundancy verification on a system design. For without such a forecast, the system design must proceed virtually uninfluenced by the verification requirement until each verification problem is solved. The end result is either that redundancy verification design becomes an afterthought to fit as it might or else that significant (in terms of cost and time) perturbations are introduced into the system design process as the design inevitably folds back for reiteration.

The impact of redundancy verification on a system design is considered the most significant and heretofore most wanting area in this field. The study team is not aware of, or has a source been located which describes, a methodology for redundancy verification. For these reasons, the word "techniques" was interpreted literally and the approach to the problem was not one of detailed development of specific cases, but rather one of development of methodology. Probably the single most important advantage of a methodology is its power to allow inference to be drawn about a related collection of design circumstances. For it

is here that the similarities and differences in individual design approaches can be ascertained and statements can be made collectively about common points in many approaches based on the methodology. Implicit to these statements is the necessity of developing "grounds for commonality," identifying pertinent characteristics which describe the problem and last but not least, identifying the problem and its interfaces in detail. To achieve these ends, it became necessary to develop the methodology from the ground up; complete with definitions and algorithms. The end result is believed to be a comprehensive discipline and a fresh approach to an old problem. It is not claimed that the results are the optimum solution or even that they represent the only solution, only that they represent an acceptable solution. No apologies are made for the lack of elegance in the development since the emphasis has been placed on a usable solution and it is felt that this has been achieved.

The third phase addressed itself to the treatment of "unverifiable" situations. The problem was attacked by scrutinizing the meaning of verifiability and identifying the things which can cause a situation to become classed as "unverifiable." This having been done design criteria were developed to aid in the avoidance of such situations and technological advances were suggested to aid in the alteration to a verifiable form of such situations.

Considering the specific sections of this report, Section 2.0 presents a system which was developed for the classification of redundancy and relates the redundancy verification problem of status identification.

Section 3.0 reflects on the need for automated redundancy verification and examine the role of redundancy and its verification under varying maintenance policies and mission profiles.

Section 4.0 presents, in detail, the redundancy verification methodology developed in Phase II.

Section 5.0 presents the design processes, guidelines, and considerations which have been identified as being integral to the implementation of redundancy verification.

Section 6.0 outlines the development of design criteria and presents plans for the development of technologies deemed profitable in the pursuit of expanded verification capabilities.

Section 7.0 discusses the reasons for undertaking a case study and the nature of the case selected for the exercise.

Section 8.0 presents conclusions and recommendations.

Appendix A is a series of discussions on the various coincidence development techniques and enumerates the advantages and disadvantages of each.

Appendix B is a technical description of the system chosen as a case study.

Appendix C gives the solution to the verification problem chosen as a case study.

Appendix D presents the design criteria of Section 6.2 in a form consistent with NHB 8040.2.

Also included is a glossary of the terms developed and employed throughout the study.

The reader should note that this work is devoted to automated redundancy verification. Wherever statements about redundancy verification appear, it should be understood that functions involved are to be in an automated fashion.

2.0 REDUNDANCY CLASSIFICATIONS AND THE STATUS IDENTIFICATION PROBLEM

As indicated in Section 1.0, one of the purposes of this report is to develop a methodology for automated redundancy verification. To achieve this end, it will be necessary to investigate the interfaces, constituents and ramifications of redundancy verification. It is obvious that the investigation should commence by examining the concepts of redundancy. But what is less obvious are the interrelationships between redundancy, various applications and verification techniques and their affect on the final results. Can redundancy approaches be described independent of applications? Will the description of a redundancy approach be sufficient to determine a verification technique? What features should be used to describe a redundancy approach? Is it possible to devise a single scheme which will describe redundancy approaches and verification techniques? These are the most pertinent questions which come to mind on addressing the problem and each must ultimately be answered.

2.1 Classifications of Redundancy

Let us begin by considering redundancy concepts, but in a special light--that of automated verification. The major considerations in a redundancy design are shown in Figure 2.1-1. On examining this figure two points immediately become obvious.

a. There are a large number of features required to describe a redundancy approach. This quantity must, in some fashion, be reduced to a manageable size if usable results are to be achieved.

b. A classification scheme must be developed from the features such that detailed approaches can be described collectively based on commonality of features. If this cannot be accomplished there will be a hopeless patchwork of descriptions, terms and techniques.

There is a third consideration of importance but which is less obvious from the figure. This is the independence of the fault detect/recovery scheme and the complexity of redundant equipment. It is not difficult to cite examples of elaborate fault detection schemes under which redundant equipments are not independent. It is also easy to envision complex equipments with multiple inputs and outputs or equipments which perform multiple functions. If any headway is to be made in determining classifications for redundancy, consideration of these complications must be deferred until a foothold is gained on the fundamental problem. The rationale for developing redundancy classifications is contained in the paragraphs that follow. Throughout the discussion the following simplifying assumptions hold.

- Instances of redundancy are treated as entities.
- The operation of all (both on-line and off-line) equipments is to be verified.
- Equipments are considered dedicated solely to the single input-single output operation.

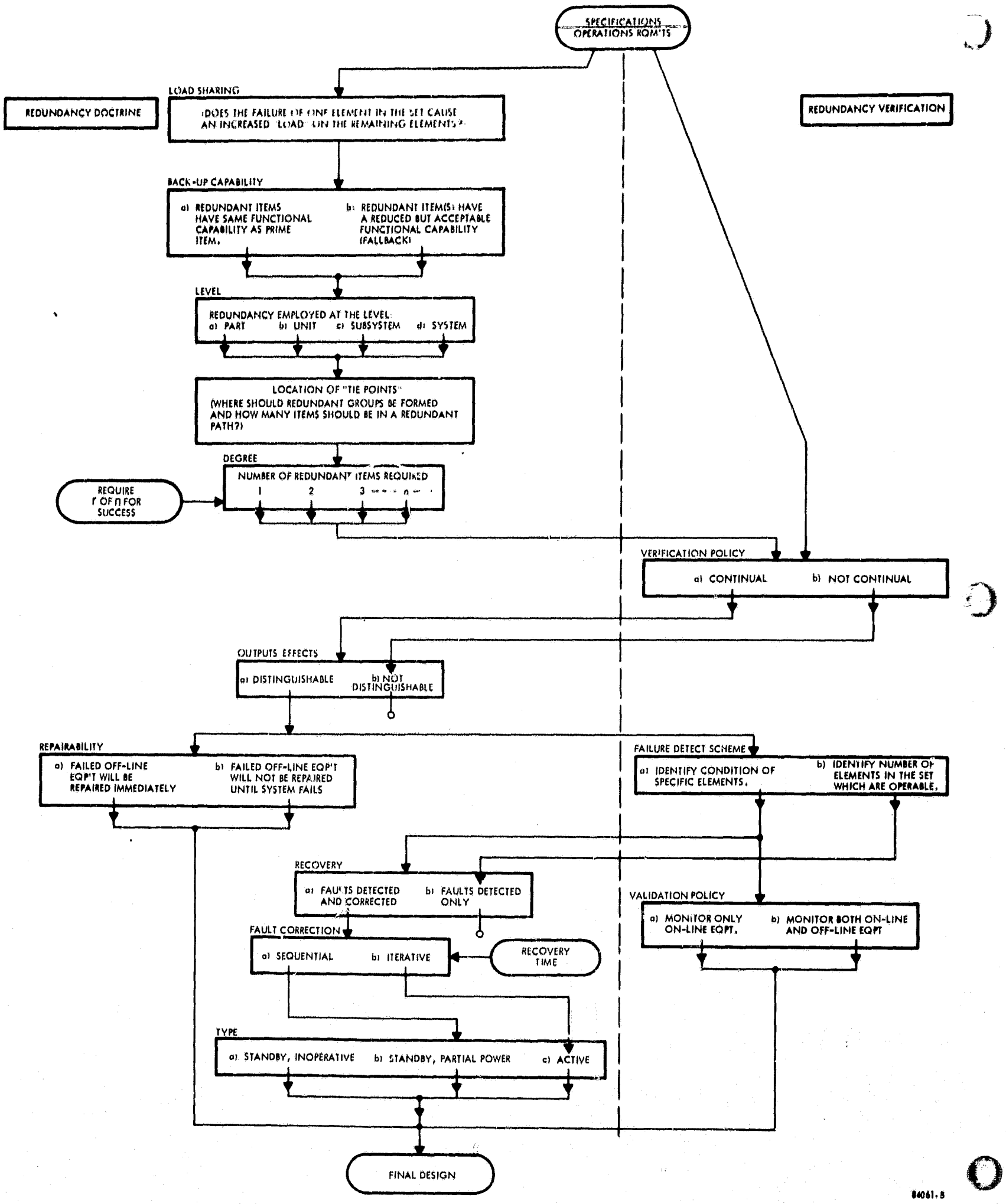


Figure 2.1-1. Redundancy Design Flow Chart

In classifying redundancy approaches it is necessary to consider those features which comprise the redundancy doctrine, e.g., hardware configuration and failure recovery, and redundancy verification, e.g., failure detection and time at which the detection is performed. Accordingly, this development will draw directly from the information contained in Figure 2.1-1. Since this area of technology suffers from a terminology trauma, each of the major features which characterize redundancy will be described before proceeding.

Redundancy Doctrine

- Load Sharing
  Explained in the figure

- Back-up Capability
  Do redundant items have same functional capability as the prime or do they represent a reduced but acceptable capability (fall-back)?

- Level
  Is the redundancy at the part, assembly, unit, etc., level?

- Location of Tie Points
  Where should redundant sets be formed and how many items should be in a redundant set?

- Degree
  How many items are redundant?

- Outputs/Effects Distinguishable
  Are the outputs (and inputs in some instances) of redundant items distinguishable from each other or are they "tied" (physically) together?

- Repairability
  Are failed off-line equipments repaired immediately after failure, scheduled for repair, repaired only when all redundant items in a set have failed or not repaired at all?

- Recovery Policy
  Are failures only detected and then manually corrected or are failures automatically detected and corrected?

- Fault Correction
  If automatic failure detection and correction is used, are failures detected and corrected for each redundant set or only detected at system output and diagnostic routines isolate and correct failure?

- Type
  Are redundant elements active and functioning, idle and powered down or on standby partial power.

- Recovery Time
  How long may a redundant set be out of specification limits following the failure of one of its elements?

Redundancy Verification

- Verification Policy
  Are the elements in a redundant set checked continuously for proper operation or checked initially or periodically?

- Failure Detect Scheme
  What is the nature of the failure detection process? Is concern centered on identifying r of n redundant items are operable or with identifying which specific item is operable?

- Validation Policy
  If identifying the condition of specific elements, is only the on-line equipment validated or is off-line equipment also validated?

Having answered all of the above questions, a redundancy design will be uniquely identified. However, the immediate task is to classify redundancy with regard to verification techniques. With this added constraint it should be possible to decrease the large number of variables identified above. Before pursuing this task; however, it should be pointed out that eliminating some of the variables in a classifying scheme in no way implies that approaches classified according to this scheme are independent of these variables. Quite the contrary; the classifications serve to group approaches which possess common features such that statements may be made about the impact of the entire group on the remaining variables. Just as we group circuits into digital and analog, this does not imply that the circuits are independent of other variables such as power dissipation, reliability, accuracy, drift, etc. Once a circuit is identified as, say, digital in character, it is usually possible to attribute general features to that circuit regarding power dissipation, accuracy, etc. And so, the analogy holds for the redundancy classifications with regard to verification.

Let us at this point resume the task of decreasing the number of variables in our classification. Throughout the following discussion, the theme is one of eliminating features which do not directly describe how redundancy is verified from the standpoint of a redundancy design*. No mention has been made of the type of signal being used to judge the operation of

---

*It should be pointed out that while the eliminated features may not be of first order in describing a verification technique, they may impact the implementation of the technique to the extent of making it infeasible.

equipment. Signal types will radically influence verification techniques and this subject is discussed in Section 2.2. The immediate concern here is the classification with regard to redundancy.

On examining Figure 2.1-1, a little reflection will reveal that level, degree and load sharing do not immediately influence the verification technique. These features very directly influence the application of redundancy, the reliability of the redundant set and the relative ease, or difficulty, by which verification can be achieved. But knowing these features tells us little about the verification technique.

The feature of backup capability has some interesting ramifications. If the off-line equipment provides a reduced capability, it is tempting to state that the redundancy can be verified since it is usually a simple matter to determine which capability is present. However, there is usually no way to verify the reduced capability equipment when the prime equipment is operating--outside those described below. Thus, the manifestations of back-up capability can be described by other features and it will not be considered as a candidate.

To the extent that location of tie points is influenced by reliability, this feature falls in the same category as level and degree and does not influence the description of a verification technique. Location of tie points will affect, in general, the type signal to be considered and will influence verification in this regard. However, these considerations are not redundancy descriptors and so location of tie points can be deleted as a candidate.

Distinguishable outputs is the next feature of concern. Aside from a special case to be described in the next paragraph, if the output of each redundant equipment is not in some way distinguishable, it is not possible to verify redundancy. For by the very definition of redundancy (assuming the redundant equipments provide equal functional capability), the output of a set of redundant equipment must remain within a specified tolerance to prevent failure. For this reason, distinguishable outputs is identified as a feature which characterizes redundancy.

Closely related to distinguishable outputs and not shown on Figure 2.1-1 is a more subtle feature which deserves attention. This is the variation of an output from a redundant set of equipment as the number operational equipments varies. This feature would provide a method of redundancy verification when the outputs were not distinguishable, provided the variation was still within specified limits. It should also be pointed out that this feature will not identify which equipment is not operating, only the quantity that are operative. This feature is then identified for redundancy classification.

Repairability, Recovery Policy and Fault Correction all relate to the circumstances after a failure has been discovered. While these will influence verification they do not aid in the description of a verification technique, and will be deleted. It is interesting to note in passing that if redundant equipments are repaired only after all equipments have failed, there is little point in having continuous verification.

Examining Type of redundancy, again we see that this adds little to the description of a verification technique. This feature may, however, indicate that verification of redundancy cannot be achieved unless the elements of a set are completely operative.

Recovery Time can also be deleted. This feature may well influence the type of verification achievable but does not describe it.

Considering Verification Policy, it is obvious that this feature is descriptive of redundancy verification. Verification Policy introduces the dimension of time into the description. It will be convenient without too much loss of definition to describe this feature by two characteristics, viz., continuous verification and noncontinuous verification.

Failure Detect Scheme is the last feature to be included in the list, for Validation Policy is rather one sided. If we do not validate off-line equipment, we can not verify it. Failure Detect Scheme identifies the basic principle of verification. This feature will be described by two characteristics, viz., concern is only with whether all elements of a redundant set are operating--with no regard to identifying which element has failed--or a specific element is identified as having failed.

In summary, the redundancy classification have been reduced to the following features:

- Distinguishable Outputs
- Verification Policy
- Failure Detect Scheme
- Variation of output with the number of operating equipments.

In turn, each of these features has two characteristics. If we consider the redundancy classifications to consist of exhaustive combinations of characteristics we account for a total of 2^4 or 16 classifications. These classifications are shown in Figure 2.1-2. Examining these results, it should be possible to further reduce the number of classifications on the basis of inconsistencies. However, there is a more pronounced problem which pervades the entire discussion above. That is, we have all but ignored the influence of application. It is somewhat surprising that the derived features claimed to be descriptive of redundancy have little to do with what are typically recognized as descriptors of redundancy. It is even more enlightening to realize that redundancy verification cannot be typified on the basis of redundancy approaches alone. Of the questions asked at the outset of this section, we have answered but two--(a) the features used to describe a redundancy approach and b) a redundancy approach can be described independently of application. And these are only qualified answers since the derivation contained only the fundamental redundancy problem.

It is obvious that a more fundamental problem will have to be addressed if additional information is to be obtained, or indeed, if the above results are to be validated. This problem will be that of status identification and is the subject of the following section.

Class #	Distinguishable	Not Distinguishable	Distinguishable Outputs: An Equipment in a Set Has Failed	Distinguishable Outputs: A Specific Equipment Has Failed	Failure Detect Scheme: Continuous	Failure Detect Scheme: Not Continuous	Verification Policy: Output Varies	Verification Policy: Output Does Not Vary	Variation of Output w/# of Operating Equipments
1	X		X		X		X		
2	X		X		X			X	
3	X		X			X	X		
4	X		X			X		X	
5	X			X	X		X		
6	X			X	X			X	
7	X			X		X	X		
8	X			X		X		X	
9		X	X		X		X		
10		X	X		X			X	
11		X	X			X	X		
12		X	X			X		X	
13		X		X	X		X		
14		X		X	X			X	
15		X		X		X	X		
16		X		X		X		X	

Figure 2.1-2. Redundancy Classification, Exhaustive Enumeration

2.2 A General Look at Status Identification

It is appropriate to begin with a deceptively simple premise - one does not measure the status of a device; one measures physical properties of input and output signals/effects and deduces the status. It is this deductive process that is the key to status identification and the heretofore missing link in the classification attempts. The development in Section 2.1 treated the instances of redundancy as entities, divorced from the remainder of the system. Under these circumstances the required deduction for status identification is trivial.* If under a given application, the redundant sets can be treated as entities, the results of Section 2.1 would be a good representation of the situation.

Let us then address the problem of status identification. The process is depicted in Figure 2.2. Since this figure will be the guidepost for Section 4.0 of the repor it is not the intent at this time to discuss it in detail. Rather, the discussion will be carried to the extent necessary to determine redundancy verification classifications and to assess the results of Section 2.1.

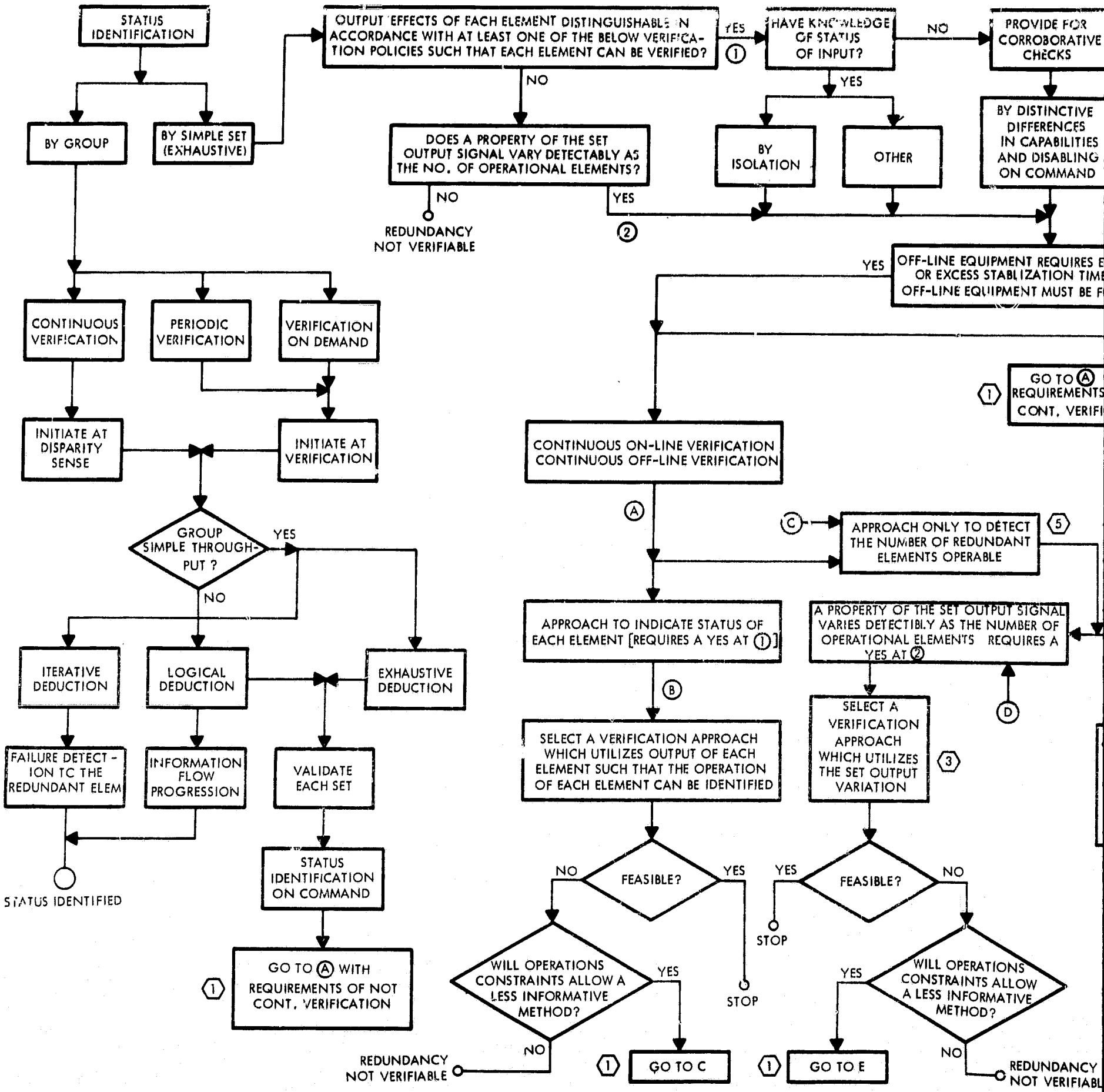
Referring to Figure 2.2, we note that status identification has been divided into two primary areas--identification by simple set and identification by group (see Glossary). Essentially, a simple set meets the assumptions of the development in Section 2.1 above and a group is anything that is not a simple set. One fundamental difference is that group identification is centered about system-related schemes whereas set identification schemes are centered about the set as an entity. The latter is exclusively redundancy verification where the former is not necessarily so. A detailed discussion of isolation by group will be deferred to Sections 3.0 and 4.0. Suffice it to say that the group problem is typically concerned with such schemes as pattern recognition, sequential testing algorithms, etc.

The first block in Figure 2.2 under "simple set" is a rather crucial one. The branch to the right indicates that the outputs are distinguishable by one of the methods identified in the three blocks immediately below and in accordance with at least one of the three verification policies, vis., continuous on-line and off-line, continuous on-line and periodic off-line or periodic on-line and off-line. Note that the lead-in premise is applied here since we must either know, or make provision to determine, the status of the input. The branch to the left of this block indicates the outputs/effects are not distinguishable and passes to a second test. This test is applied to determine if the output signal/effect varies as the number of operational elements in the set. If the output does not, redundancy cannot be verified. If it does, then a limited form of verification can be performed (see below).

We next pass into a test block which is concerned with the behavior of the off-line element(s). The concern here is whether the off-line elements must operate or not. If they must be operational, it would be desirable to verify their status on a continuous basis. It should be noted that the questions in this block do not directly influence the status identification but they are considered important enough to place on the diagram.

---

*Note that the deduction is trivial. This by no means implies that obtaining the information on which to base a deduction is trivial.



FOLDOUT FRAME 1

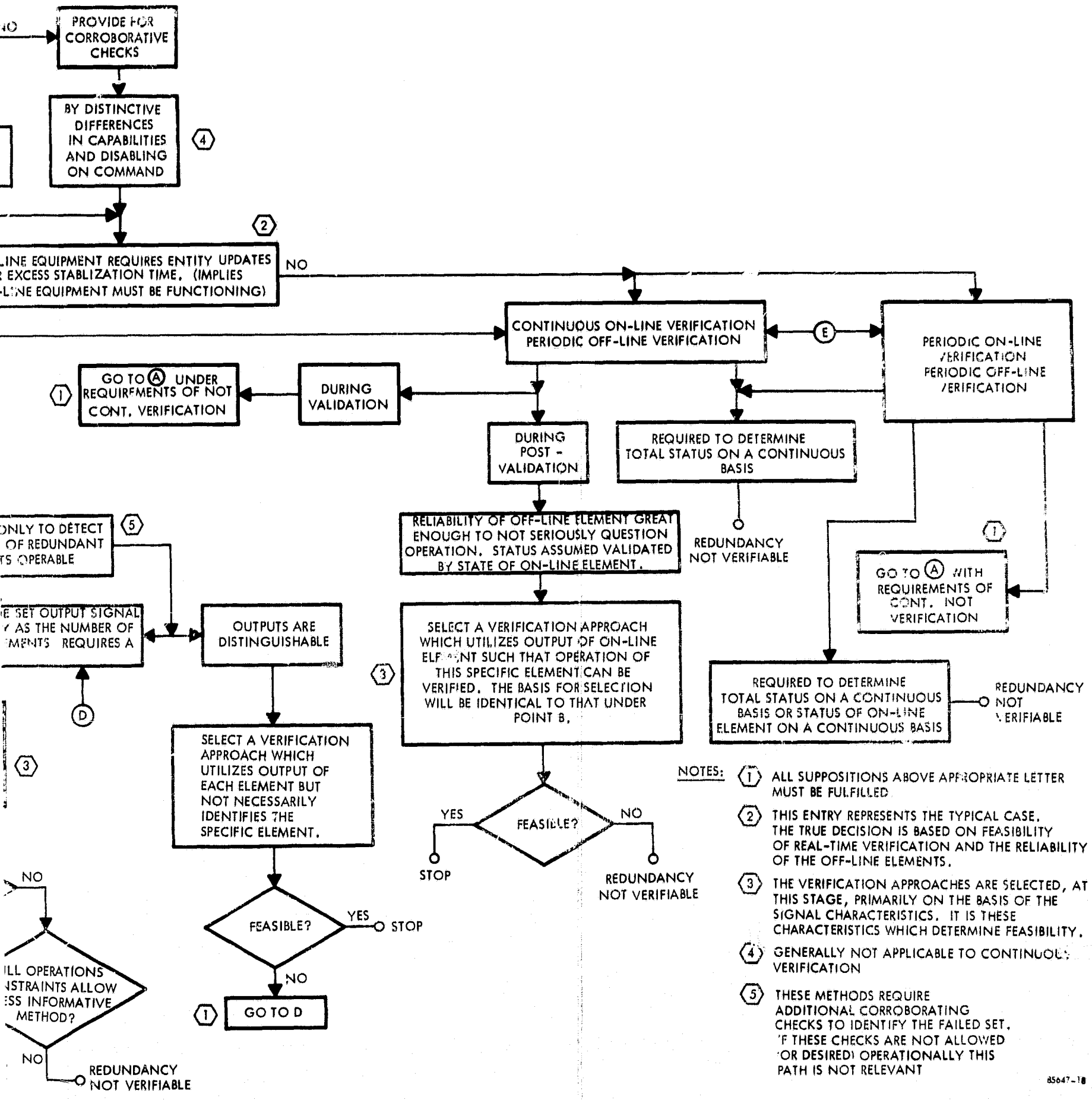


Figure 2.2. Status Identification Process Flow Chart

FOLDOUT FRAME 2

The next set of blocks represents the three verification policies as described above. While these blocks are felt to be self-explanatory, a few words regarding periodic verification are in order. By periodic verification we mean verification that is either performed only once in the life of the equipment, or at the beginning of each mission or at some time interval which is large compared to timing or frequency internal to the system. In general, periodic verification implies the requirement to terminate normal functions of the set while status indication is being performed.

Let us now consider the branch under point A. The right-hand branch considers the characteristic of not identifying which specific element in a set is faulty but only the quantity that are faulty. This is a subtle but rather important distinction--especially in the area of cost. Without pursuing the details (see Section 5.0), it should be intuitively evident that the task of simply identifying one of a group of items is not operational is easier than identifying which specific one. From the figure it can be seen that there are two characteristics of redundancy which will make this form of verification possible. One is a property of the redundant set output signal which varies with the number of operational elements in the set and the other is distinguishable outputs. We note that in the former characteristic, the outputs of the elements do not have to be distinguishable. Considering the latter characteristic of distinguishable outputs, all that is required to meet the operations demand is that the element outputs be compared.

If we are to indicate the status of each element in the set, the problem becomes somewhat more involved. (See left-most branch under point A in the figure). Recalling the premise cited at the outset of this section we must measure, on a continuous basis, a physical property of the output signal/effect to determine the status of each element. This points directly to the final missing ingredient in the classification scheme--the type of signal. This ingredient, however, introduces a whole new classification problem since the signals must be classified for the same reasons we desired to classify redundancy features. A moment's reflection will indicate the scope of this task - and confirm the desire for classification. Since the nature of measuring devices and schemes is highly correlated to the statistical character of the signals, it seems reasonable to classify signals by these methods. This classification, however, will have no immediate effect on the present development and details of the classification will be deferred to Section 5.0.

At this point some general comments about Figure 2.2 are necessary. There is a feasibility test after each verification selection block. An obvious inference to be drawn here is that a verification approach may be acceptable from the redundancy features and yet not feasible due to technology or the operations requirements. Table 2.2 lists some of the most pertinent reasons for an approach not being feasible. A second general point of interest in the figure is the decision block in the lower left-hand corner where the process is directed back to another verification policy--should this be allowed by the operational constraints. The point to be made is that the feasibility of verification is also influenced by operational considerations.

Table 2.2. Reasons for an Approach Not Being Feasible

- False alarm rate too high
- Distorts through-put information
  - loading
  - phase shift
  - frequency stability
  - bandwidth
  - error rate
  - accuracy
  - pressure
  - speed
  - inertia
- Will not detect all of the most probably failure modes
- Too heavy
- Spatial constraints exceeded
  - form factor
  - size
- Power dissipation too great
- Reliability too low
- Cost
- Response time too great
- Beyond the state-of-the-art
- Cannot implement an approach due to signal restrictions

2.3 Conclusions

There are several important conclusions to be drawn from the material in this section. These conclusions will be referred to repeatedly throughout the remainder of the report and are itemized below for easy reference.

- The investigation of the status identification problem corroborates the redundancy classification results of Section 2.1. As a result of the status identification investigation, it is possible to pare down the exhaustive enumeration of classes depicted in Figure 2.1-2 to the eight shown in Figure 2.3. These eight classes constitute the final catalog of redundancy features for simple sets.

- The automated status determination of a redundant set is primarily contingent on being able to distinguish outputs of the elements. From a practical point of view this implies that in most cases the outputs be gated or switched to achieve isolation. If maintenance is to be performed on a failed element while another element in the set is continuing the on-line function, the isolation of outputs is imperative. In addition, the gross sensitivity of hardware failure mode distributions to manufacturing processes makes isolation even more attractive.

- Whether a particular redundancy scheme is considered amenable to automated status verification is as much a function of operations considerations and input/output signals (and the method in which they carry information) as it is the redundancy design.

- The redundancy features identified in Section 2.1 are both necessary and sufficient to characterize a redundancy approach relative to verification.

- While redundancy features can be identified independent of signals, both facets must be considered to classify a redundancy verification approach.

- While emphasis has been placed on classifying signals, in actuality each failure mode of the signal properties which affect the carried information must be considered.

- It is advisable to separate status identification into the two major divisions of group and simple set. This separation provides a natural dividing line in the overall process.

CLASS	Distinguishable Outputs/Effects		Failure Detect Scheme		Verification Policy		Variation of Set Output With # of Oper. Elements	
	Outputs/ Effects of each element are distinguishable	Outputs/ Effects of each element are not distinguishable	Approach to detect the number of redundant elements operable	Approach to indicate status of each element	Verification performed on a continuous basis	Verification not performed on a continuous basis	Set output varies detectably with number of operational elements in the set	Set output does not vary detectably with number of operational elements in the set
A	X		X		X		X	
B	X		X		X			X
C	X		X			X	X	
D	X		X			X		X
E	X			X	X		DON'T CARE	
F	X			X		X	DON'T CARE	
G		X	X		X		X	
H	NOT VERIFIABLE UNDER REDUNDANCY FEATURES							

Figure 2.3. Classification of Redundancy Features for Simple Sets with Regard to Verification

3.0 WHY REDUNDANCY VERIFICATION

It is opportune at this point to ask why one should be concerned about redundancy verification. Why should there be concern over how much redundancy is present so long as the system is performing its function? There are several significant reasons for requiring this information, depending on the circumstances. Let us consider three of the most prominent situations under which information about redundancy is important. The first situation is the most universal since it involves redundancy in any design. Consider a system which is intended to perform a mission of a predetermined length. The system will have an inherent probability of completing this mission without loss of predefined functions. Should the system contain redundancy, this probability will undoubtedly be based on the assumption that the redundancy was present at the start of the mission. Is this a valid assumption when the system has had time logged prior to the mission? The answer obviously depends on the amount of time logged prior to the mission, the length of the mission, the reliability of the equipment in question and the criticality of the mission.* In any event it seems prudent to verify the existence of redundancy. It is important to note that this same situation exists for a newly purchased one-shot system such as an ICBM or a system which will perform many missions over its lifetime such as a fighter plane.

Consider next a system such as a spacecraft which has several distinct phases in its mission, each representing successively greater commitments in terms of risk and fuel consumption. Before commitment is made to the next phase, an appraisal is made of the likelihood of completing that phase in terms of the present condition of the system (and its crew). If the spacecraft contains redundancy (and the chances are slim that it doesn't), the condition or status of this redundancy will likely be determined before further commitment is attempted. Note that in contrast to the first situation which addressed redundancy verification at the start of the mission, this situation is concerned with verification during the mission. The two are fundamentally different in terms of an approach to verification. In the former instance, most of the verification equipment could be designed as extrasystem check hardware. In the latter situation much of the verification equipment must fly with the spacecraft (or be allocated telemetry channels for remote analysis and verification). It is also worth noting that this situation might also apply to a system that is capable of aborting its mission at any time (as contrasted to the discrete commitment levels described). If this decision were based on the amount of redundancy present to allow a "safety factor," the verification would likely be on a continuous basis.

*It should be noted that these comments assume only the system output or total performance is observable.

As a final situation, consider a system which has, for all practical purposes, an indefinite mission such as a communication relay link. It is likely that MTBF would be used as a measure of the reliability for such a system. Assume that a maintenance crew is on duty at all times and further recognize that the system contains redundancy and redundancy verification. Will redundancy verification, along with the possibility of maintenance, influence the MTBF of the system? The answer is, generally, a decided, yes.* Let us examine the impact of redundancy verification on the MTBF of a system where maintenance is performed under three typical policies. Consider first a redundant set (see Appendix A for definition) with no redundancy verification. Typically, the only time a failure will be indicated under this situation is when all equipments in the set (elements) have failed. Only at this time will maintenance be effected and the effort will be relatively large since all elements must be repaired. The equation for the MTBF of a redundant set with n identical elements and one of the n required for success is,

$$M_s = M_e \sum_{i=1}^{n} \frac{1}{i}, \qquad (3.0\text{-}1)$$

where

M_e = MTBF of an element

M_s = MTBF of the set.

A family of curves showing M_s as a function of M_e for n = 2, 3, 4, 5 is shown in Figure 3.0-1.** Note that for a set comprised of a redundant pair of elements (redundancy of degree one) and an element MTBF of 100 hours, the set MTBF is only 150 hours.

*There are several important assumptions which must accompany this answer. These are: (a) the failed equipment can be isolated from the on-line operation of the system, (b) the verification indicates which equipment has failed and (c) maintenance can be performed on a noninterfering basis with operations.

**It has been assumed that no element has zero failure rate.

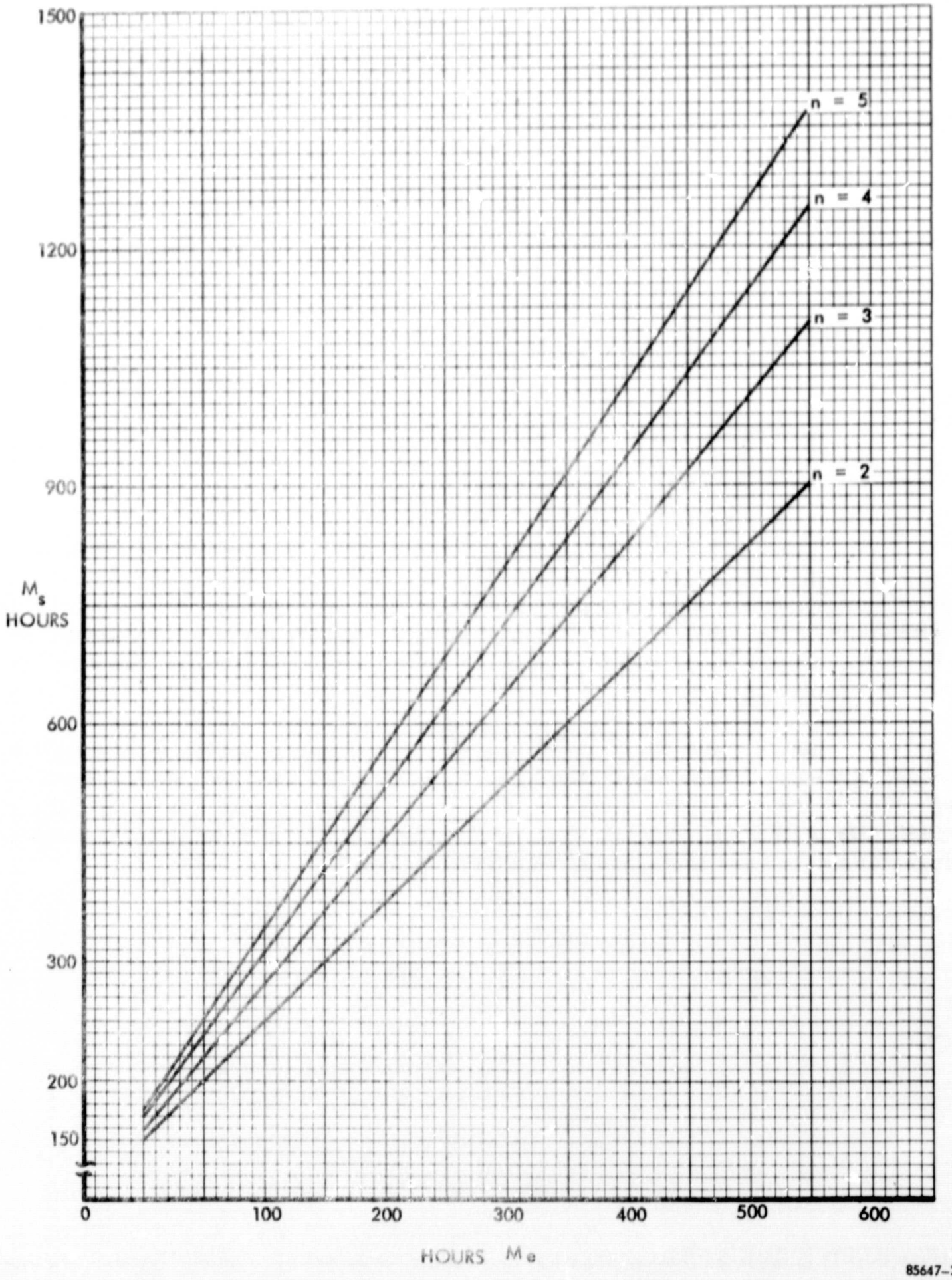


Figure 3.0-1. Plot Of Set MTBF (M_s) vs. Element MTBF (M_e) For The Number Of Elements (n) Ranging From Two To Five -- Unmaintained Redundancy

Consider next a redundant set with redundancy verification employed on a continuous basis and repair of a failed element is effected as soon as the verification equipment indicates this condition. The equation for the MTBF of a redundant set with n=2 identical elements and one of the two is required for success is,

$$M_s = \frac{M_e^{\,n}}{D^{n-1}\, n}; \quad D << M_e \quad ,$$

$$M_s = \frac{M_e^{\,2}}{2D} \quad ; \; n=2 \quad , \qquad (3.0\text{-}2)$$

where

M_e and M_s are defined for (3.0-1)

D = mean down time of an element due to unscheduled maintenance.

A family of curves for M_s as a function of M_e for D=1/2,1,2 is shown in Figure 3.0-2 (note the log scale on the ordinate). Under this condition, for a redundant pair with element MTBF of 100 hours and mean down time of one hour, the set MTBF is 5,000 hours. Compare this result with that obtained above.

Consider as a last situation, a system in which redundancy verification is performed periodically every T hours and if an element (or elements) is found failed, it is repaired.* The only other time maintenance is initiated is when all elements in a set fail (since without verification, this is the only recourse). The equation for the MTBF of a redundant set with n=2 identical elements and one of the two is required for success is,

*Note that it is assumed the verification and repair times are very much less than the verification interval T.

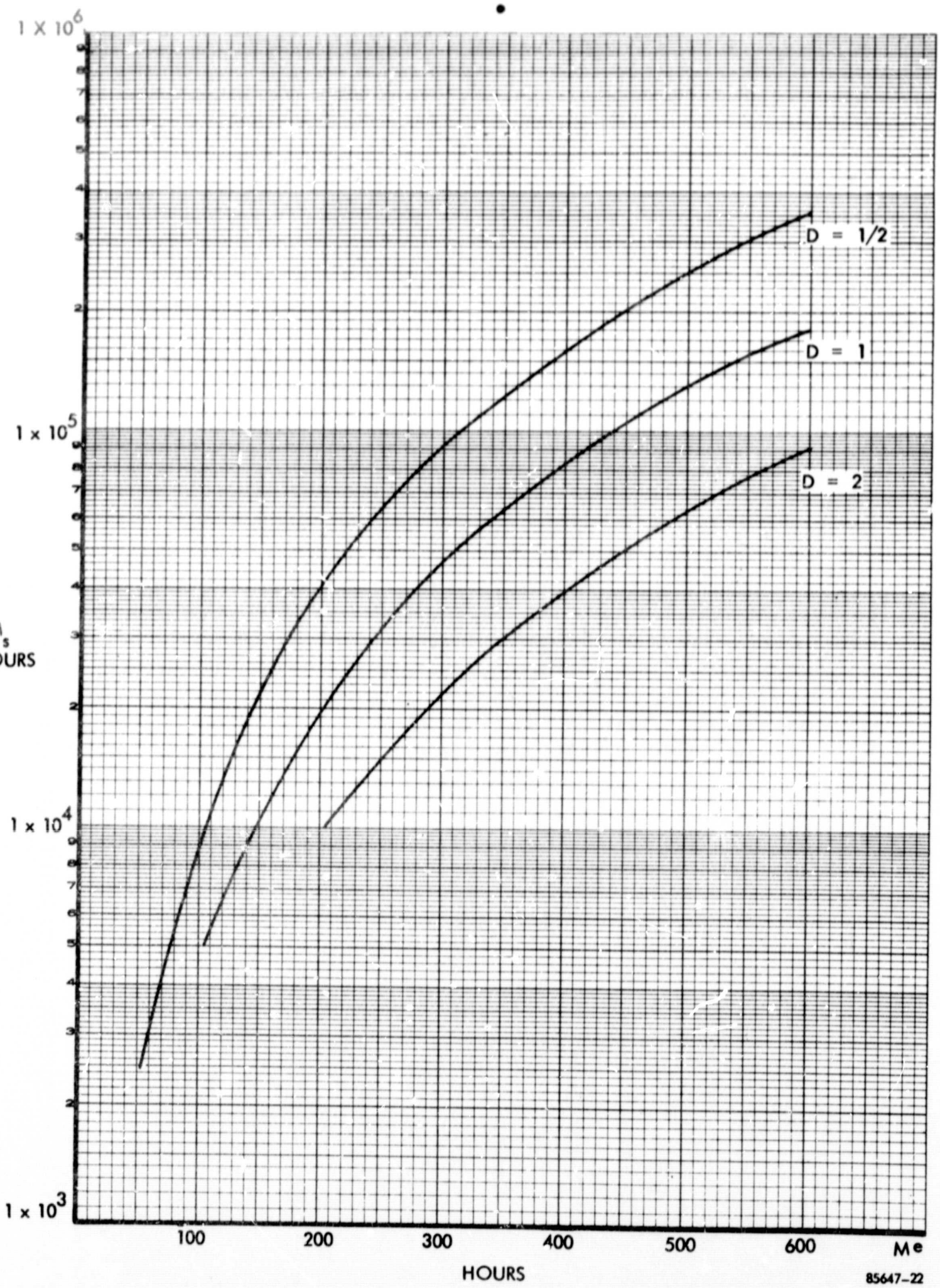


Figure 3.0-2. Plot Of Set MTBF (M_s) vs. Element MTBF (M_e) For Average Element Down Time (D) = 1/2, 1, 2 - Redundancy With Immediate Repair

$$M_s = \frac{\int_o^T R(t)\ dt}{1 - R(T)} \quad ,$$

$$M_s = \frac{\int_o^T \left[2e^{-t/M_e} - e^{-2t/M_e}\right] dt}{1 + e^{-2T/M_e} - 2e^{-T/M_e}} \quad ; \quad n=2 \quad . \quad (3.0\text{-}3)$$

A family of curves for M_s as a function of M_e for T=50, 100, 500 is shown in Figure 3.0-3 (note the log scale on the ordinate). Here the set MTBF is 208 hours for an element MTBF of 100 hours and T=100 hours (about every four days).

Recalling to the question asked at the outset of this section, it is recognized that no answer has been explicitly provided but ample argument has been advanced to indicate the importance of redundancy verification. Where redundancy is involved in a design, the verification of that redundancy is a natural consequence. The remaining sections of this report describe what must be considered in the design for redundancy verification under various cases and circumstances. The reader will likely identify, in that material, some of the situations described in this section and may find it helpful to use the situations in cementing ideas.

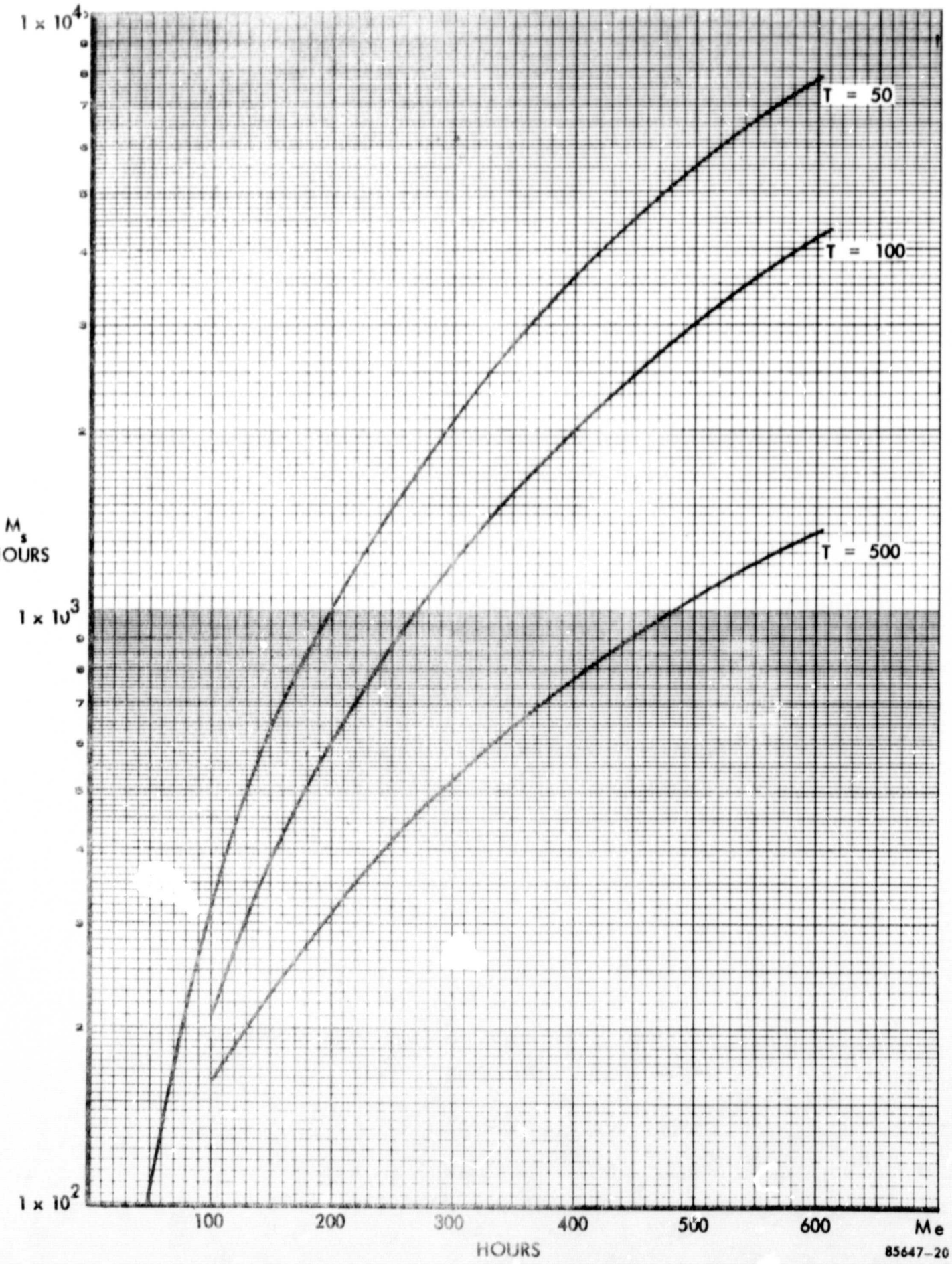


Figure 3.0-3. Plot Of Set MTBF (M_s) vs. Element MTBF (M_e) For Three Durations Between Verification (T) - Redundancy With Deferred Maintenance

4.0 SOME GENERAL CONCEPTS

This section is intended to introduce some of the most important and basic notions developed during the study. These notions will serve as the foundation for the detailed developments of succeeding sections. The scheme of the section is more one of appealing to the intuition of the reader than a formal presentation of definitions and methodology.

The study has attempted, among other things, to lend a degree of formalism and unification to the area of redundancy verification which heretofore has been virtually nonexistent. This approach has the singular advantage of allowing a monolithic treatment of the subject but the disadvantage of requiring a vocabulary of its own to express the ideas. Accordingly, it has been necessary to identify numerous terms and classifications during the study. The classifications are a means to an end and not the end themselves. As such, they are a convenient means of expressing notions and descriptions, and not just slots for sorting. If one is told to design an amplifier, one has some idea of the task ahead. But if he is told it is to be a small signal amplifier, his information is greatly increased. The specialized terms are used to describe the nature of the redundancy verification problem and the methodology or technique for designing redundancy verification is developed about these terms. When a specific problem is stated in these terms, the methodology for its solution is outlined and the information required to achieve this solution has already been spelled out. With these thoughts in mind, let us look at a few of the concepts.

4.1 The Implications of Redundancy Verification

The problem of redundancy verification on an automated basis is essentially one of determining whether the equipments forming the redundant operation (called a set) are operating in an acceptable or unacceptable manner.* The acceptability of operation of an equipment will be called status and we may conclude that the problem is one of determining status.

It is appropriate at this point to recall a premise from Section 2.2, viz, one does not measure the status of a device; one measures physical properties of input and output signals and deduces the status. We have thus introduced two more steps in the verification process, i.e., deduction and measurement. These steps will be discussed further in the following paragraphs but let us first direct our attention to two more obvious considerations--the influence of the redundancy design itself and the signals which are being measured. Classifications of redundancy as they described methods of achieving redundancy verification were developed in Section 2.0. (See Figure 2.3.) These classes essentially determine whether redundancy verification is feasible based on the redundancy design itself. If feasible, the classes establish one of the primary considerations for verification. These considerations impose the implications of where, when and what on the verification design. What remains is the how and this is determined to a large degree by the statistical character of the signal being considered and the

*Here we have considered only two levels of acceptability for simplicity. In the general case there could be several levels. Note, however, that in the final analysis we must state whether an equipment is redundant or not and this is two levels of acceptability.

desired confidence in the results. Redundancy verification is then a process of deducing status from operations performed on the system signals and, by some means, reporting this status.

4.2 Functional Descriptions of Signals

In the preceding paragraph we indicated that operations would be performed on the system signals. However, it is important to be able to describe these signals in more detail. We shall call the signals which exist in the system being verified, before any verification has been introduced, tenant signals. (Where the system being verified is known as the principal system.) It is also possible that signals other than the tenant signals may have to be introduced into the principal system to realize redundancy verification. These signals we shall call injected signals. We may further classify injected signals into three more specific types depending upon their relationship to the tenant signal. These are Symbiotic, Simulative and Idle and refer, respectively, to whether the injected signal is in some fashion "mixed" with tenant signal, replaces an otherwise active tenant signal or is injected into the tenant signal stream when the tenant signal is inert for long periods of time.* We note finally that there will also be signals in the verification equipment as well. These signals we shall call supporting signals. Figure 4.2 indicates the relationships of these signals.

4.3 The Notions of Groups and Sets

If we are to examine methods of redundancy verification, we must also consider the configurations which redundancy designs may take on. There are obviously an infinite number of such configurations and a moments reflection will reveal that these configurations will certainly influence redundancy verification. To further complicate the problem, it is seldom that one is interested in verifying a single instance of redundancy: we are typically interested in verifying whole systems containing numerous instances of redundancy. Some collective descriptors must then be defined if intelligent statements are to be made about the effects of redundancy configurations on redundancy verification.

Let us begin by establishing what we shall call a redundant set. This descriptor includes single instances of redundancy wherein the members of the set (called elements of the set) are dedicated solely to the function to be performed by the set and this single instance of redundancy is independent of all other instances of redundancy. A redundant set can be further divided into simple sets and, logically enough, sets that are not simple. A simple set is then a redundant set whose elements all have the same predecessors and followers in a functional flow sense.** If a redundant set does not meet these criteria it is not a simple set. Simple sets represent the classic example of parallel redundancy and an example is shown in Figure 4.3-1(a).

---

*An example of a system which might employ an idle signal is a Range Safety Command Distruct System. Such a system is idle (hopefully) over a vast portion of its missions.

**The term "functional flow" is crucial to the definition and should be interpreted in its most literal sense.

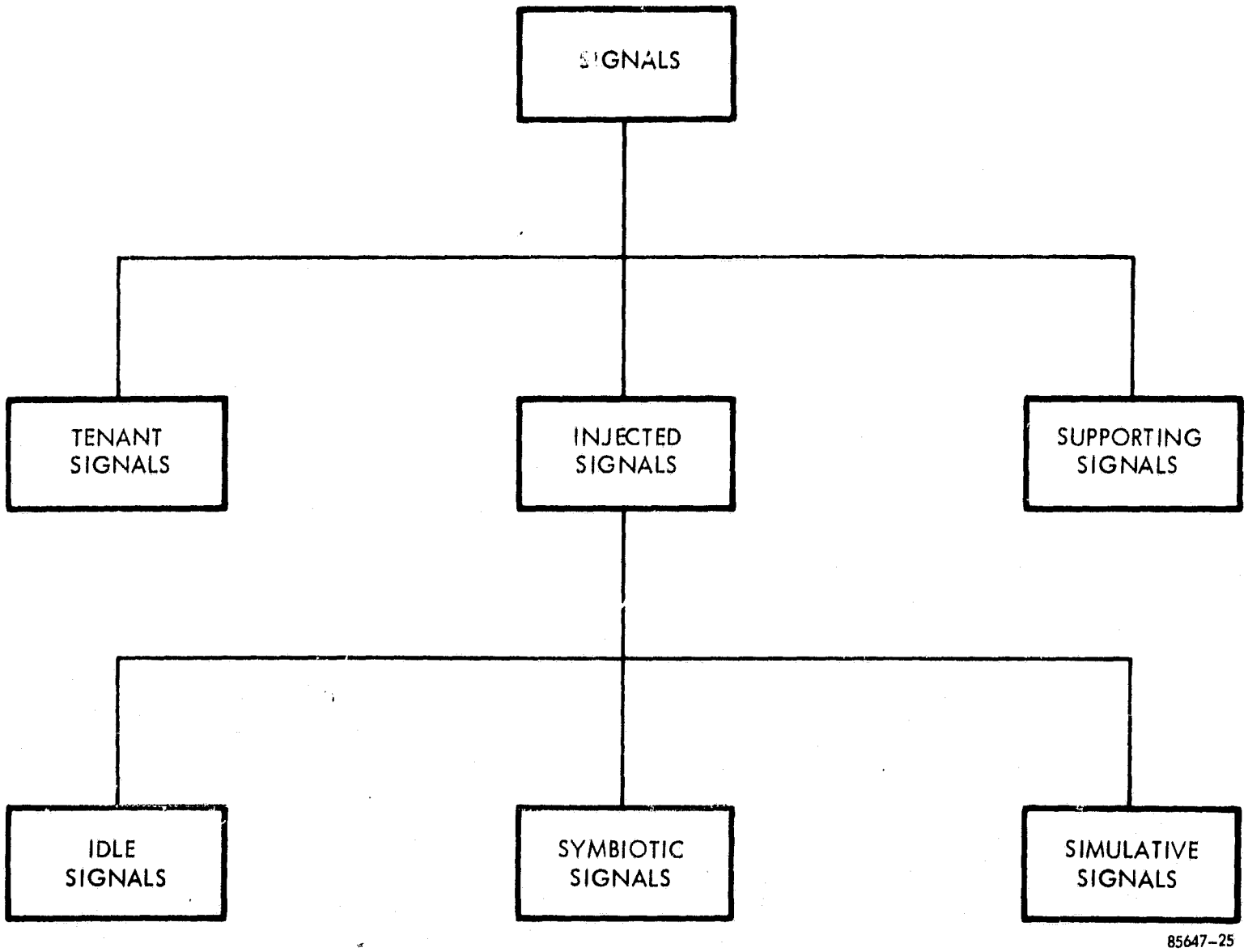


Figure 4.2. Signal Relationships

Retracing our steps, redundancy is divided into two configuration descriptors--redundant sets, described above, and interrelated redundancy. Essentially, all redundancy configurations which are not redundant sets are interrelated redundancy. An example of interrelated redundancy is shown in Figure 4.3-1(b).

Having defined the collective descriptors of redundancy configurations, it will now be necessary to indicate their relationships to redundancy verification. In this regard we shall divide redundancy verification into two distinct problems - the simple set problem and the group problem. The simple set problem involves redundancy configurations of exclusively simple sets. The group problem involves redundancy configurations of sets that are not simple and interrelated redundancy. These relationships are shown in Figure 4.3-2. From the development above we note that a group may simply be a collection of interrelated elements* which cannot be subdivided into simple sets. We shall term this a first level group. It is not inconsistent with the definitions to also think of higher level groups and this notion proves quite convenient. A higher level group can consist of more than one simple set or even other groups. The reason for this approach will become clear in Section 5.3. Throughout this report, when we speak of "the group problem" we shall mean all levels of groups unless otherwise indicated.

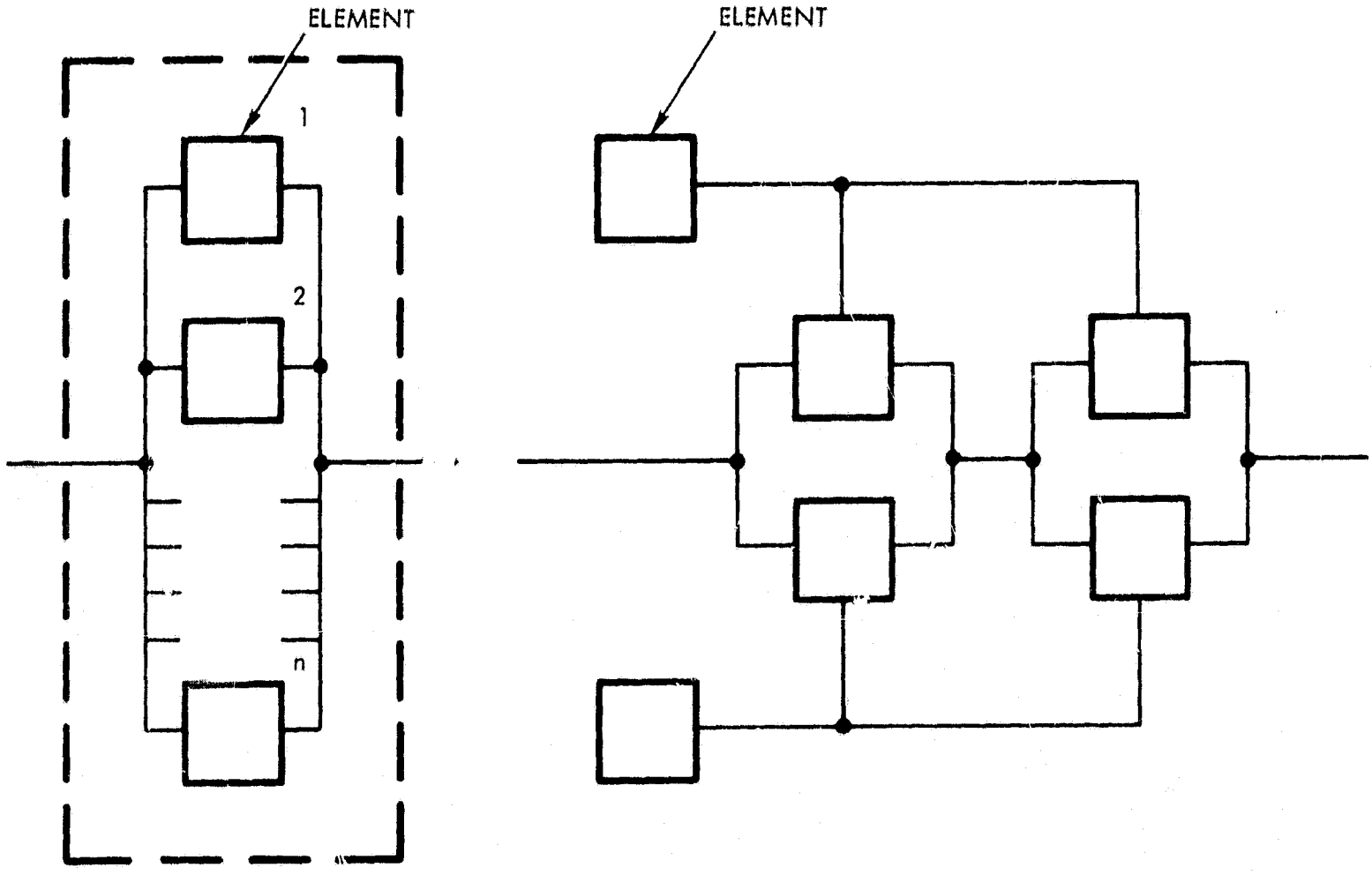
There is a final point which should be made before leaving this section. It is important to recognize that the redundancy classes defined in Figure 2.3 are classes of simple sets only. No equivalent classification could be devised for the group. It is reasonable to infer from this that groups are rather individualistic and each group problem will usually have to be solved on its own merits. Verifying redundancy in a group will inevitably involve some form of deduction and groups have been described by the deductive processes to which their verification is amenable. These descriptors will be discussed in Section 5.2.3.

4.4 The Implications of Time

The question of when redundancy verification is performed was briefly mentioned in Sections 4.1 and 2.2. This section is intended to highlight that question. Verification can be performed continuously or at discrete intervals in time. The four most important aspects influencing this decision are the importance of the duration of a failed condition, the criticality of a failure, the accessibility of the principal system for verification and the maintenance policy.** If a failure is critical, if unidentified false information is important or if repair is to be effected immediately upon a failure (see Section 3.0), then continuous verification would likely be required. However, if the principal system is not accessible for continuous verification or if, during the design of the verification technique, continuous verification is identified as not feasible, we will have to settle for noncontinuous verification. Under these circumstances,

*We shall term the lowest level at which automated verification is established as an element.

**The distinction between importance of the duration of a failure and the criticality of failure is a subtle one. In the former case one may not be concerned so much with the fact that a failure has occurred as with the fact that he is receiving false information and doesn't know it. This is contrasted with the critical failure where the loss of function is the primary concern.



(A) SIMPLE SET

(B) INTERRELATED REDUNDANCY

S5647-26

Figure 4.3-1. Examples of Two Redundancy Configurations

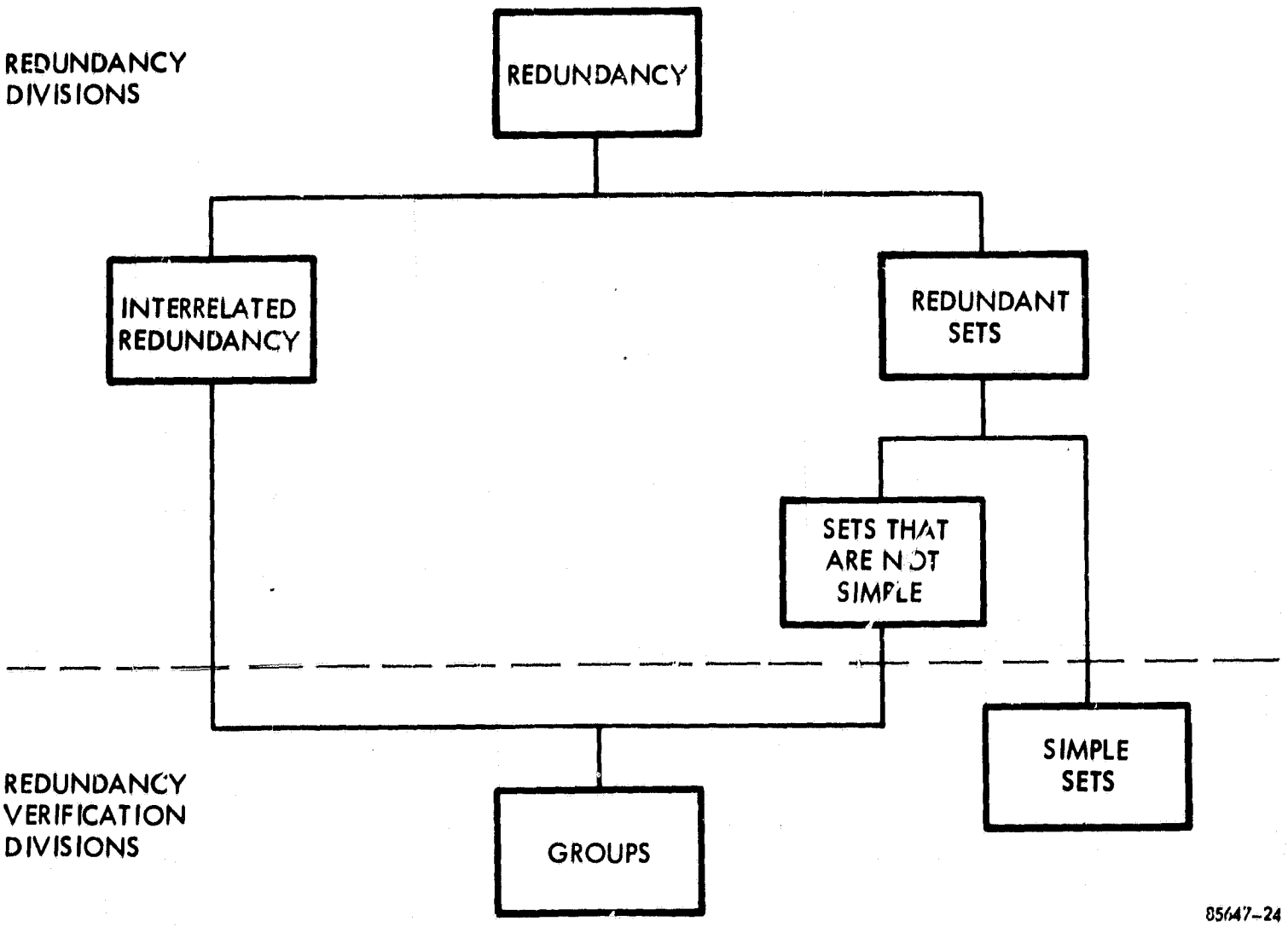


Figure 4.3-2. The Relationship of Redundancy Verification to Redundancy

the risk (in terms of criticality, reliability, false information, etc.) of not performing the function as desired increases. The relative change in risk will be a function of rhe interval between verification and this is the subject of Sections 5.1.1 and 5.3.1.

A second aspect of verification when considered in the light of time is the prospect of sampling. A discussion of sampling theory is beyond the scope of this report, however, it is easy to see that sampling is a microscopic view of the noncontinuous verification discussed above and subject to the same statements regarding risk. There are several reasons why sampling is desirable (aside from the fact that, in some instances, it is the only recourse) but the most prominent is the freedom to time share equipments. This is the subject of Section 5.3.2.

4.5 The Relationship of Verification to On-Line and Off-Line Elements

Let us begin this discussion by indicating what we mean by on-line and off-line. While this description applies to groups as well as simple sets, it is easier to describe in terms of a simple set and we shall take this approach. Consider a simple set with distinguishable outputs or more specifically, outputs which are isolated. Let us also state that only one of the elements of the set is in the information stream of the principal system at any time, i.e., throughputting the tenant signal to successive functions. The remaining elements have their outputs dead ended. The one element which throughputs to successive functions is called the on-line element and the remaining elements, off-line elements.

Thusfar in the report we have described sets and verification techniques in what may seem to be a one-to-one correspondence. This is not necessarily true. Under the situation described above, it is entirely possible that one verification technique could be used for the on-line element and a different technique for the off-line elements. Let us examine this possibility further; in particular with regard to the implications of time.

When we say continuous verification we are in actuality describing the time relationship of continuous redundancy verification. Determining the status of an on-line element on a continuous basis and the off-line elements at discrete intervals of time is not, with the exception of the case discussed below, continuous redundancy verification.*

Continuous redundancy verification implies continuous status identification of both on-line and off-line elements. One exception to this is a case where the reliability of the off-line element is great enough that we are willing to assume it will not fail over the period of interest. This being the case, continuous status identification of the on-line element and noncontinuous status identification of the off-line element would be considered continuous redundancy verification. In other words, knowing the status of the on-line element and knowing that, at some time in the past, the off-line element was operative is sufficient for continuous redundancy verification. This is equivalent to stating that during the interval when the off-line element is not being verified, the verification of the on-line element is also verification of redundancy.

*When considering continuous and noncontinuous verification of on-line and off-line elements there are four possible cases. Only the case where both on-line and off-line elements are verified continuously describes, in general, continuous redundancy verification.

A good example of this situation is the power steering in an automobile. The writer knows of no one who has disabled the hydraulics on his steering to verify the operation of the mechanical backup. Yet we all seem willing to believe that as long as the power steering is working, the mechanical backup will work when called upon, i.e., redundancy is present. The degree of our belief will once again depend on the risk we are willing to accept in the indication of redundancy verification.

4.6 Some Additional Points About Status of Redundant Sets

In Section 4.1 we indicated the relationship of status to the redundancy verification problem. Let us now consider some of the more important points about status determination. Throughout the preceding sections we have indicated the existence of risk as related to redundancy verification and status verification in particular. For reasons which will become clear in Section 5.0, it can be stated that we can seldom know with certainty the status of an element.* In providing status identification, we are attempting to draw an inference about operational integrity. The variable which is a measure of this operational integrity we shall call the status variable and its development is one of the most important functions of a verification technique. The status variable will contain statistical errors due to uncertainties inherent to the processes which develop it. This variable must then be quantized into discrete levels which indicate predetermined, qualitative statements regarding operational integrity. These discrete, and usually broad, qualitative statements are the conditional status of the element under consideration. (The reason for the term "conditional" status will be made clear in the following paragraph.) The transformation from the status variable to conditional status is a decision process and will introduce further statistical error. The process is depicted in Figure 4.6.

Let us address briefly, the reason for using the term "conditional" to describe status in the above discussion. To do this we must recall from Section 4.1 the method by which we are achieving verification. Namely, we are measuring properties of input and output signals (of an element) and deducing status of that element. When treating a redundant set as an entity, we know no more than the properties of input, output and possibly what the output should be. Can we directly infer status of an element with this information? Usually not. We must also know the status (or as a minimum the admissability) of the input. For if the input is in error, there is no guarantee the element will perform as it should and it would be a remote possibility that the output was correct. We can not, then, decide if an element is "bad" unless we know the status of the input is "good", i.e., the status variable is a measure of operational integrity,

*This statement deserves some commentary. Whether something can be determined with certainty or not, many times depends on the required accuracy of the answer. If it were required to measure the length of this page to the nearest 1/8 inch, one would likely get the same measurement each time he measured it. On the other hand, if it is required to measure the page to the nearest ten thousandths inch, one would get a distribution of results depending on paralax, temperature, humidity, etc. The former case can be considered deterministic whereas the latter case is a probabilistic result and we would be forced to describe the expected length of the page.

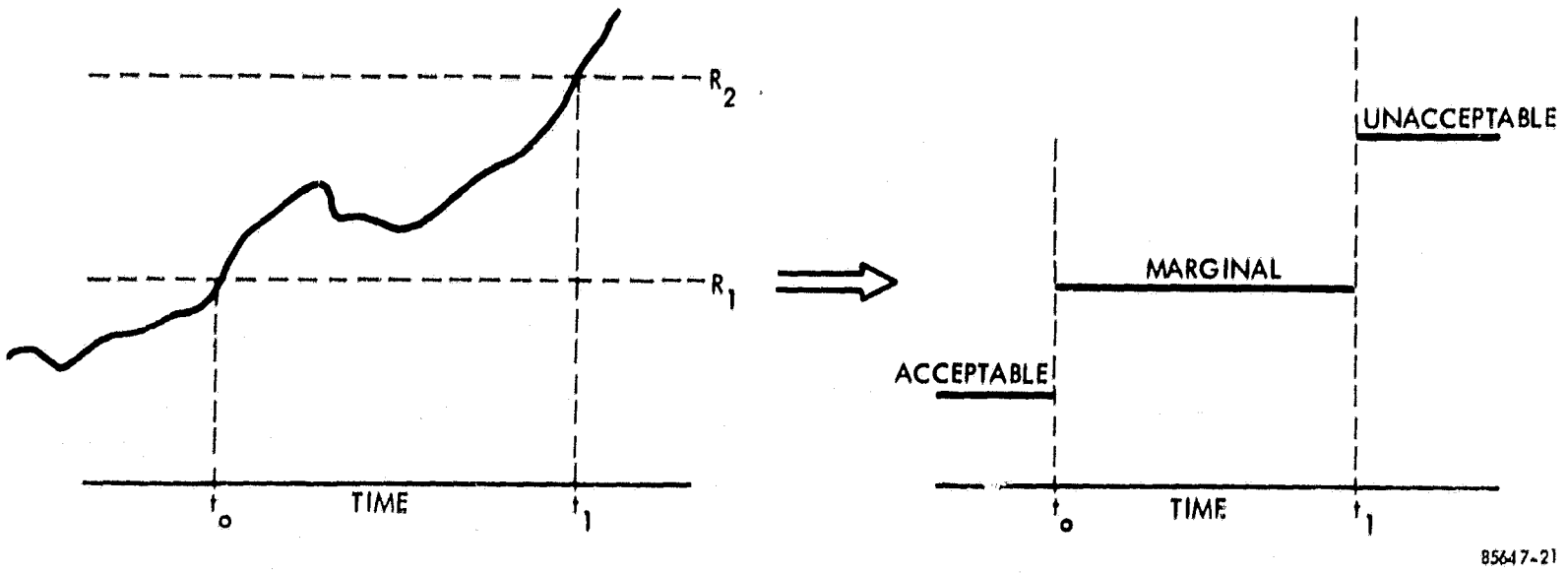


Figure 4.6. The Relationship of the Status Variable and Conditional Status

given the input is good. Thus, the name conditional status. Conditional status can not be related to unconditional status (the inferred status of the element) until we know the status of the input. This seems trivial enough until we consider a failure in the middle element of a series information chain. Typically, the conditional status of all elements to the right of the failed element will also indicate unacceptable. If we had only these indications to go by, how would we determine which element had really failed? To accomplish this on an automated basis would require a device that knew the information stream and could deduce that, with high probability, the first element in the string of "bad" elements is the culprit. It would then declare the unconditional status accordingly. We shall call this function status resolution and from the description of the function, it would typically be performed by a digital processor.* There is an exception to this general rule, however if the risk appears warranted. Some techniques of status identification may yield a conditional status that can, with a high probability, be identified as unconditional status. If these techniques are used exclusively, the status resolution function could be eliminated. These techniques are discussed in Section 5.2.2.2.

It must be recognized that there is an underlying assumption in the above discussion and that is the independence of element status. We have admitted that a failed element could cause a conditional status indication of "bad" to ripple down succeeding elements in the on-line chain. But we have also implied that, so long as the conditional status of an element is "good," that element output cannot, with high probability, degrade to a state which will cause the succeeding element to degrade its performance to an unacceptable state. Stated another way, if the conditional status of an element indicates acceptable operation and the conditional status of the immediately succeeding element indicates unacceptable operation, the fault must be in the second element. The problem usually comes about when the tolerances of two communicating elements drift in opposite directions. We see that status of an element is not only an operational consideration vested in the mind of the user, but that it is also based on the input requirements of the immediately succeeding element.

The problem of preserving status independence becomes quite crucial if more than two levels of status are required. One way around this problem is to display multilevel status and ask the automated system to act on two levels which are defined by partitioning the multilevels.

There is a natural tendency to compensate for the risk of violating status independence by enlarging the range of the status variable in the region of unacceptable operation. This is equivalent to lowering boundary R_2 in Figure 4.6 and will indeed decrease the likelihood of violating independence. However, this approach will usually increase the probability of identifying an element as unacceptable when it is, in actuality, acceptable (a Type I error).

*It should be noted that the entire concept of status resolution is based on the assumption of single failure occurrences, i.e., only one element will become unacceptable during the short term period of examination. If this assumption is violated, ambiguities will likely result.

Let us complete this section by returning our attention to the redundancy classes of Figure 2.3. We note that there are two failure detect schemes, viz, indicate status of each element in a set or indicate the number of elements operative in a set. The latter scheme amounts to a status of a set and will be identified as such throughout the remainder of this report. It is recognized that the status of a set will not identify which element is at fault and at some time this identification must be made before repair can be effected. The determining factor here is what we expect the automated system to accomplish. The distinction is effectively one of status resolution. There are several valid reasons why we may not require status identification to a specific element on an automated basis. Four of the most pertinent are:

- The packaging may not warrant the additional detail. It may be that the entire set is packaged as a single line replaceable item.
- The cost of identifying the status of each element may be prohibitive.
- The outputs of each element may not be distinguishable. This would make the status identification of each element impossible.
- Any automated scheme for identifying the status of each element may prove to be more unreliable than the element itself.

5.0 DESIGNING REDUNDANCY VERIFICATION - A DESIGN PROCESS AND CONSIDERATIONS

The purpose of this section is twofold. First, it is intended to extend and amplify the basic concepts of Section 4.0. Second, it is intended to relate the amplified concepts in the framework of a design process in the belief that they will strike closer to home and at the same time provide a method of attacking the design problem.

The section has been organized into the major areas of interest in designing an automated redundancy verification system. Section 5.1 identifies the input quantities to the design and the processes for developing these inputs from other forms of information. Section 5.2 relates the process of achieving a verification design using the inputs from Section 5.1. Section 5.3 discusses some of the more subtle considerations of the design and Section 5.4 describes the role of a central processor in verification design. Finally, Section 5.5 is a summary of the entire process.

5.1 Design Inputs

As indicated above, we will begin the description of the design process by discussing the necessary inputs. Before we begin a discussion of design inputs; however, it should be helpful to at least get a snapshot of the problem to be solved. The actual process during a total system design (design of the principal system to include automated redundancy verification) will be one of continuous evolution between capability design, redundancy design and the verification design, with feedback and correction until a final design is converged upon. If the design of redundancy verification is to be explained in any reasonable manner, we must break the loop and identify a beginning. We shall assume that the capability design (signal flow, signal characteristics, element characteristics, etc.) and the redundancy design are fixed as inputs to the verification design.

With the assumed starting point, the task of a redundancy verification design is to operate on the existing capability and redundancy designs, under the constraints of operations requirements and specifications, to produce an automated indication of the condition of redundancy in the principal system. To operate on the capability and redundancy designs, the verification design must have several identifiable inputs: (a) an expression, either quantitative or qualitative, of the desired confidence in the final indication of redundancy, (b) a partitioned principal system indicating all elements, simple sets, first level groups and higher level groups, (c) signal descriptions (both statistical and waveform) at the output of each element in the principal system, (d) the redundancy class for each simple set, (e) the levels of status desired, (f) properties of the output signals which are indicative of element operation and their relationship to status, (g) operational description of each element, (h) operating time profiles of each element and their relationships to the overall operations profile of the principal system, and finally (i) a general philosophy of approach to the highest levels of groups.* These items will

*It should be pointed out that the final design will seldom make use of all this information, however; a large percentage will be necessary to perform tradeoffs.

be treated in more detail in the following paragraphs. While the reader will recognize the value of some of these inputs, some may seem unnecessary without further explanation. Their purpose will become clear in Section 5.2. It is appropriate to point out at this juncture that the purpose of the verification design is fault detection not fault anticipation; i.e., diagnosis, not prognosis.

5.1.1 Design Confidence

Throughout Section 4.0 the implications of risk appeared as a recurring theme. This is not coincidental. Probably the most far-reaching and difficult task of a redundancy verification design is that of establishing a desired confidence in the resulting status indication. It is one thing to say that the results should always accurately represent the true picture and quite another to achieve this end. It is all but a foregone conclusion that a confidence of 100 percent cannot be realized. If signals are measured, errors are introduced. If they are compared in some manner, we must ascertain what degree of similarity is desired. If threshold techniques are used, we are making a decision subject to error. The design must settle for something less than 100 percent confidence. It is interesting to note that, if no verification existed, no errors could be made regarding status (we would simply remain ignorant). We are in effect trading off information about status (decreasing our uncertainty of this subject) with the fact that some of this information may be incorrect and falsely influence operations decisions. We must ask the worth of this tradeoff. How much is it worth not to blindly assume redundancy is present and find out ultimately, perhaps catastrophically, that it actually was not present? Is it worth the delay and cost of indication that redundancy was not present when indeed it was?* The verification design must have some notion of the desired confidence for this factor enters into virtually every tradeoff.

There are many considerations influencing confidence and we shall address the most important. The first consideration is that of tolerance "snowballing" in measuring equipment. Principal system reference signals, in particular timing signals, typically have very small tolerance limits. One method of determining the accuracy, and thus the functional integrity of the generator, is to compare the tenant signal with a "standard" generator as part of the verification equipment. For this approach we can say, as a rule of thumb, that the standard will require at least one more place of accuracy. Such a piece of equipment would typically be less reliable than that of the principal system and this fact has little appeal. One way around this problem is to use differential comparisons in time rather than absolute comparisons as the one above. These techniques would depend only on very short term stability.

A second consideration is that of decision error. The verification equipment is essentially making decisions regarding the operational integrity of the principal system for each element in the system. What is the effect of this on the total confidence in design? Let us look at an example. If one is to make five independent decisions and his probability of a correct decision is 0.6 for each decision ($p = 0.4$ of incorrect decision for a single decision),

*Note that here we are trading off Type I errors (See Glossary) only. Under the circumstances, this is justified, however, if one is comparing two different verification designs, both Type I and Type II errors must be evaluated.

the probability of at least one of the five decisions being incorrect is $1-(0.6)^5 = 0.92$. The results are quite revealing and a conclusion to be drawn is simply minimize the number of decisions. We are making decisions at numerous points and each point consists of a time sequence of decisions. The first place to reduce decisions is to reduce the number of decision points. This typically implies that elements should be made as large as possible. Instead of making five decisions on five separate entities, lump the five decisions into a single element. This approach will also improve the results from a tolerance viewpoint. It may be that the drift on two entities is marginal but in opposite directions. If a decision is made on each entity, one (or both) could be identified as unsatisfactory. However, if a decision is made on the output of all five, the drifts may well cancel and the ultimate output is satisfactory. And isn't this all we are asking for? Making decisions on too small a level will tend to make the verification quite sensitive (if not hypersensitive).

Let us return to our conclusion of minimizing decisions and look now at the time sequence of decisions. As a device makes more and more decisions, the likelihood of a wrong decision out of all decisions made becomes greater. One way of keeping this problem in bounds is to establish a rule that the device must identify, say, five unacceptable decisions in a row before the element status is declared unacceptable. Using the probabilities in the above example; if the element is actually good the probability of five wrong decisions in a row is $(0.4)^5$ which is 0.010.

A final consideration is that of multilevels of confidence. Acceptable operation can take on a range of connotations from requiring compliance to complete specifications to requiring only the presence of a signal. We will typically be concerned with a region somewhere between these extremes, but it is quite possible to require, say, two levels of confidence for a system. One level would critically verify the integrity of operation, approaching compliance to specifications. The other level would verify operation to a "reasonable" confidence. The former would likely be performed on a noncontinuous basis, requiring the principal system to interrupt its intended function while verification is performed. The latter could be performed real time on a continuous basis while the principal system is performing its intended function. The former approach would represent a higher confidence but would likely require injected signals and predefined checkout sequences typical of most Automatic Checkout Equipment (ACE) today. The latter approach would represent a lower confidence but has obvious advantages. When considering the remainder of the material in this section, it should be recalled that it may well have to be applied to more than one confidence level. Different techniques would likely result from considering the two verification approaches above.

5.1.2 Properties Indicative of Operation and Their Status Relationships

There are two basic approaches to determining properties indicative of operation. These are:

- The problematic approach whereby each function and each failure mode of an element is examined and ultimately related to the failure detection requirements. Here an equipment is judged on the basis of performance of many internal factors - we could look at every state variable.

- The symptomatic approach whereby the output of an element is considered to be its sole function and judgments about the operation of the equipment are made based on characteristics of the output. Here we are not concerned about the intricacies of the element, but only the quality of its output.

There have been many systems designed using the problematic approach and the design process is quite involved; usually requiring investigations into areas which are of second or third order importance. We shall subscribe to the symptomatic approach. For, using this approach we are concerned with the output of the element and consider internal properties only when circumstances warrant* (see below).

There are four ways of addressing the output of an element, viz, output signals and their absolute properties, output signals as they relate to the element input, signals (both input and output) as they relate to the element operation and output signals as they relate to output signals from other like elements in a set. In any of the cases, specific properties must be identified which are indicative of operation and ranges must be defined on each property which correspond to the desired levels of status. (As indicated in Section 5.2.2.3, it is also possible that functions may be defined for these properties and a similar range definition applied). Let us look at each of the ways of addressing the problem.

The first method of addressing the output is to define the output signals and their absolute properties. With this method, we are effectively saying that as long as an element is producing signals whose selected properties meet pre-established bounds, the element is operating in an acceptable manner.** For example, voltage and frequency of a signal may be selected as properties which satisfy operation (i.e., they meet the dimensional requirements of the element functional description). We may next determine that the peak voltage must not go below 10 volts or the frequency deviate outside the range of 1 MHz ±5 kHz. For, if this were to occur, the immediately succeeding element could no longer be expected to operate on the output (i.e., the levels are defined to the specification). We have thus defined the properties and their relationship to status. In addition, we have implied a very important result, viz, there is no reason why the same verification technique should be applied to each pertinent signal property.

Now consider an element whose functional description is simply: provide a faithful reproduction of the input signal amplified by A. In the first case, the functional description did not relate directly to the input. In this case, the output is described almost exclusively in terms of the input. This is a good example of the second method of addressing element output, i.e., output signals as they relate to the element input. Here we have the

*This discussion will consistently refer to the output of an element for the purpose of clarity. The same remarks will apply to the output of groups.

**Throughout the remainder of this report, verification techniques which operate in this fashion will be termed, collectively, monitoring techniques.

option of taking the absolute approach of the first case or identifying properties in terms of the relative measures. It will likely be difficult to translate "faithful reproduction" into absolute properties of the output and relative properties would likely have more meaning.* Here we could interpret phase shift, element frequency response and gain as relative properties.

The third method, input and output signals as they relate to the element operation, is more subtle than the first two. Consider an element whose output is complex and we desire comprehensive information about this element in real time. A possible method to achieve this is by introducing random noise at a very low level into the input signal (a symbiotic signal). If the output of the element is cross-correlated with the injected noise, the signal will cancel and the result will be the impulse response of the element.** The fourth method, comparison of the outputs of like elements in a set is straightforward. It is based on the premise that like elements performing the same function should have the "same" output for identical admissible inputs. If they differ, one of the elements is operating unsatisfactorily. We should note, however, that this method is not capable of indicating which element unless a form of voting is used.

In the preceding discussion, we addressed only those properties which immediately described the signal's form. If the pertinent properties of a signal are stochastic, these descriptions become all but meaningless. Under these circumstances, it is entirely possible to describe a signal by its statistics, particularly where continuous verification is desired. If the statistical representation provided sufficient confidence in the design, we can consider these as absolute properties of the output signal.

Let us add one more complication. To this point we have assumed that there would be a causative relationship through all time between the output and the operation of the element. That is, there is no part of the element which is not contributing toward producing the output. This can be violated in two ways: (a) the element contains nonlinearities (e.g., limiters, clippers, saturation, etc.) such that regions of the input signal will not effect a response in some portions of the element, (we say that the element is not exercised), and (b) the element contains distinct operating modes such that at least one mode does not require all element functions. If either of these two conditions exist, knowing the status of the output will not always be the same as knowing the status of the element - given the input is acceptable. In the former case, if the time during which portions of the element are not exercised is predictably short, there is probably little loss of information. If this time is known to be long and if the function not being exercised is critical, it is likely that we have to identify a state variable (which is otherwise unobservable) for verification.***

*This will be particularly true if the signal is stochastic and statistical representation is inadequate.

**This description has been oversimplified to illustrate the method. A detailed description of the technique is contained in Section 5.2.2.2.

***An alternate method is to inject a signal which exercises the element. It is not likely that this can be a symbiotic signal.

In the case where the element function changes with operating modes, we must account for this change by a comparable change in the verification design. Under these circumstances, there is not likely to be a reasonable means of verifying a function that is not used.

5.1.3 Time Profiles and System Partitioning

The first part of this section concerns itself with the time at which verification can be achieved on a noninterfering basis with the operation of the principal system. The motivation for time profiles is primarily centered around interest in when idle or simulative signals can be used without disrupting operations. The time profiles will also provide information on the duration of the operating modes described in the latter part of Section 5.1.2.

The second part of the section concerns itself with the functional relatedness of the principal system and identifying elements, sets and groups for synthesis of the verification design.

If redundancy in a principal system is to be verified on a continuous basis, properties of either the tenant signals, symbiotic signals or idle signals must be used. It is entirely possible that this cannot be realized at the desired level of confidence. This leaves but one alternative and that is the interrupting of system function for noncontinuous verification. Having resigned ourselves to this state of affairs, the next reasonable question is whether this type verification can be performed on a noninterference basis with the mission of the principal system. The time profiles will provide this answer and indicate the duration (or as a minimum the statistics of the duration) of time available for verification. If time profiles are available for each element, and these profiles are registered to a top system profile, it may be possible to find blocks of time when elements are not required during the mission. If we are fortunate, there will be a block of time for each element and simulative signals can be injected during these blocks of time to achieve the desired confidence in the design. However, if successive blocks of time for an element are spaced very far apart, it may still not be possible to achieve the desired confidence (see Section 5.3.1). Here we are left with but two choices; either interrupt the mission to perform verification or perform continuous verification, at a reduced confidence, during the time between "free" blocks. Some systems, such as aircraft, will have successive missions interrupted by periods of time on the ground for refueling, servicing and the like. This is a block of time during which all elements are available (or can be made available) for high confidence verification. A lower confidence verification can then be performed during flight (the mission).

There is an additional piece of information that can be extracted from the time profiles and that is programmed modes of operation for the elements.* As indicated in Section 5.1.2, these various modes of operation can (and usually do) influence the element output or its causative relationship with the operation of the element. Knowing the occurrence and duration of these modes will allow us to apply strategies similar to those described in the

*Programmed modes have been indicated since there are many forms of operation which, for the purposes of determining their occurrence, exhibit random use of modes.

preceding paragraph. We note also that modes which occur randomly can be handled by extending the principal system mode control signals to the verification equipment, causing it to alter its characteristics commensurate with the change in element output character.

Let us now turn our attention to system partitioning, for it is here that the groups and simple sets are established. To illustrate the process, a hypothetical system has been partitioned in Figure 5.1.3. A functional diagram was selected to portray the system in lieu of a reliability diagram since the functional interrelationships of the elements is quite important.* This approach also has its disadvantages in that it is difficult to distinguish redundancy from parallel flows of information through separate functions. In this regard, care must be taken in interpretation. Blocks 1.0, 3.6, 2.0 and 3.0 are intended to be parallel flows through separate functions. Parallel paths in the remainder of the diagram represent redundancy in various forms. Block 1.4 exemplifies interrelated redundancy since one element feeds two instances of redundancy. This block is then identified as a group. Block 1.5 is a simple set with degree zero redundancy. Since one leg of the parallel paths in block 1.6 contains redundancy, these elements have been identified as a group (a set cannot contain another set). Block 3.4 is a simple set since point A feeds both elements and no other instances of redundancy. Block 3.6 is a simple set with degree zero redundancy (all three parallel functions are required).

System partitioning accomplishes four things: (a) it breaks the principal system into manageable pieces, (b) it identifies signal flows at the major points of interest, (c) it identifies groups and sets and (d), it provides a basis for identifying whether status of each element in a set can be determined or whether status of a set itself is all that can be achieved. Point (c) is quite important since the group and simple set problems are approached from different viewpoints.

5.1.4 The Group Policy

Before design can begin, it is important to establish guidelines and concepts under which the design is to evolve. These guidelines represent the initial translation of gross system specifications and operations requirements into generally broad requirements of the redundancy verification design. As such, they will typically address the group problem and form the group policy. This policy will aid in selecting (if not dictate) the group fault deduction methods and influence the extent to which a central processor (or satellite processors) will be used in the design. Some of the primary functions of the group policy are to establish functional interfaces with other systems, indicate compatibility implications and provide an indication of available resources in the principal system which might also be utilized or shared by the redundancy verification system.

---

*The importance of functional descriptions and functional interrelatedness cannot be emphasized too strongly. Section 5.1.2 indicates the importance of functional descriptions in identifying the method of treating the output signal and identifying the properties of that signal indicative of operation. The relationship between functions is important to the extent that it is the key to redundancy and how it is achieved. Equipment does not necessarily have to be electrically or mechanically connected to be functionally related.

Also of prime importance in this initial stage are policies regarding isolation/independence of the redundancy verification system. These points will many times conflict with the latter point of the previous paragraph and the resolution can only be achieved through trade studies. It is important that the verification system remain isolated from the principal system from the standpoint of inducing failures. It is also important that, within reasonable bounds, the verification system remain independent on a power and environmental basis. Where these points cannot be achieved, additional care must be given to failure modes which may not be detected due to commonality of power or common thermal drift rates in parts for both systems.

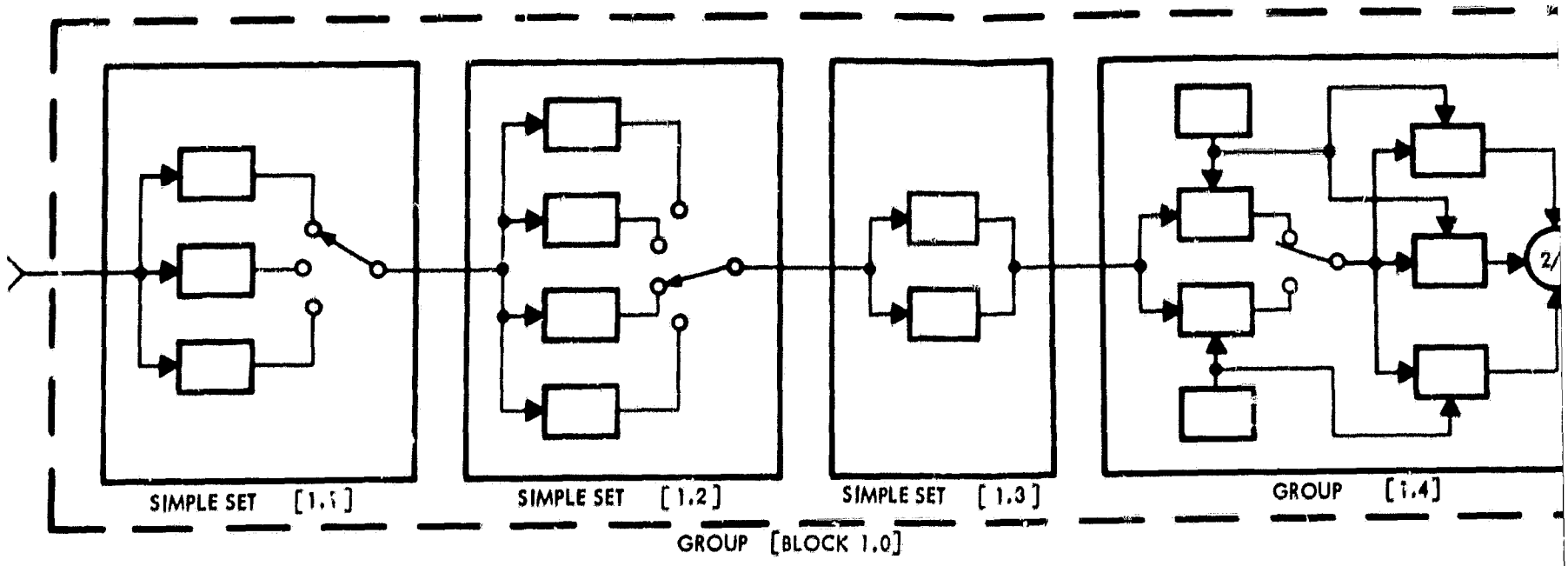
Having sketched the inputs and initial design efforts, let us now proceed to describe the design process itself. This is the subject of the following section.

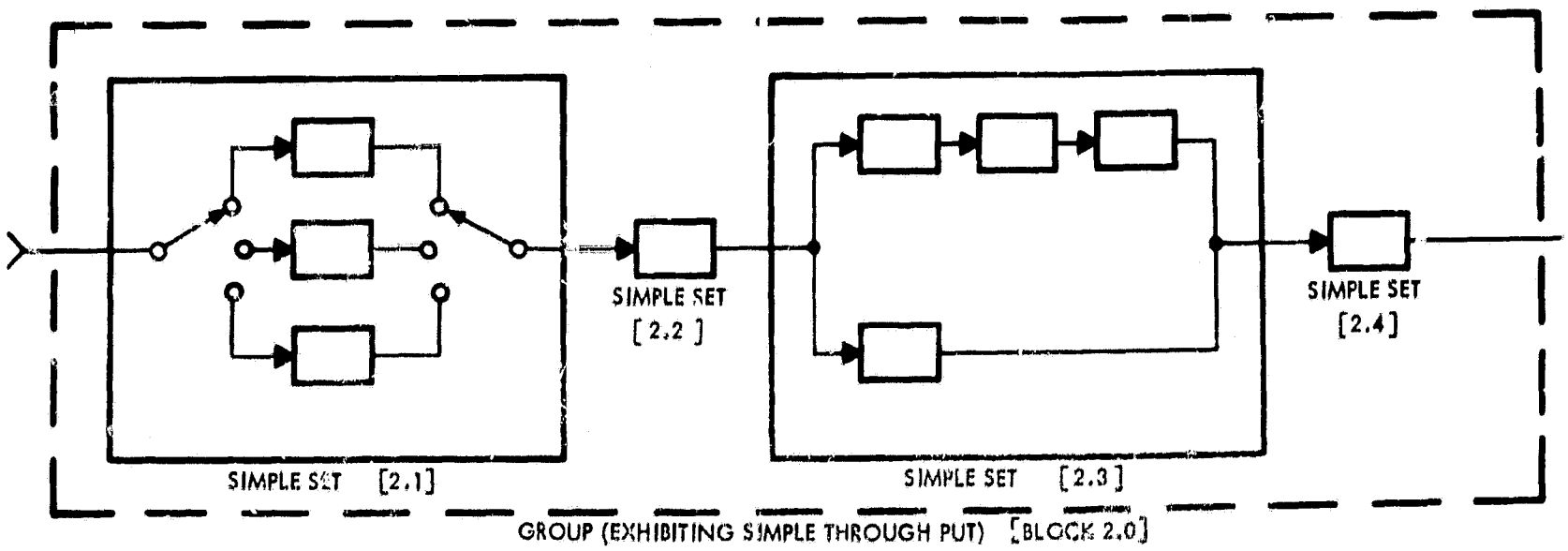
5.2 The Design Process

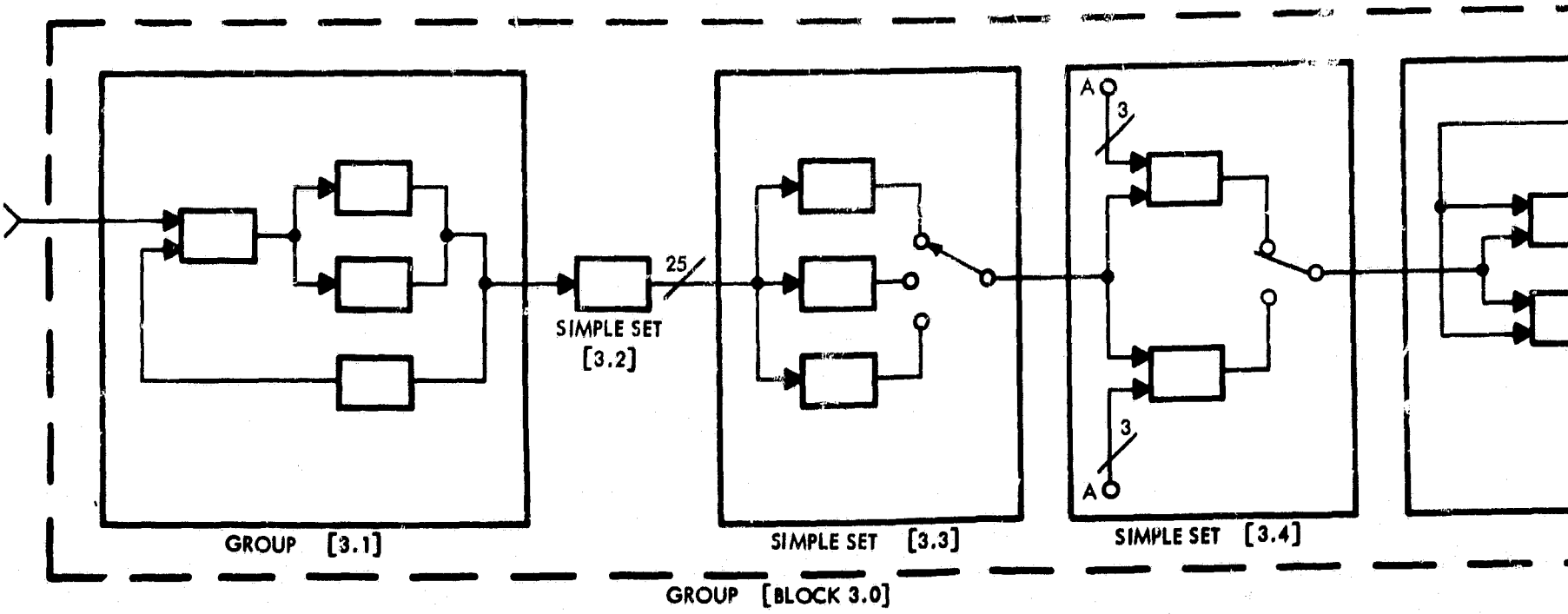
This section is intended to describe the steps in the design of a redundancy verification system using the information described in Section 5.1. The theme is one of presenting design alternatives and guidelines for selecting an alternative under a given set of circumstances. The section has been organized to address the two basic divisions in the design process--the set problem and the group problem. The set problem has been approached from the standpoint of the functions which must be performed to determine redundancy verification at this level. The group problem has been approached from the standpoint of the deductive methods which can be used to determine verification under the comparatively involved relationships existing in groups.

Before the design methodology is described in detail, it is appropriate to consider the flow of the process. As shown in Figure 5.2, the design process begins by consideration of the higher level group problem. It then branches to two parallel paths - the set (simple set) and the general group problem. The parallel branches are not intended to imply independence, rather they imply two distinct problems requiring two different methods of solution. The two problems can be solved somewhat autonomously but a constant exchange of information is required to realize a rapid convergence to a final design. The implication of convergence and feedback is portrayed by the last block. It is not expected that a design can flow smoothly down a well marked path to a final solution. Trade studies must be made to direct the course of the design and folding back to retrace portions of the path already traveled is inevitable as more detail is developed and the picture becomes clearer.

The higher level group problem, the set problem and the general group problem are discussed in Sections 5.2.1, 5.2.2 and 5.2.3 respectively. Before we begin these discussions; however, it is appropriate to add some further explanation to the selection of the names for the two group problems. The higher level group problem is fundamentally systems oriented and the name has simply been selected to reflect this fact (recall that a level one group was the smallest identifiable group). The general group problem is concerned exclusively with status identification for all levels of groups. Throughout the remainder of the report we shall, for brevity, identify the simple set problem as, simply, the set problem and the general group problem as, simply, the group problem.







FOLDOUT FRAME 7

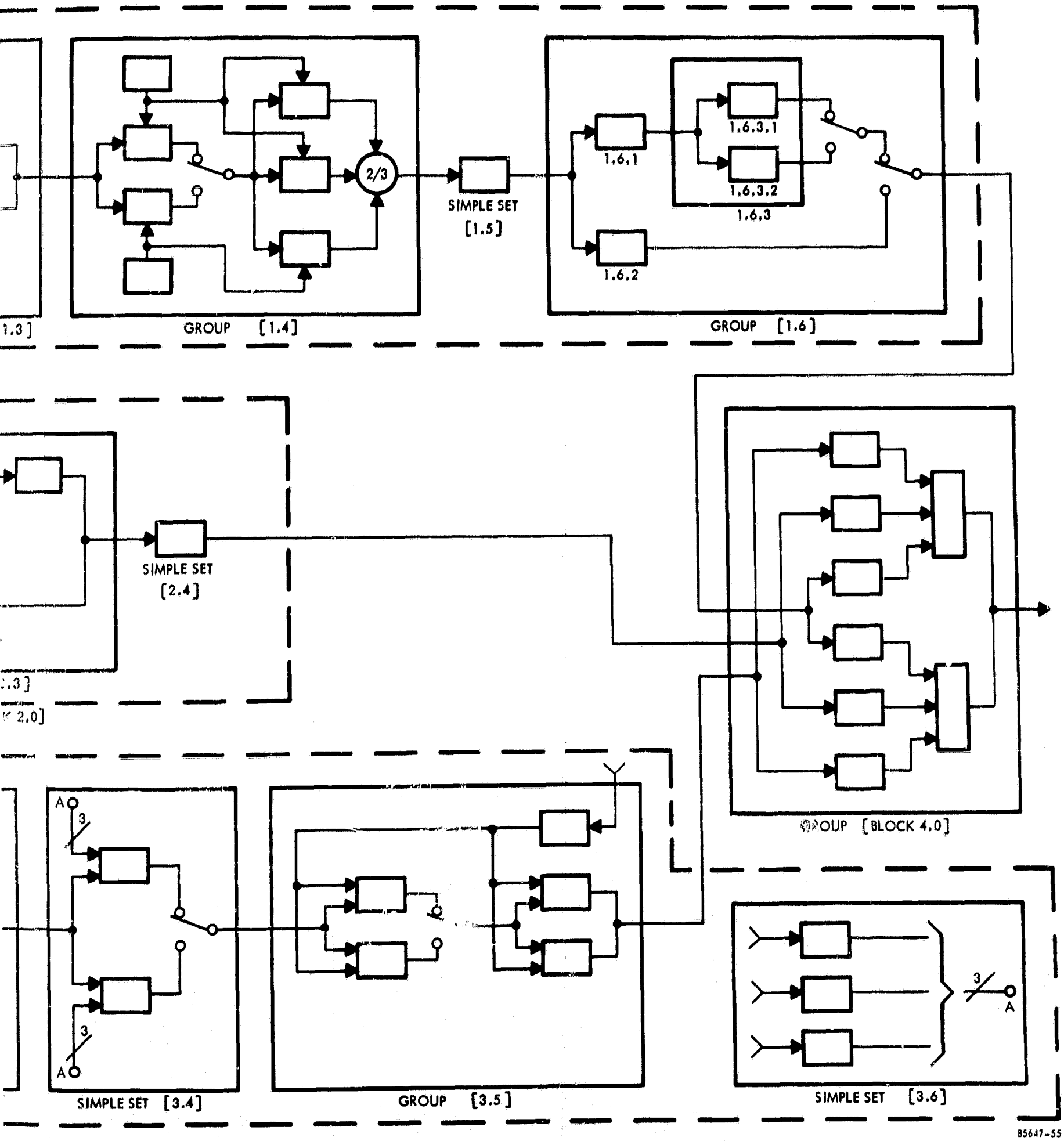


Figure 5.1.3. Sample System Showing Identification of Groups and Sets, Functional Diagram

FOLDOUT FRAME 2

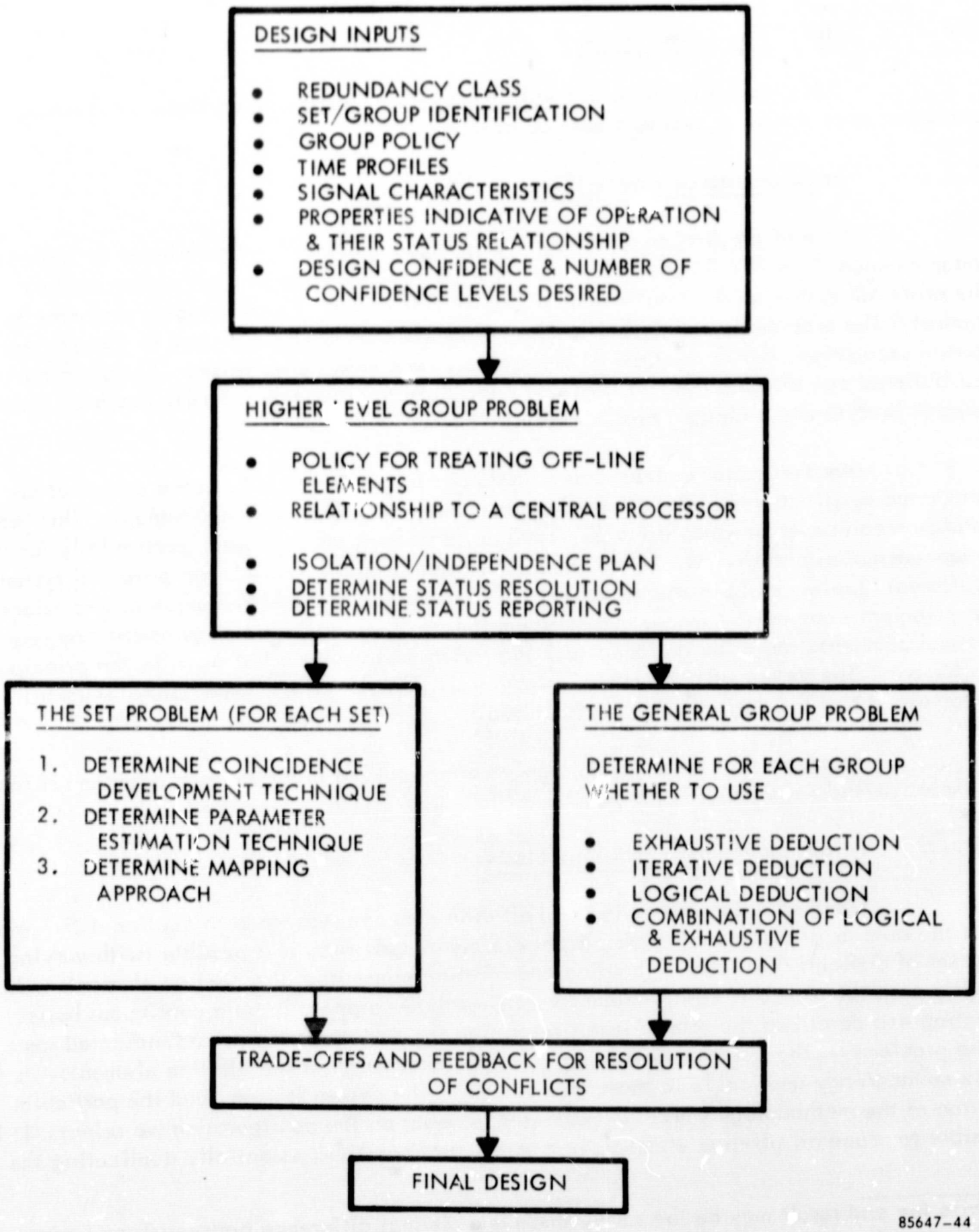


Figure 5.2. The Redundancy Verification Design Process

5.2.1 The Higher Level Group Problem

This problem is concerned with the overview of the redundancy verification design. Let us examine the most pertinent considerations.

5.2.1.1 Isolation/Independence Plan

One of the first concerns about any automated verification scheme is that of failure independence.* Will a failure in the verification equipment cause a secondary malfunction in the principal system or short out tenant signals? This is a legitimate concern and must be guarded against. The problem is usually not so chronic in the mechanical area due to the existence of spatial separation, but in the area of electronics, care must be exercised. Long leads that are not buffered can affect pulse rise time and contribute to cross-talk. Poorly designed grounding can lead to unanticipated cross-coupling.

Another major concern, as pointed out in Section 5.1.4, in the design of an automated verification system is that of independence of power and environment. This independence can never be completely achieved but care must be exercised, particularly for thermal independence of electronics. If the verification equipment is housed with principal system equipment, (unless it is put in an oven) it will experience the same temperature excursions as the principal equipment. Under these circumstances, the verification equipment may require thermal compensation or be designed such that drifts essentially offset drifts in the principal equipment. The extent of these measures obviously depends on the temperature extremes encountered and the desired accuracy required.

To assure that these points receive attention and that a uniform approach is taken, an Isolation/Independence Plan should be set forward.

5.2.1.2 Policy for Treating Off-Line Elements

The distinction of on-line and off-line elements was made in Section 4.5. Whenever the outputs of elements in a simple set are distinguishable, it is possible (with varying degrees of difficulty) to identify on-line and off-line elements. The on-line elements will usually pose the most difficult problem for verification--especially on a continuous basis. (Section 4.6 described the role of status resolution for on-line elements and indicated some of these problems.) The question now arises as to the disposition of the off-line elements. Is the same methodology applicable to these elements?** The answer is, yes, and the particular portion of the methodology which is applicable depends on the configuration we select. It is possible to place all off-line elements in a series configuration, essentially duplicating the

---

*While the end result may be the same, there is a distinct difference between Type I errors (or failures) within the verification equipment and failures induced in the principal system by the verification equipment.

**It is not the intent here to address specific techniques for verification since these are thoroughly covered in Section 5.2.2.2.

on-line system. The extention of the methodology under these conditions is obvious but let us note some special points about this approach. First, switching would be necessary to accomplish the reconfiguration. Second, a failed element, either on-line or off-line, would curtail verification of the "off-line" system until repair was effected.

A second, and more obvious method of treating off-line elements is to simply let each be an entity and verify it on its own basis. This can be accomplished in two ways: (a) perform verification while the element is operating on the input tenant signal, or (b) inject a simulative signal into the element. If the element contains entities which must be updated in time, (stored data, time variable logic, etc.), approach (a) is the only feasible solution. If the redundancy is nonsymmetrical or if the capabilities of the elements differ, (b) is usually the logical choice.

There are other schemes applicable to this problem--especially if there are two off-line elements in a set. Without pursuing these; however, it can be seen that a policy regarding the treatment of off-line elements is essential at the outset of a design. Perhaps the most important point to be made in this section is that there is no reason why verification of on-line and off-line equipment should employ the same techniques.

5.2.1.3 Determination of Status Resolution and Status Reporting

Status resolution and status reporting are two functions which must be accomplished at the system level. Status resolution has been discussed but status reporting is a new term. The status reporting function is simply the displaying, presenting, annotation, etc. of verification results. It is the machine-man interface. The only point to be made here about reporting is that the medium and frequency of reporting must be established at the outset of the design.

Depending on the verification approach used, status resolution can be a key ingredient in the design. Recall that status resolution performs the function of identifying the faulty element in an on-line system from possibly several unconditional status indications of unsatisfactory operation. This is a deductive process and it can be accomplished so long as we are not trying to identify elements in a closed loop that are using the tenant signals for verification. Or, so long as no ambiguities exist. Such a function would typically be implemented by a digital processor. Less costly hardware approaches are feasible; however, for systems which do not change operational configurations. The hardware approach has the advantage of simplicity and reliability. The processor approach is flexible and, if a processor is required for other functions, provides compatibility. The extent to which a central processor will be used for status resolution must be identified. The final choice could be a combination of hardware and software.

It should also be recognized that, for noncontinuous verification, status resolution can be augmented (or completely replaced) with the use of simulative signals injected at various points. This is essentially the reverse of the approach used above for on-line continuous verification.

5.2.1.4 Relationship to a Central Processor

Part of this topic has already been discussed in the previous section and the entire subject is addressed in detail in Section 5.4. We should like to point out that a processor can be used in varying degrees of sophistication to accomplish varying numbers of functions. Aside from status resolution, there will be statistical and smoothing problems to be solved, mapping (decisions) to be performed and comparisons to be made. (See Section 5.2.2.) To this point we have only considered functions and not how those functions would be implemented. It is now possible to purchase off-the-shelf, 8-bit A/D converters in a single microcircuit package. With such devices we can run the gamut of sophistication. A processor could perform one function, say, status resolution or it can perform the entire redundancy verification, starting with A/D converters at the tenant signals. The relationship to a central processor, at least in terms of functions to be performed, should be clear during early stages of the design.

5.2.2 The Set Problem

Whether attacking the problem of verifying a great amount of redundancy or the problem of an isolated occurrence of redundancy, the designer will frequently discover that his attention has become focused on verifying redundancy which may be described, according to the notions introduced in Section 4.3, as a simple set. Indeed, some forms of solution of the group problem will be seen to lead one to the consideration of verifying the redundancy of one or more simple sets in order to determine the presence of redundancy within the group. It is therefore proper that the problem of verifying redundancy in simple sets be directly addressed.

The uniqueness of the simple set lies in the fact that for the purposes of redundancy verification it may be considered as an entity, independent of other redundant sets and groups. This means that the simple set may be isolated, at least mentally, from all surrounding equipment and that its status may be determined entirely from its own input and output.

Throughout this discussion, it will be considered that if element outputs remain distinguishable, no set output as such will have been formed. If, for example, element outputs are time multiplexed into a serial information stream, no true set output will be present. Element outputs will still exist, only in a different arrangement. It should be recalled from the definition of redundancy class H that, if a set output is formed, the verification of redundancy will be impossible unless there exists some output effect which varies as the number of operating elements in the set.

In approaching the simple set problem, it should be considered that a first goal is to achieve continuous verification since, if this is possible, one may always choose to use the available information on a periodic or occasional basis. However, if continuous verification is not achievable, it may be difficult for the user to establish in his mind, confidence in the operation of his equipment during the period between redundancy verifications. When, in the course of the design process, continuous verification becomes unrealizable, the use of periodic verification will be looked upon as a retrenchment from a desirable but untenable position.

Certainly, to achieve redundancy verification on either a continuous or a periodic basis, it will be necessary to observe a signal which possesses all the characteristics necessary for the establishment of design confidence. The question is whether the tenant signal fits this description.

The desire to achieve continuous verification and the necessity of having a signal suitable for verification lead to the conclusion that one should, first of all, try to accomplish verification using the tenant signal. If this is not possible, the next step should be the consideration of signals which may be injected without interrupting the flow of tenant signal information. Failing the identification of a suitable solution here, one will be forced to use injected signals and divert equipment from its primary purpose in order to dedicate it to verification.

5.2.2.1 Functions to be Performed

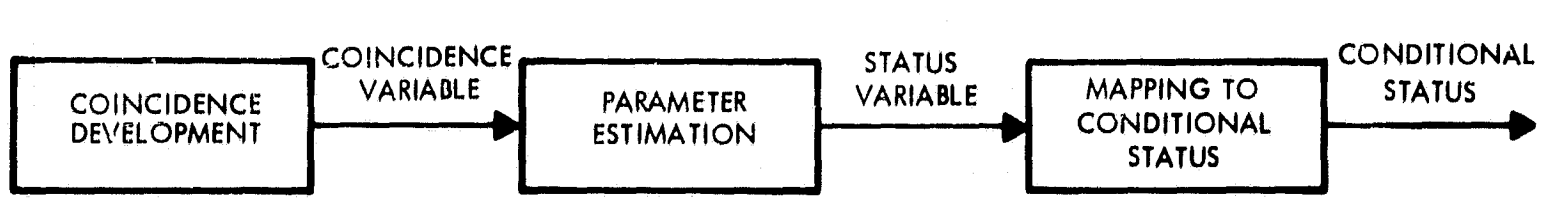
It will be advantageous to consider redundancy verification, as applied to the set problem, as being comprised of three distinct functions. These functions are depicted in Figure 5.2.2.1-1.

In every case of verification, the first step is to derive from the system some indication of its operation and perform a comparison with information which describes, either directly or indirectly, either wholly or in part, what the operation is expected to be. Because this comparison is a test of coincidence between the expected and the actual, this function has been denoted as coincidence development. Because the output of this operation will be a variable quantity indicative of the degree of coincidence between the two items being compared, it has been denoted as the Coincidence Variable.

The following function, an operation on the coincidence variable, has the task of transforming this information into a quantity indicative of the conditional status of the item being verified (IBV). The output quantity spoken of here, because of its role in the operation, will be referred to as the status variable. The transition to a status variable will generally be performed by one of a set of techniques referred to mathematically as parameter estimation techniques. Hence, this second function has been called the parameter estimation function. It will become clear as this discussion continues just why such a function is necessary.

When the status variable is interpreted, the result is a statement of conditional status. It may be anticipated that conditional status will be a set of discrete statements such as go-no go, good-bad, stop-caution-go, etc. The interpretation process is depicted in Figure 4.6 and may be viewed as a decision of into which slot to put a given value of a status variable. This is a mapping operation in which status variable values are mapped into the possible regions of conditional status. The third function, for these reasons, has been designated the mapping function.

A simple example is given in Figure 5.2.2.1-2 to illustrate the application of these concepts. In this example, the coincidence development function derives an indication of peak signal value and expresses the coincidence between this derived value and an expected



85647-48

Figure 5.2.2.1-1. Verification Functions - Set Problem

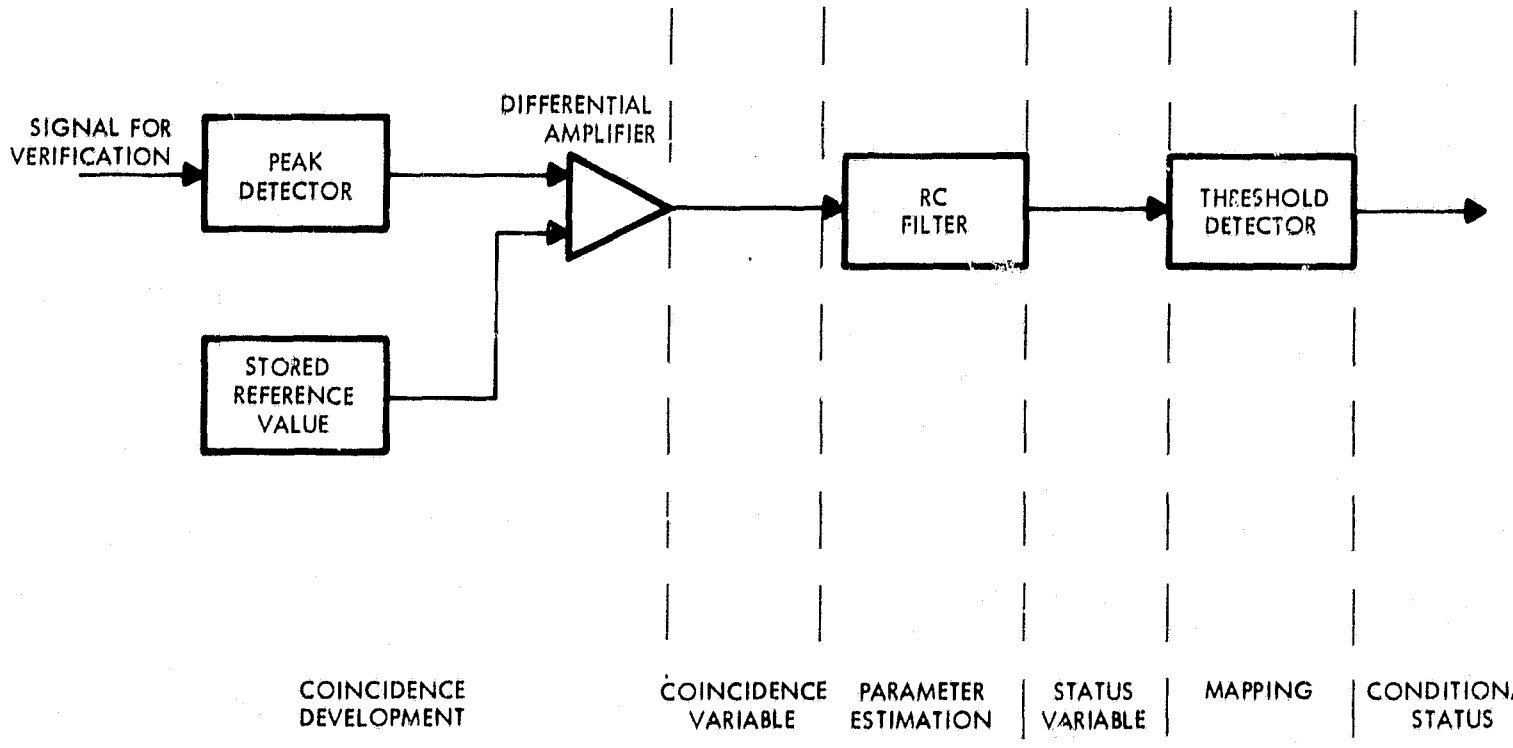


Figure 5.2.2.1-2. Example of Verification Functions

value. An RC filter then performs an exponentially-weighted integration on the coincidence variable. The output of this filter, the status variable, is then compared against a threshold. It is implied here that there are two regions of conditional status. For present purposes, call these conditional go and conditional no-go. Values of the status variable below the threshold value will map into the conditional go region. Values above the threshold value will map into conditional no-go.

While the coincidence and status variables have been represented here as straightforward, one dimensional quantities, in many practical cases they will be multidimensional with their values expressed as vectors. Also, it is possible, indeed likely, that the verification of a single item will require the employment of several combinations of these three functions or several different "chains" of the three. The degree of complexity realized in these areas of implementation is primarily dependent on the amount of information required to establish the desired level of design confidence.

The three functions introduced here are discussed in detail in the following sections.

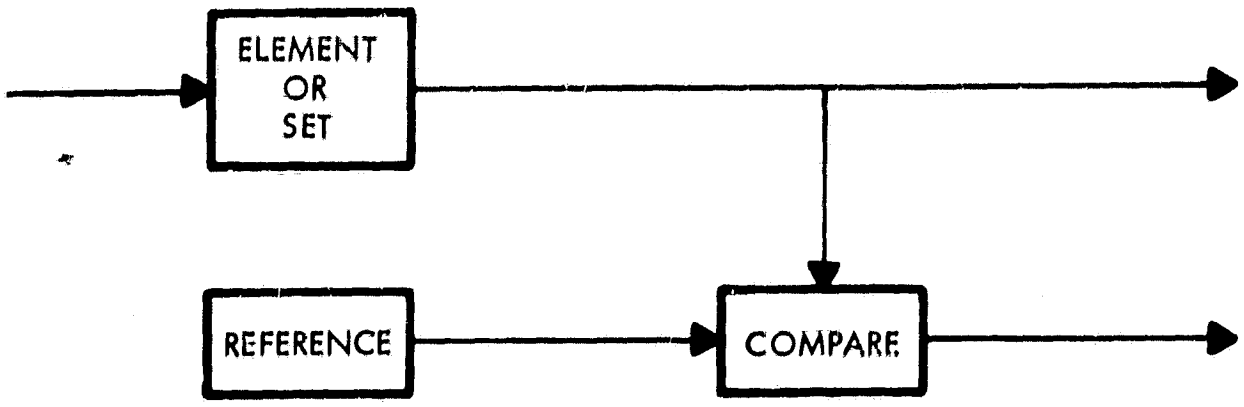
5.2.2.2 Coincidence Development

The first function to be performed has been identified as that of coincidence development. In every case, the object of this function is to gather, in elementary form, information reflecting on the operation of the element or elements under scrutiny. In fact, it is taking the first step toward determining whether that operation is what it is expected to be. The word operation is applied under the concept that the input signal is operated on to form the output signal. For a linear system (additive and homogenous), a complete description of this operation in the time domain is the impulse response; for the same system, the transfer function is a complete description in the frequency domain.

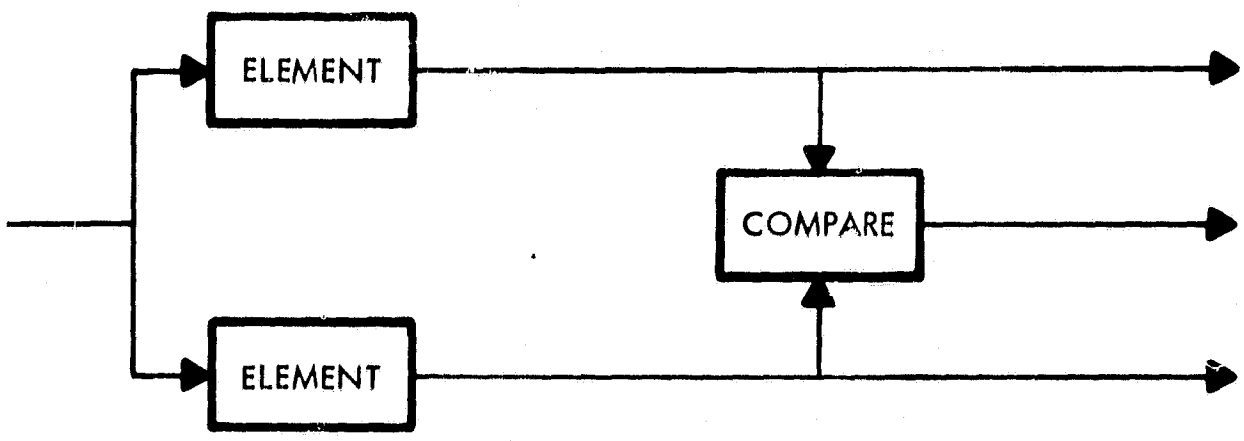
There are three possible approaches which are represented in Figure 5.2.2.2-1.* One may compare output to a stored reference. If the character of the input is known and the reference represents the expected output signal or a property thereof for an input such as is used for verification, a comparison between the output and the reference will reflect on the similarity between the operation of the item being verified (IBV) and the operation expected of it. Alternately, wherever two or more identical (and independent) operations have the same input, a comparison of their outputs reflects on the similarity of the two operations. In this case, status identification of the elements must rely on the assumption that both (or all) operations have not changed in the same way from their expected form; i.e., that they have not been altered to be identical but unacceptable operations.

Both of the above approaches involve deductive processes. The third, the comparison of output to input is a direct measurement of the operation which may be checked against the expected operation.

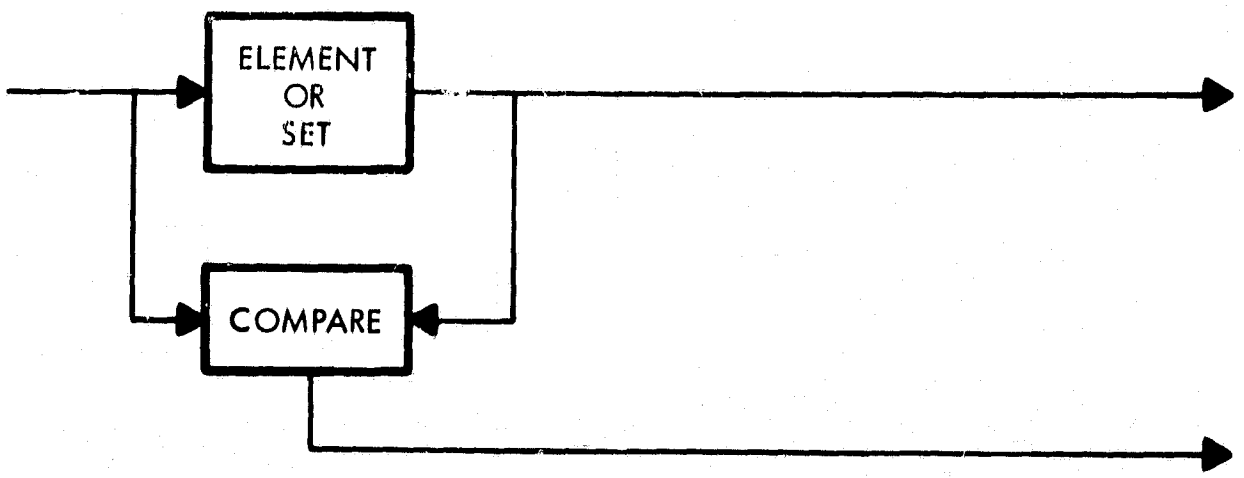
*These approaches are the same methods identified in Section 5.1.2 with methods two and three of that section merged to form the single approach of Output/Input comparison.



OUTPUT/REFERENCE COMPARISON



OUTPUT/OUTPUT COMPARISON



OUTPUT/INPUT COMPARISON

85647-45

Figure 5.2.2.2-1. Approaches to Coincidence Development

The comparisons here may be instituted in either the time or frequency domains and in the time domain may be carried out either on the basis of signal values or signal form characteristics such as mean value, rms value, etc., which are functions of signal form. These thoughts have led to the establishment of the following classes of techniques for coincidence development.

Output/Output Comparison

Compare Two (time)
Voting (time)
Crosspower Spectral Analysis (frequency)

Output/Reference Comparison

Value Checks Sequential (time)
Value Checks Nonsequential (time)
Coding (time)
Signal Form Analysis (time)
Spectral Analysis (frequency)

Output/Input Comparison

Inverse Transform (time)
Correlation (time)

If it is the case that the item under investigation is characterized by a signal generation such as an oscillator instead of by an operation on an input signal, comments to be made about those techniques employing output/output comparison or output/reference comparison may be applied with no loss of generality. Techniques using output/input comparison will not be applicable at all.

The techniques enumerated above will be defined as follows:

- Compare Two - techniques whereby the outputs of two elements are compared on the basis of their values.

This definition allows the comparison of signal values on an analog or discrete basis. A conceptual example appears in Figure 5.2.2.2-2.

- Voting - techniques whereby inference to operational integrity is drawn from a logical polling of outputs or combinations of outputs.

It should be pointed out that Voting here means voting as an approach to parameter determination and has no relationship to voting in the achievement of redundancy or accuracy. To make this clear, the conceptual example in Figure 5.2.2.2-2 shows Voting applied to a majority voting system.

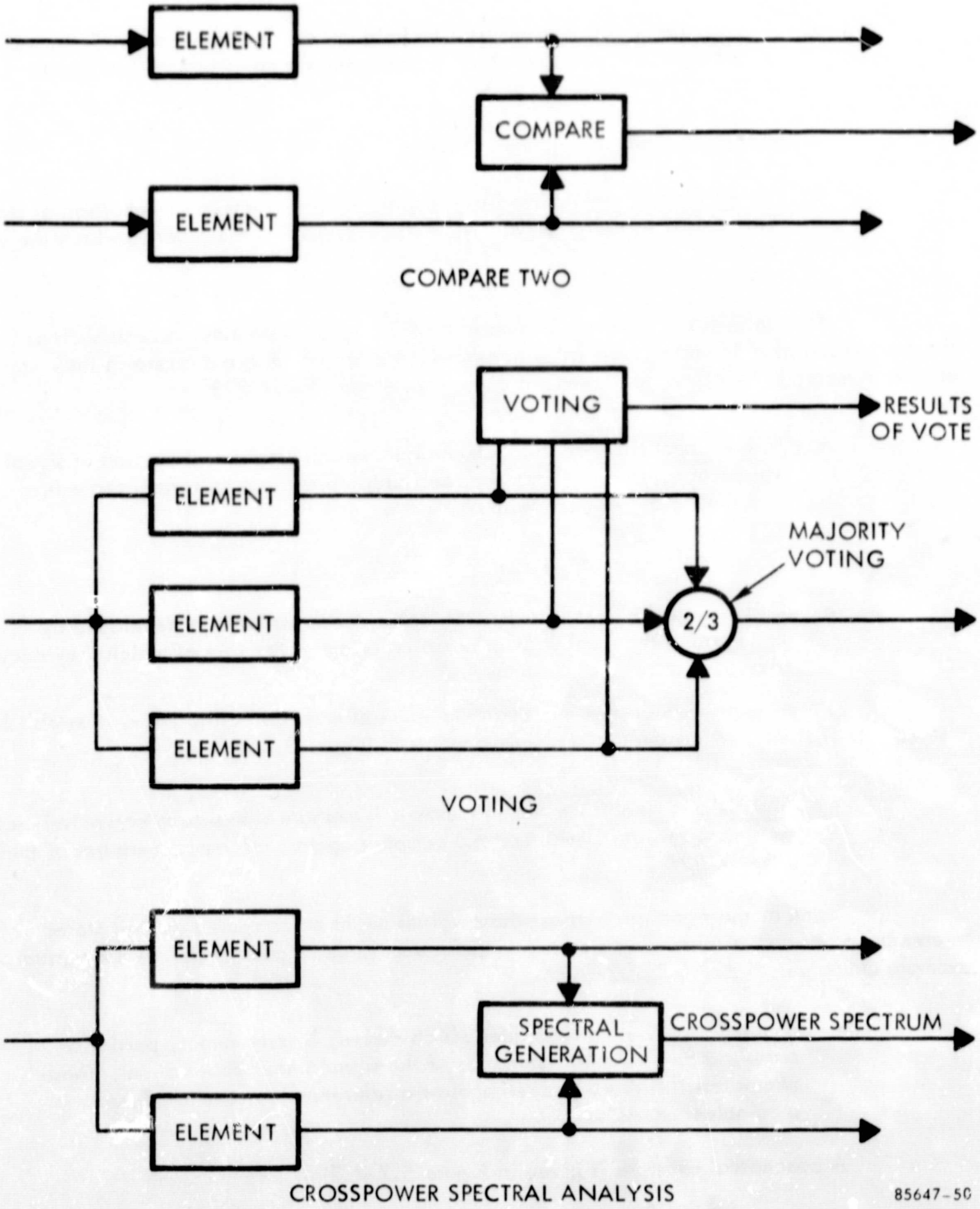


Figure 5.2.2.2-2. Examples of Coincidence Development Techniques

- Crosspower Spectral Analysis - techniques which involve the development of a frequency spectrum which is the combination of the spectra of two output signals.

A conceptual example appears in Figure 5.2.2.2-2.

- Value Check; Nonsequential - techniques which employ comparison of signal value(s) with reference value(s) without regard to the order in which the values occur.

This definition allows the comparison of values on a continuous basis such as the comparison of a dc voltage against a threshold. Values which are discrete in time may also be compared. A conceptual example appears in Figure 5.2.2.2-3.

- Value Checks; Sequential - techniques which employ comparison of signal values in a sequential manner, deriving information both from the values and their order of occurrence.

A conceptual example appears in Figure 5.2.2.2-3.

- Coding - techniques whereby the coincidence variable is developed by determining the number of information errors or the rate at which they occur.

These techniques employ the characteristics of error detecting codes to establish a statement of status. A conceptual example appears in Figure 5.2.2.2-3.

- Signal Form Analysis - techniques which measure signal form characteristics, as opposed to signal values, and compare against reference measures of these properties.

Some of the signal properties whose values might be compared against stored reference values are instantaneous frequency, peak amplitude, signal mean. A conceptual example appears in Figure 5.2.2.2-3.

- Spectral Analysis - techniques which derive, by any means, partial or complete spectral characteristics of the signal under observation. These characteristics are compared against a reference in order to generate a coincidence variable.

A conceptual example is given in Figure 5.2.2.2-4.

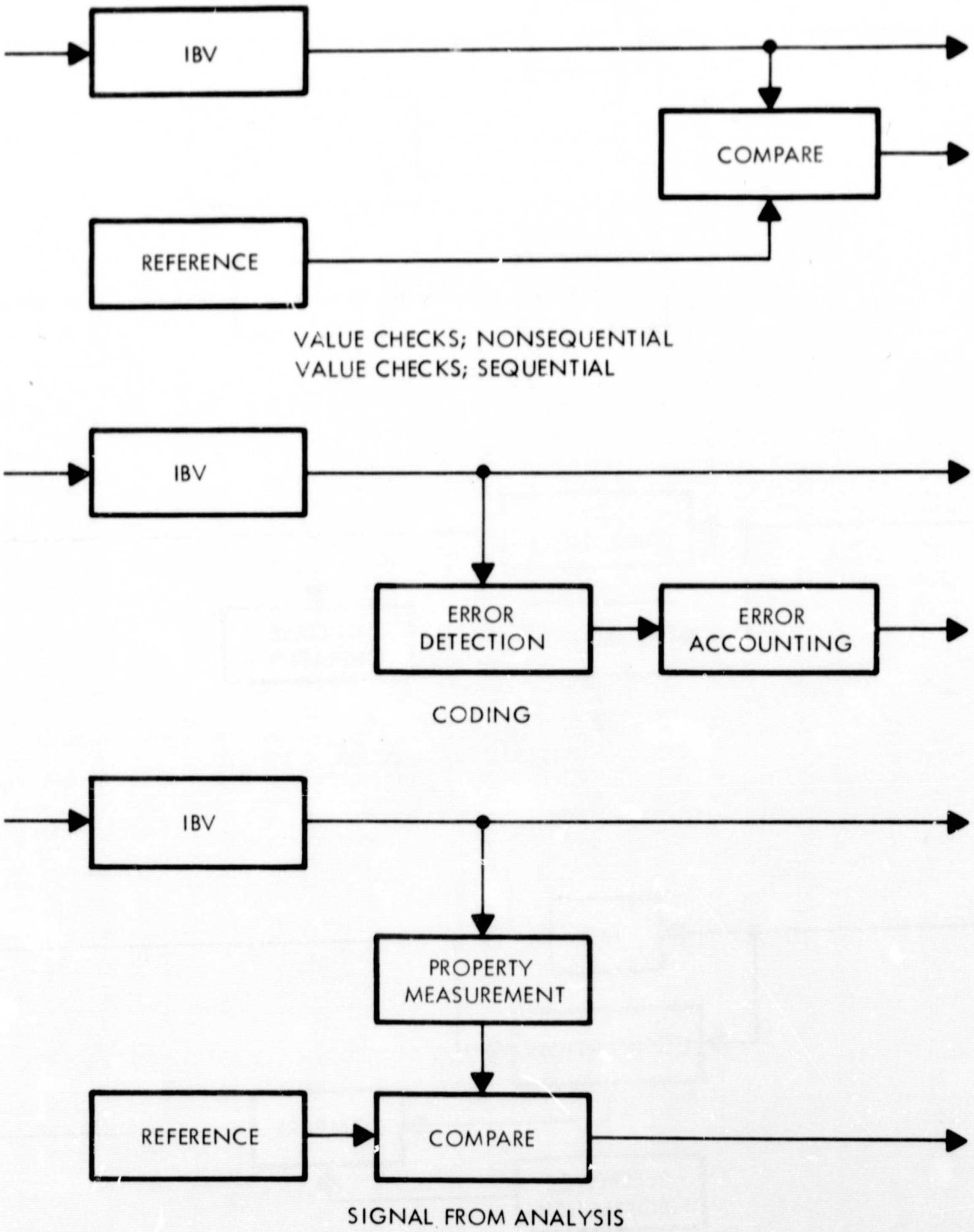
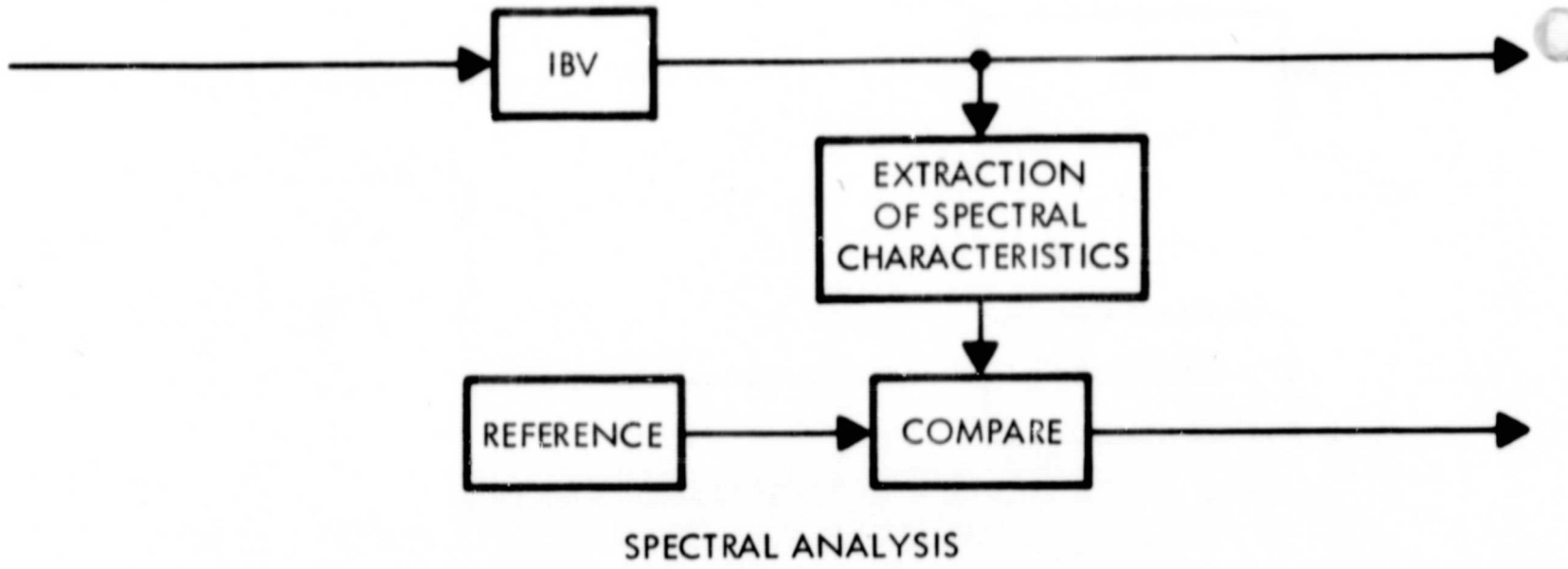
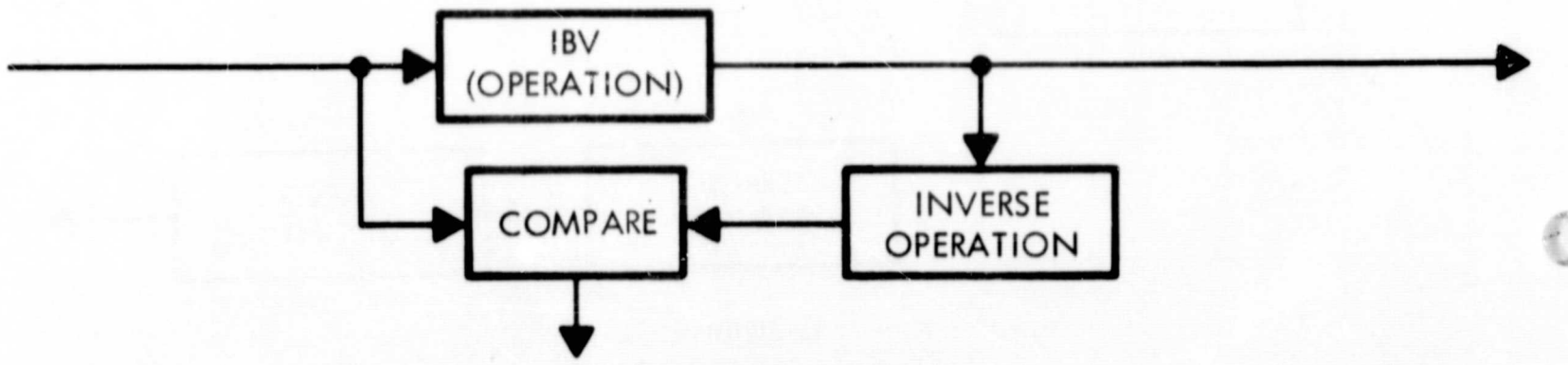


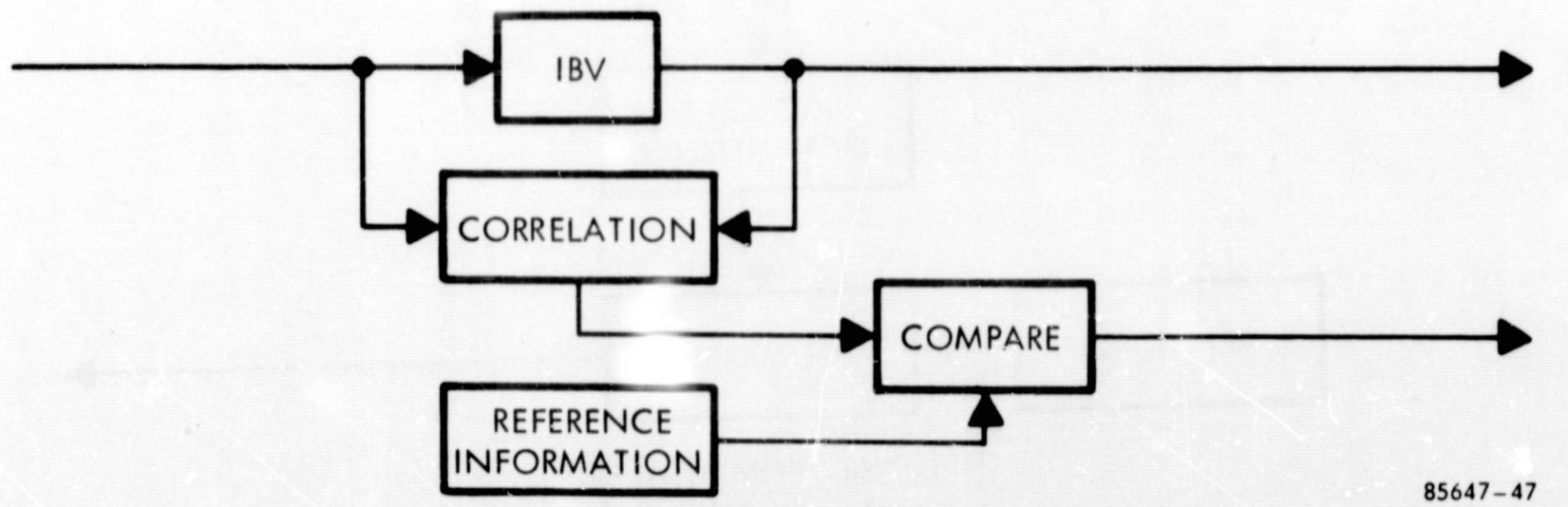
Figure 5.2.2.2-3. Examples of Coincidence Development Techniques



SPECTRAL ANALYSIS



INVERSE TRANSFORM



CORRELATION

Figure 5.2.2.2-4. Examples of Coincidence Development Techniques

- Inverse Transform - techniques which perform, on the signal under observation, an operation which is the inverse of that performed by the item being verified and compares the result to IBV input.

The idea behind these techniques is to convert IBV output to the state of IBV input and compare the two. A conceptual example appears in Figure 5.2.2.2-4.

- Correlation - techniques whereby an inference to operational integrity is drawn through correlating the input with the output of the IBV.

A conceptual example is shown in Figure 5.2.2.2-4. The reference information represents expected results of the correlation.

For the sake of completeness, two other presently used schemes have been included.

- Acknowledgment - techniques whereby the receipt and desired effect of a command is indicated through a separate return signal.

- User Complaint - techniques whereby the status is directly determined by the observation and judgment of the user.

These approaches may be considered to be means of automated redundancy verification only if one accepts the groundrule that backup equipment is so reliable that it does not require verification. (See Section 2.2.) A good application of User Complaint would be to automobile power steering. The pilot of an aircraft with landing skids would consider the Acknowledgment that his landing gear was down a verification of redundancy.

It will be helpful to employ two additional notations.

- Signal Form Analysis/Compare Two will be taken to mean approaches in which a signal form characteristic of an output signal is observed and the observation is compared to a similar one made upon a different output signal. A comparison of the rms values of two element output signals would exemplify such an approach.

- The term "monitor methods" will be used to refer to those techniques which employ the storage of reference information concerning signal values or signal form characteristics. This will be advantageous because several general statements can be made on the basis of this characteristic alone. Monitor methods will include Sequential Value Checking, Nonsequential Value Checking, Coding, Signal Form Analysis, and Spectral Analysis.

The discussion thus for has concentrated on identifying techniques. It is now pertinent to inquire as to the relationships of these techniques to the design inputs and the material of Section 2.0. To what extent do redundancy classifications and signals influence the use of these techniques? Recall from Section 2.2 the redundancy classes were found to

be independent of signals. Using this conclusion and developing a signal property classification, it is possible to realize a matrix showing the applicability of each technique to various conditions of redundancy and signal property classes. This applicability is shown in Figure 5.2.2.2-5. Here, the appearance of a coincidence development technique in an element of the matrix indicates that technique may be applied to the situation represented by the coordinates of the element. Recall that the redundancy classes are defined in Figure 2.3.

The reasoning leading to the expression of adaptability set forth here is perhaps most simply understood by first considering, in turn, each class of coincidence development techniques and listing those characteristics of various situations which would obviate the employment of that class.* This leads to the following facts:

- Monitoring techniques (value checks; nonsequential, value check; sequential, spectral analysis, and statistical moments) cannot be applied to stochastic nonstationary signal properties. This is because these techniques demand comparison against stored information which represents what is expected of the output.

- Compare Two and Cross Power Spectrum techniques are not applicable to set output nor where it is necessary to indicate the status of each element. Therefore, they must not be associated with redundancy classes E, F, and G.

- Coding and Voting techniques, like those classed as Compare Two, cannot be used when the outputs/effects of each element are not distinguishable and cannot be associated with class G.

- Neither Acknowledge nor User Complaint techniques can be used if outputs/effects of each element are not distinguishable or if continuous verification is required. Therefore, these techniques cannot be identified with any of redundancy classes A, B, E or G.

- Value Check techniques require the prediction of signal values and therefore cannot be applied where no deterministic signal is present.

These observations dictate a large number of matrix elements wherein particular coincidence development techniques may not appear. This is not sufficient information, however, since it is true that the appearance of a class of techniques in a matrix element does not restrict application to either set or element output. This is because, in addition to the definitions of the redundancy classes, the verification techniques themselves may impose such a restriction. Superscripts are employed in Figure 5.2.2.2-5 to make clear this situation.

In interpreting the completed matrix, one should realize that the rightmost column, "Independent of Signal Class," must always be given consideration. That is, a list of all classes of coincidence development techniques applicable to a given situation should be

*The reader will find it helpful to refer to Figure 2.2.

SIG. PROPERTY CLASS / RED. CLASS	DETERMINISTIC	STOCHASTIC W/ DETERMINISTIC SYMBIOTIC SIG.	STOCHASTIC STATIONARY	STOCHASTIC NONSTATIONARY	STOCHASTIC NONSTATIONARY W/RANDOM NOISE	INDEPENDENT OF SIGNAL CLASS
A	SP^2 VN^2 SF^2 VS^2	SP^2 VN^2 SF^2 VS^2	SP^2 SF^2		SP^2 SF^2	CD^2 V^3 IT^2 CS^3 CR^2 CR^3
B	SP^3 VN^3 SF^3 VS^3	SP^3 VN^3 SF^3 VS^3	SP^3 SF^3		SP^3 SF^3	CD^3 V^3 IT^3 CS^3 CR^3 CT^3
C	SP^2 VN^2 SF^2 VS^2	SP^2 VN^2 SF^2 VS^2	SP^2 SF^2		SP^2 SF^2	CD^2 V^3 IT^2 A^3 U^3 CT^3 CS^3 CR^2
D	SP^3 VN^3 SF^3 VS^3	SP^3 VN^3 SF^3 VS^3	SP^3 SF^3		SP^3 SF^3	CD^3 V^3 IT^3 A^3 U^3 CT^3 CS^3 CR^3
E	SP^3 VN^3 SF^3 VS^3	SP^3 VN^3 SF^3 VS^3	SP^3 SF^3		SP^3 SF^3	CD^3 V^3 IT^3 CR^3
F	SP^3 VN^3 SF^3 VS^3	SP^3 VN^3 SF^3 VS^3	SP^3 SF^3		SP^3 SF^3	CD^3 V^3 IT^3 A^3 U^3 CR^3
G						IT^1 CR^1
H	NOT VERIFIABLE					

IT - INVERSE TRANSFORM
CT - COMPARE TWO
CR - CORRELATION
CD - CODING

V - VOTING METHODS
A - ACKNOWLEDGEMENT
U - USER COMPLAINT
SP - SPECTRAL ANALYSIS

SF - SIGNAL FORM ANALYSIS
VN - VALUE CHECKS: NONSEQUENTIAL
VS - VALUE CHECKS: SEQUENTIAL
CS - CROSS POWER SPECTRUM

1. MAY BE APPLIED ONLY TO SET OUTPUT
2. MAY BE APPLIED TO EITHER SET OR ELEMENT OUTPUT
3. MAY BE APPLIED ONLY TO ELEMENT OUTPUT

85647-43

Figure 5.2.2.2-5. Applicability Matrix

comprised of those techniques appearing in the matrix element describing the situation plus the classes of techniques listed as applicable to that redundancy class but independent of signal class.

Another point to be made here is that the explicit statements of applicability set forth in this matrix say nothing whatsoever concerning the efficiency of employment of a given coincidence development technique. Certainly, the use of Spectral Analysis will in some cases represent an "overkill" of the problem. A comparison of verification techniques appears in Appendix A and provides information for the matching of verification requirements with coincidence development capabilities. Again, the matrix given here only presents the candidate verification techniques.

With some thought, it becomes obvious that, if a technique is to be applied to the output of the entire redundant set, that characteristic of the set output which varies with the number of elements in the set should be detectable by the coincidence development technique. Clearly, it would be foolish to use a Spectral Analysis technique on a set output whose spectral content does not vary as the number of elements in the set. Still, this should be consciously observed when interpreting the matrix.

It is reasonable to assume that if one desires to add a symbiotic signal to a stochastic signal, that additional signal will be made deterministic. The entries under the second column of the matrix represent techniques which make use of the deterministic symbiotic signal for verification purposes. Spectral Analysis and Signal Form Analysis techniques might also be applied to the stochastic portion of the signal. If this is the case, restrictions on the stochastic signal, both implied in other columns of the matrix and discussed earlier in this section, should be observed.

It is appropriate at this point to briefly discuss the selection of stationarity as a statistical descriptor for signals. It may be anticipated that all investigations of system signals will be on a time series basis. That is, no ensemble collection of samples will be employed. Then, while it is likely that the principle of ergodicity will be invoked in design and performance prediction calculations, it will not influence the applicability of coincidence development techniques so long as the reference statistic is also a time average.

Assuming that one has properly identified the redundancy class/signal property class coinciding to the situation of interest, has consulted the Applicability Matrix and has compiled therefrom a list of candidate coincidence development techniques, the next step is to examine the signal to be observed and determine if it possesses the desired properties in the desired time frame.

At this point it is necessary to involve the required design confidence in two examinations.

Firstly, it must be determined whether the signal to be observed possesses the properties and characteristics necessary to satisfy design confidence requirements. If these requirements include, for example, information on frequency response, a sinusoidal signal could not establish the desired level of confidence.

Secondly, it must be asked of each candidate technique whether it is basically capable of satisfying the design confidence requirements. Is the comparison of two outputs sufficient to convince one of proper operation? With what degree of agreement between the two? Up to this point the discussion has concentrated on signal properties. How can signal properties be interpreted in terms of the compare-two example above? This is a valid question and points up an important distinction to be made for Output/Output and Output/Input comparison techniques. These techniques inherently compare complete signals and not just selected properties. This does not violate any of the previously developed points. When considering these two techniques one simply enters the Applicability Matrix with "signal property" replaced by "signal".

If the first of the two conditions above is not met, and assuming that design confidence is fixed, the only choice is to change the signal class and/or the properties of the signal used for verification. This implies the consideration of simulative, symbiotic, or idle signals.

If, for a given coincidence development technique, the second condition is not met, that technique must be stricken from the list of candidates. If confidence levels still cannot be met, an alternation in the signal used for verification will be a possibility. This means returning to the Applicability Matrix and shifting to another signal class column in order to make available more candidate techniques.

If and only if both conditions are met, one may proceed with the consideration of the remaining candidates. The remaining factors to be considered are whether the candidates can achieve the desired verification confidence and whether they can comply with imposed constraints such as restrictions on the use of sampling, reliability requirements, and cost ceilings.

The process of the selection of coincidence development techniques is summarized in Figure 5.2.2.2-6. The uppermost block represents a description of the signal for verification. At the start of the process, a tenant signal characterization should appear here. This characterization is carried to the Applicability Matrix where signal characteristics and more design inputs, redundancy class information, dictate a choice of matrix element. A list of candidate techniques, determined from the matrix, is compared against design confidence requirements as are signal characteristics/properties. If inconsistencies result, a return path to the uppermost box is provided. This denotes a change in the signal used for verification. In the lowermost box, techniques surviving previous test are examined for their compatibility with system constraints. Incompatibilities here will also result in a change of the signal used for verification as is denoted by a feedback arrow.

While design inputs have been spoken of here as being fixed, it is unlikely that this will be the case in the real world. It may be anticipated that an active exchange will take place between the design and the design inputs as the requirements of the design and the capabilities of verification are mated through compromise and tradeoff. The main points to be made here are the utility of the matrix and the way in which the process suggests the use of a different signal for verification.

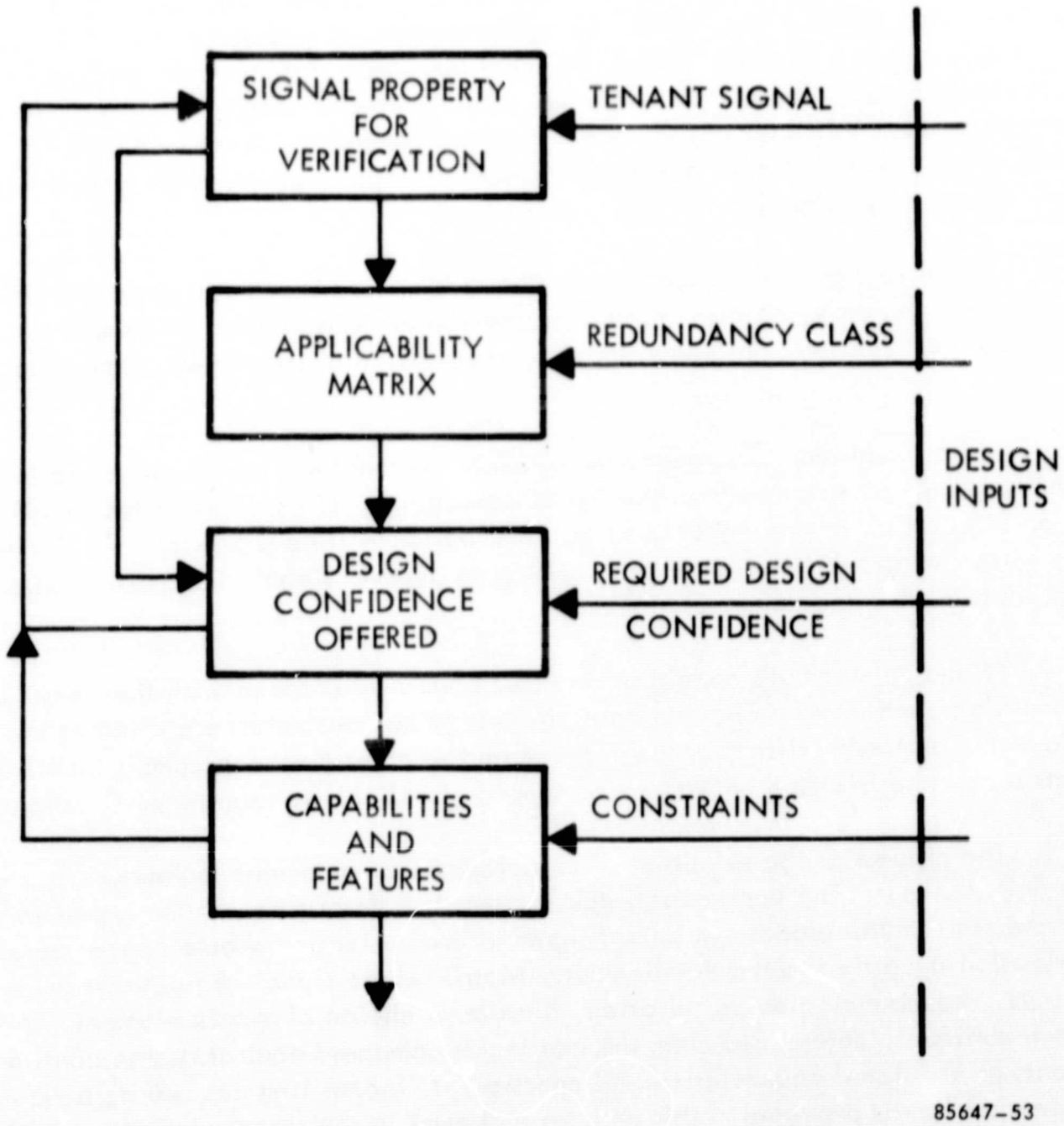


Figure 5.2.2.2-6. Selection Process for Coincidence Development Techniques

It should be borne in mind that combinations of these techniques may be worthy of consideration, and that, where no suitable pairing of signal and technique is possible, the use of different techniques with given signals might be used in a time sequenced arrangement. Both of these solutions would lead to multidimensioned coincidence variables.

Going beyond the statements of applicability which appear in the matrix of Figure 5.2.2.2-5, an investigation of the characteristics and capabilities of the various coincidence development techniques has been carried out. Such items as failure types detectable, ability to discriminate among failure type, sharability, complexity, and amenability to computer implementations have been identified as areas of interest and have been examined with respect to each class of techniques. A discussion of the findings along with summaries of the advantages and disadvantages of each class of techniques appears in Appendix A. The reader is encouraged to make full use of the information presented therein.

From the foregoing development and the discussions of Appendix A, some conclusive statements may be made.

- No coincidence development technique, in itself, negates the possibility of continuous verification. It is the ability of signals to provide the foundation for design confidence that is the basic limitation in this area.
- Under certain circumstances, the transition from conditional status to status may be made knowing only that an admissible input is present.
- All the techniques offer the possibility of implementation on a sampled basis.

5.2.2.3 Parameter Estimation and Status Variables

It has been pointed out that the coincidence variable results from a comparison of two pieces of information. If the simplest form of Compare Two is used, the coincidence variable will be a point-by-point comparison of two element outputs; if Correlation is employed with a pseudorandom input, the variable may be a point-by-point comparison between equipment impulse response and expected impulse response. It is then required to know whether the two pieces of information are sufficiently alike to indicate proper system operation. The big question, then, is, "How much alike is enough alike?". More fundamental is the question of what appropriate measures of similarity may be applied.

Consider the two functions of Figure 5.2.2.3-1. Among other things, these two functions might represent two analog inputs to a Compare Two arrangement. The second curve is a plot of the difference of the two original functions and might represent the coincidence variable. If no parameter estimation function were employed, this would become the status variable and would be considered to be indicative of conditional status.

The third curve is the square of the difference of the two functions. Obviously, the degree of resolution offered by observing the squared difference is much greater than that

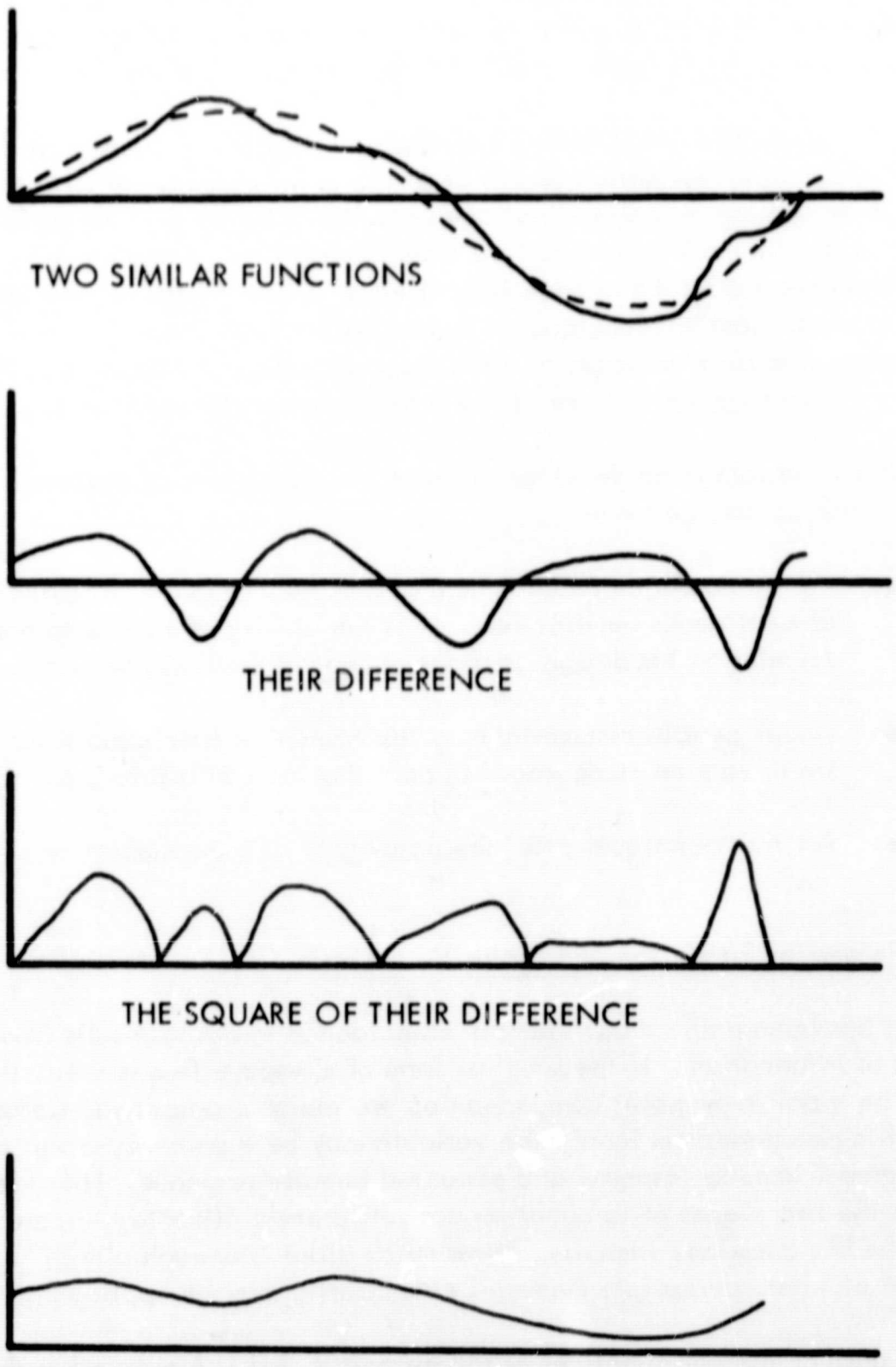


Figure 5.2.2.3-1. Illustration of Parameter Estimation

obtainable by simply observing the difference and information concerning which function is of greater magnitude has been lost.

The fourth curve is the mean of the squared difference. (Some liberties have been taken in the construction of the figure, but the idea should be clear.) An investigation of this curve will reveal that a difference of short duration tends to be masked and that, again, the sign of the difference has been lost.

Now, if one were asked to express, through these curves, the difference between the original functions, the manner of expression would be different for each curve and it might be expected that an "acceptable" degree of similarity would mean different things depending on which method of expression were chosen.

This is the dilemma that exists within the functional area called parameter estimation. What are the proper methods for expressing a status variable? Two methods, squaring, and mean squaring have been exemplified here. There are scores of other possibilities; averaging, weighted averaging, ratio or percentage expression, differentiation, and coherence functions to name a few.

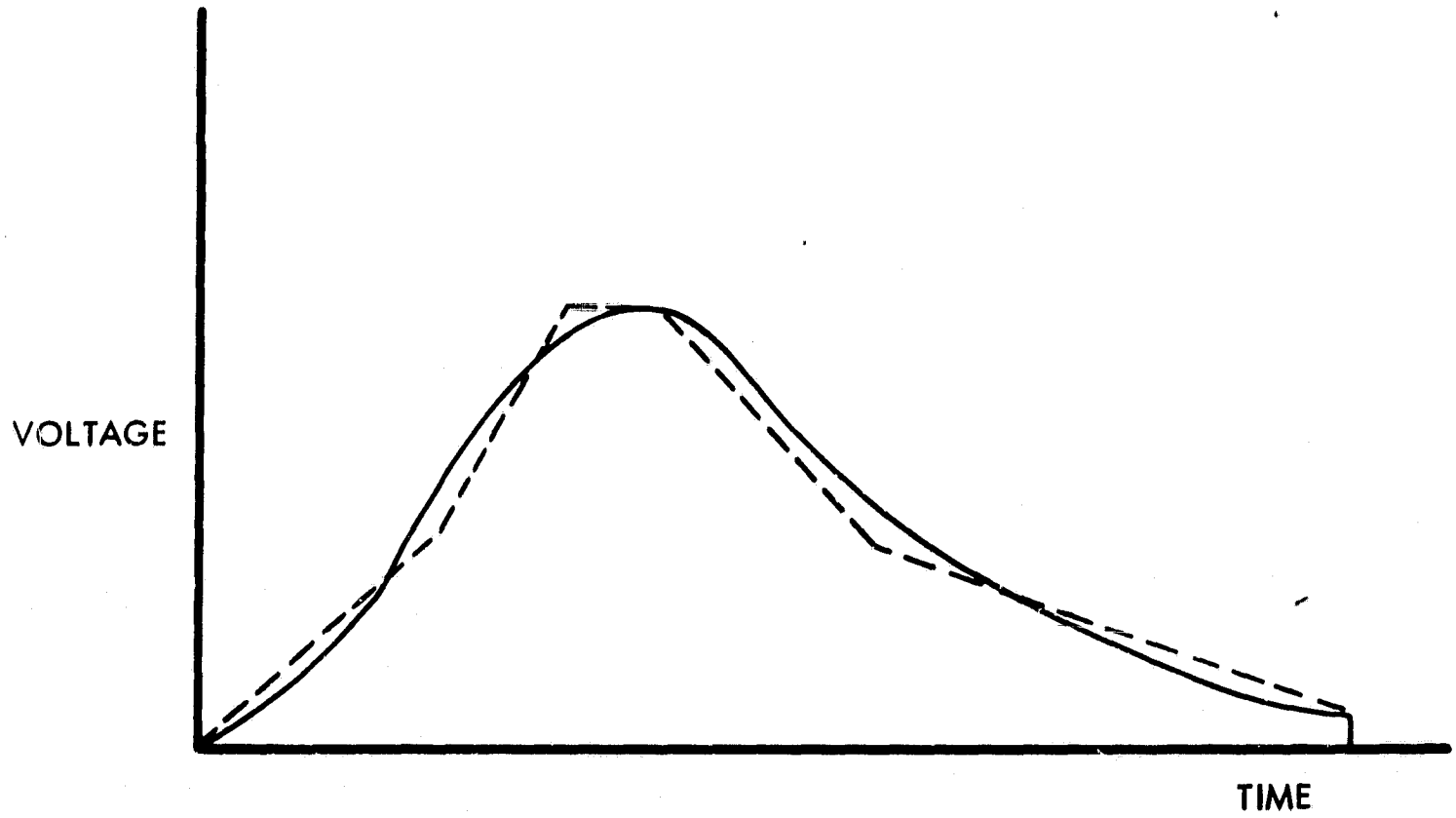
There are two primary and important considerations here. Firstly, will a given parameter estimation technique destroy sensitivity to information that is of interest and available in the coincidence variable? If it is desired that the status variable reflect information concerning the existence of excessive noise in element output, the use of uniform averaging in the parameter estimation function may be a very poor choice. The choice of the parameter estimation technique is heavily dependent on the functional description of the IBV.

Consider the case of Correlation which produces system impulse response. An expected impulse response might be stored in a piecewise linear diode circuit so that the two functions would appear as shown in Figure 5.2.2.3-2. What the mean-squared difference of these functions implies about gain or signal distortion could be a difficult matter to determine.

The second consideration is that the chosen technique of parameter estimation must be capable of achieving the requirements of design confidence. If an integration method of parameter estimation is used in a noisy situation, the likelihood of Type I errors will be diminished. At the same time, the ability to provide assurance that functions remain within a narrow tolerance is also decreased. It is easily possible that the parameter estimation function could render impotent the coincidence development function.

An additional complication arises when the computation of a statistical variable over a limited-size sample set is involved. Then the confidence level set by the sample size must also be taken into account when matching a parameter estimation scheme to design confidence requirements.

It may be seen that the parameter estimation function is of great importance in the process of verification. It is able to dictate design confidence and limit the comprehensiveness of the coincidence detection technique.



85647-51

Figure 5.2.2.3-2. Derived and Stored Impulse Responses

It would be extremely helpful if one could make general statements about the different kinds and classes of parameter estimation techniques. To do so, however, would require extended investigation into the various techniques, the identification of common features among the techniques, and grouping according to these features--an excercise very similar to that carried out here on the coincidence development techniques. For the present, such an orderly approach to the problem, as it applies to redundancy verification, does not exist and the designer will be forced to examine the different options as they apply to each individual occurrence of redundancy.

5.2.2.4 Mapping into Conditional Status

With the status variable having been generated, the third operation of simple set redundancy verification is the mapping to conditional status. The concept here is that there will be, for every value of the status variable, a coinciding statement of conditional status. The existence of a unique inverse will not be the usual case. That is, given a statement of conditional status, one will not be able to reconstruct the value of the status variable which led to the statement.

The values of a status variable will not, in practice, be restricted to expression as a simple voltage. In fact, the status variable will in many cases be multidimensional, perhaps derived from several combinations of coincidence development and parameter estimation functions. An example would be a two dimensional status variable one of whose components is derived from the rms properties of the signal under observation, the other being derived from the signal mean. Then different combinations of these components of the status variable would be interpreted as indicating different conditional status.

Where multidimensional status variables are involved, the designer will be responsible for setting up a sometimes complicated mapping function. In general, the mapping can be viewed in terms of logical operations on the components of the status variable. Looking to the example of the two-dimensional variable above, it might be possible to construct a truth table such as that shown in Figure 5.2.2.4.

The implementations of the mapping function will generally be straightforward, comprised of one or more of threshold decisions, logic gates and computer-implemented logical decisions.

5.2.2.5 Sample Coincidence Development Implementations

Section 5.2.2.4 above completes the description of the set problem. It is probably not necessary to comment that a great deal of material has been covered in previous sections relating to the set problem: with particular emphasis on Coincidence Development. In this light, it should be helpful to view some hardware implementations of these techniques. This section illustrates typical methods of Coincidence Development implementation. Notes germane to each method, including possible applications to KSC equipment, are included with each

← STATUS VARIABLE →		
MEAN - DERIVED COMPONENT	RMS - DERIVED COMPONENT	CONDITIONAL STATUS
HIGH	HIGH	CAUTION
HIGH	LOW	STOP
LOW	HIGH	GO
LOW	LOW	STOP

85647-54

Figure 5.2.2.4. Status Mapping Truth Table

method. The material has been organized into the three methods of addressing output signals, viz., output/output comparisons, output/reference comparisons and output/input comparisons.

5.2.2.5.1 Output/Output Comparisons

Compare Two, Voting and Crosspower Spectral Analysis all forms of output to output comparisons, are detailed in this subsection.

Compare Two (Digital)

Refer to Figure 5.2.2.5.1-1.

The Compare Two (Digital), sometimes referred to as a coincidence detector, enables two parallel digital signals, to be compared at the same epoch of time, thus a bit by bit comparison is quite feasible.

Composed of two (2) AND gates, two (2) inverters and an OR gate, an output indicating both inputs are alike, regardless of whether both are zero's or one's will be received at the OR gate output.

Compare Two (Analog)

Figure 5.2.2.5.1-2 shows a basic differential amplifier of two transistors with a common emitter resistor.

The output Vo is a function of transistor gains (K) and the difference of $V_1 - V_2$

$$Vo = K (V_1 - V_2)$$

The common mode effect in this circuit grants a 1% (Max. error) to this circuit.

The common mode effect may be minimized by utilizing the composite amplifier shown in Figure 5.2.5.1.1-2. In this configuration, the common mode voltage has a unity gain, but the differential voltage has a gain of (1+m+n).

Voting

Voting techniques can include any odd number of parallel channels greater than one. In this discussion the parameter of three will be delved into and the general configuration will be referred to as Triple Modular Redundancy (TMR).

A typical application of voting is shown in Figure 5.2.2.5.1-3. The following discussion shall be primarily focused on the redundancy Voting--circuits, though the principles can also apply to the signal selection voting circuits.

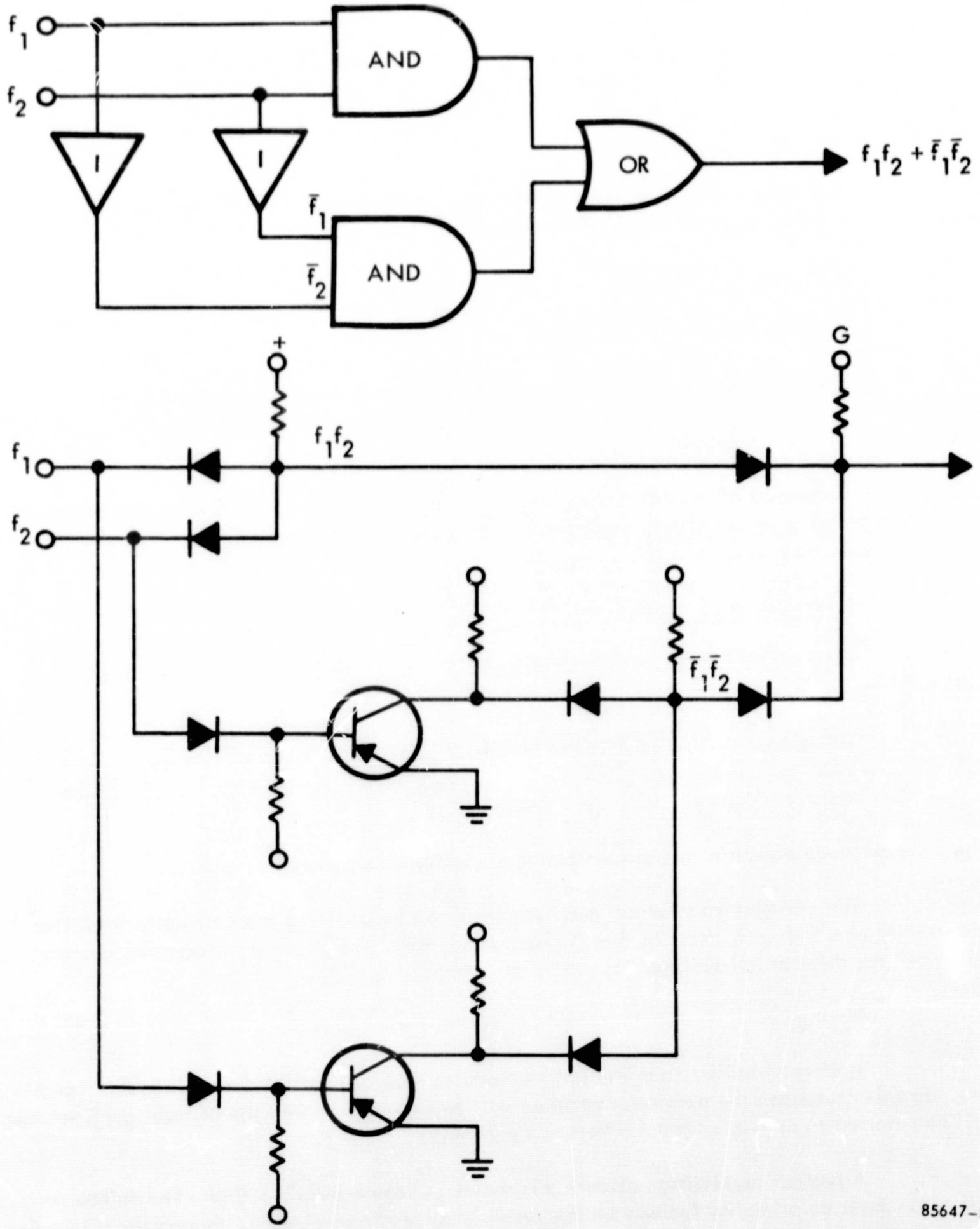
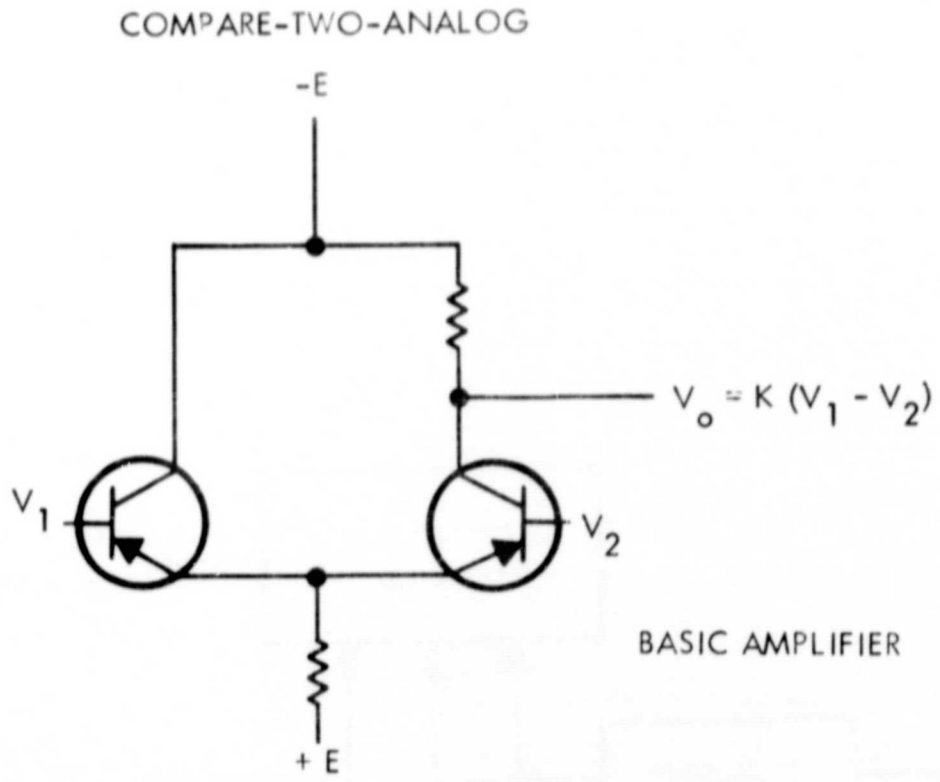
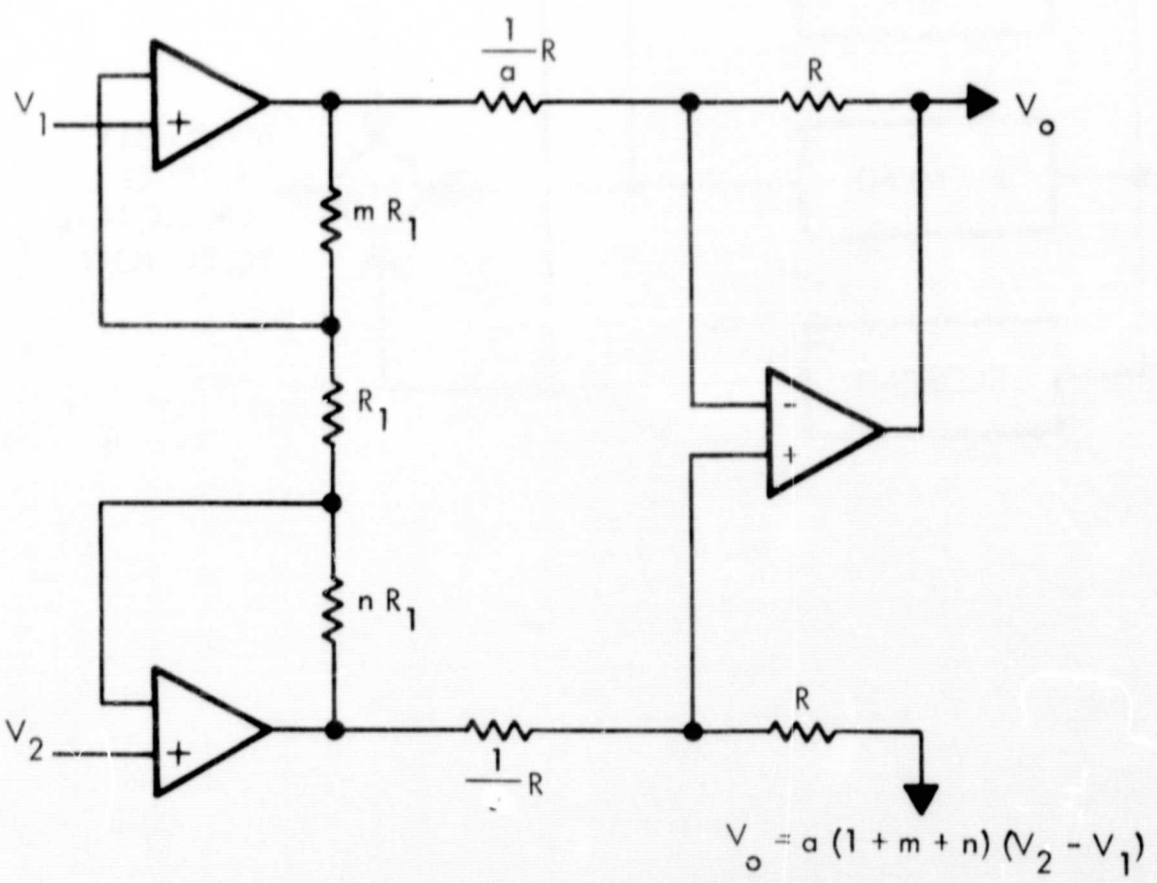


Figure 5.2.2.5.1-1. Compare Two - Digital





85647-57

Figure 5.2.2.5.1-2. Compare Two - Analog

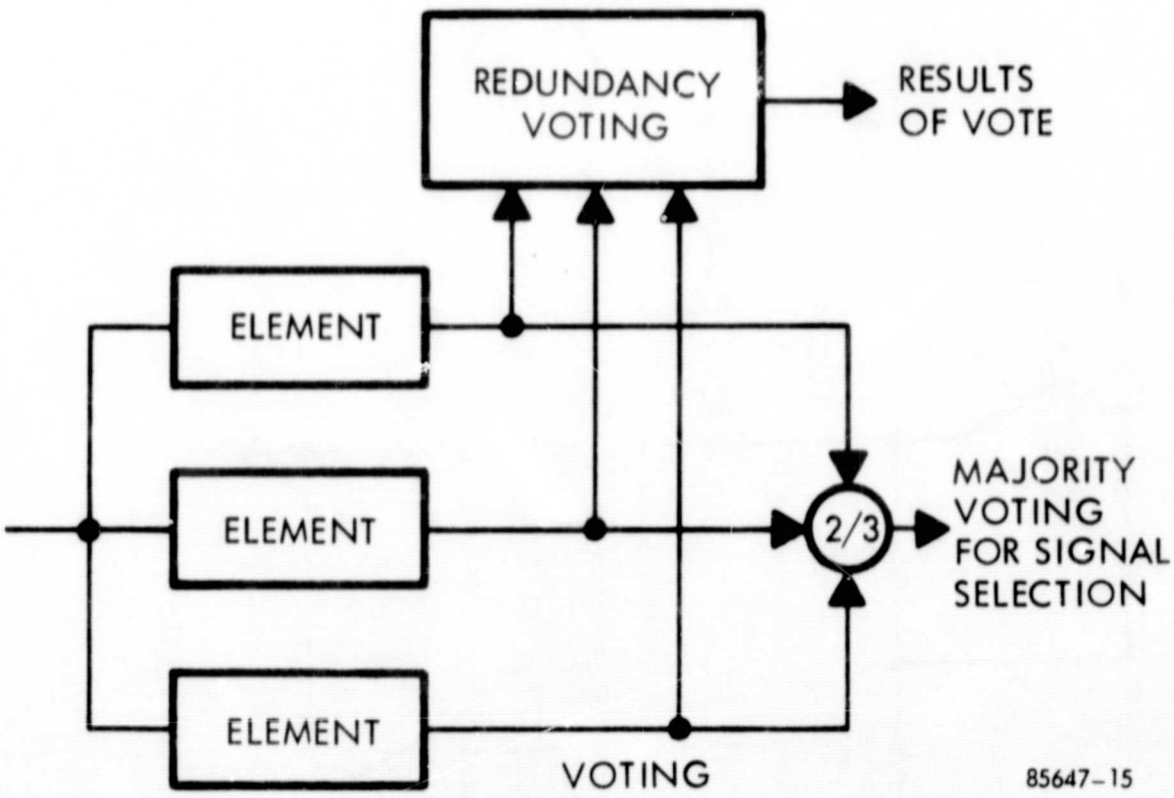


Figure 5.2.2.5.1-3. Voting

The redundancy Voting techniques consist of a logical polling of the outputs of each element: The results of the vote are utilized in determining the status variable.

There are two types of voters, threshold detectors and logic voting.

The threshold sensing devices perform a switching function when either a specified current or voltage level is exceeded. Refer to Figure 5.2.2.5.1-4.

The threshold circuits operate basically as a summing amplifier. Two of the three channels on the input must be up to provide sufficient voltage to overcome the back-biasing from the -3V supply on the base of the transistor Q_1. Q_1 will turn on, thus providing a negative going output, with Q_2 inverting the signal for a positive going signal on the output. Thus, a Q_2 positive output is a function of the input signal on the Q_1 base which is a function of 2 or 3 inputs being up. If two channels fail in the compensating manner, one open and the other providing a high current output to the summing mode at Q_1 base, the threshold detector would be ineffective and would provide a distinct Type II error.

Disagreement Detectors

Refer to Figure 5.2.2.5.1-5. Disagreement detectors may be used to define the presence or absence of a disagreement between the three elements.

In the disagreement detector the absence of a channel will alter the base emitter biasing of Q_1 turning on Q_1. The negative going output of Q_1 is inverted by Q_2 to provide a positive signal for a disagreement indicator.

Further logic and implementation would be necessary to indicate status of each specific element.

If desired, switchable voters incorporating Disagreement Detectors and Error Correctors may be employed to provide the voted output after detecting one element is in disagreement with the remaining two elements.

The switchable voters are composed of Nand and AND gates and can be utilized in determining the status of individual elements. A typical switchable voter is shown in Figure 5.2.2.5.1-6.

5.2.2.5.2 Output to Reference Comparisons

This subsection details various output to reference comparisons, consisting of Value Checks, Sequential and Nonsequential, Coding, Signal Form Analysis, Spectral Analysis and Acknowledgment.

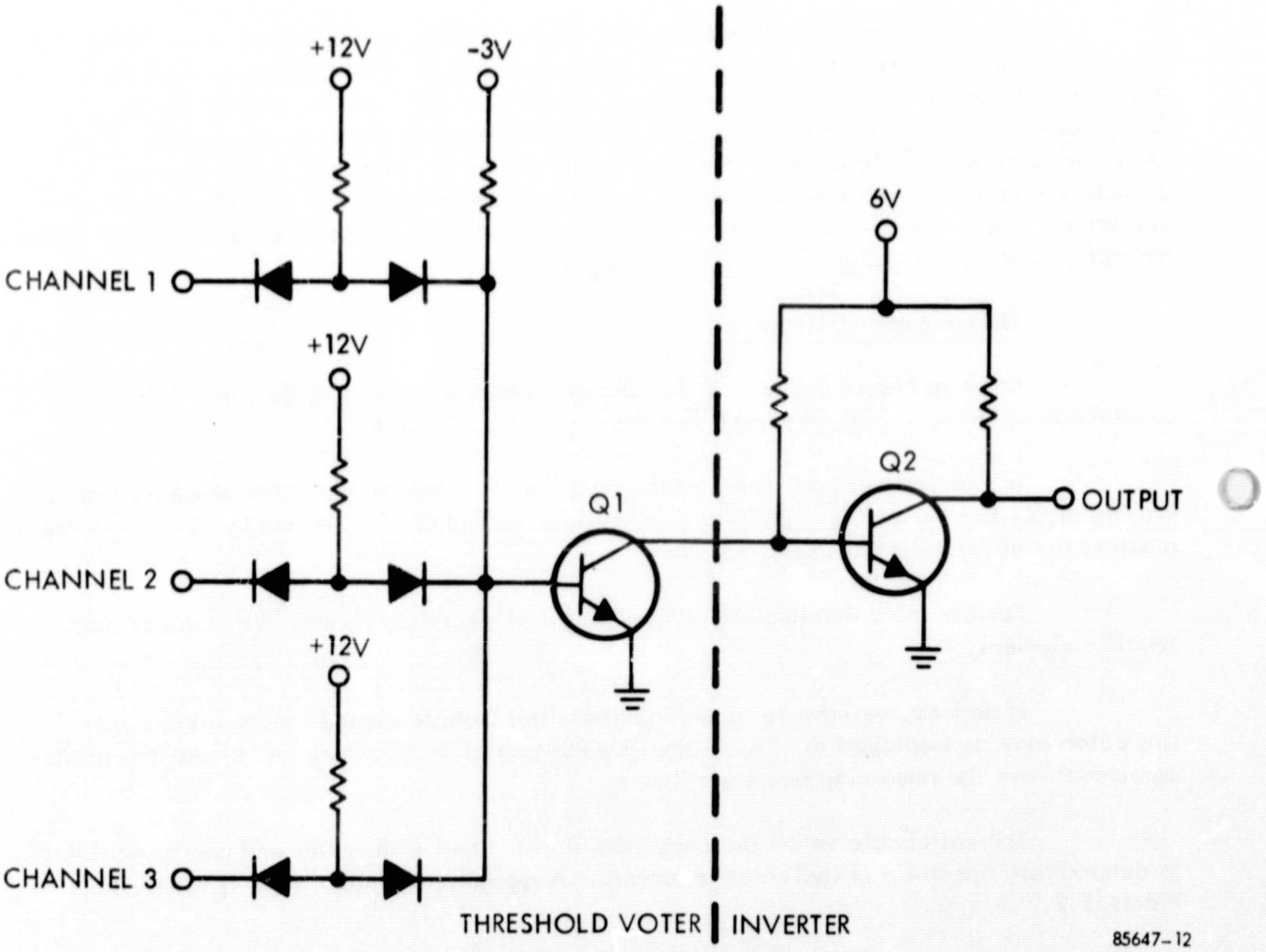


Figure 5.2.2.5.1-4. Threshold Voter, Schematic Diagram

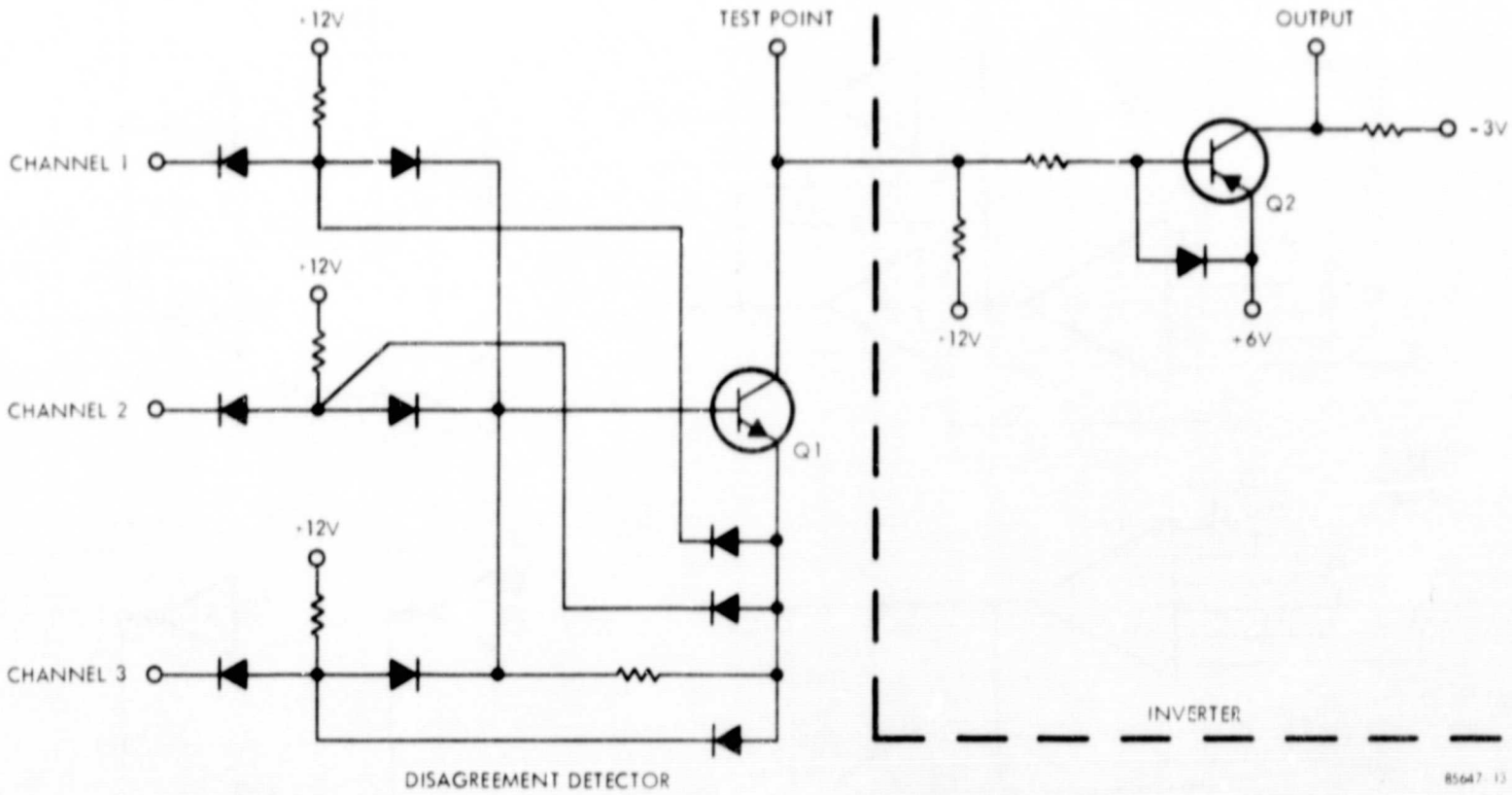


Figure 5.2.2.5.1-5. Disagreement Detector Circuit

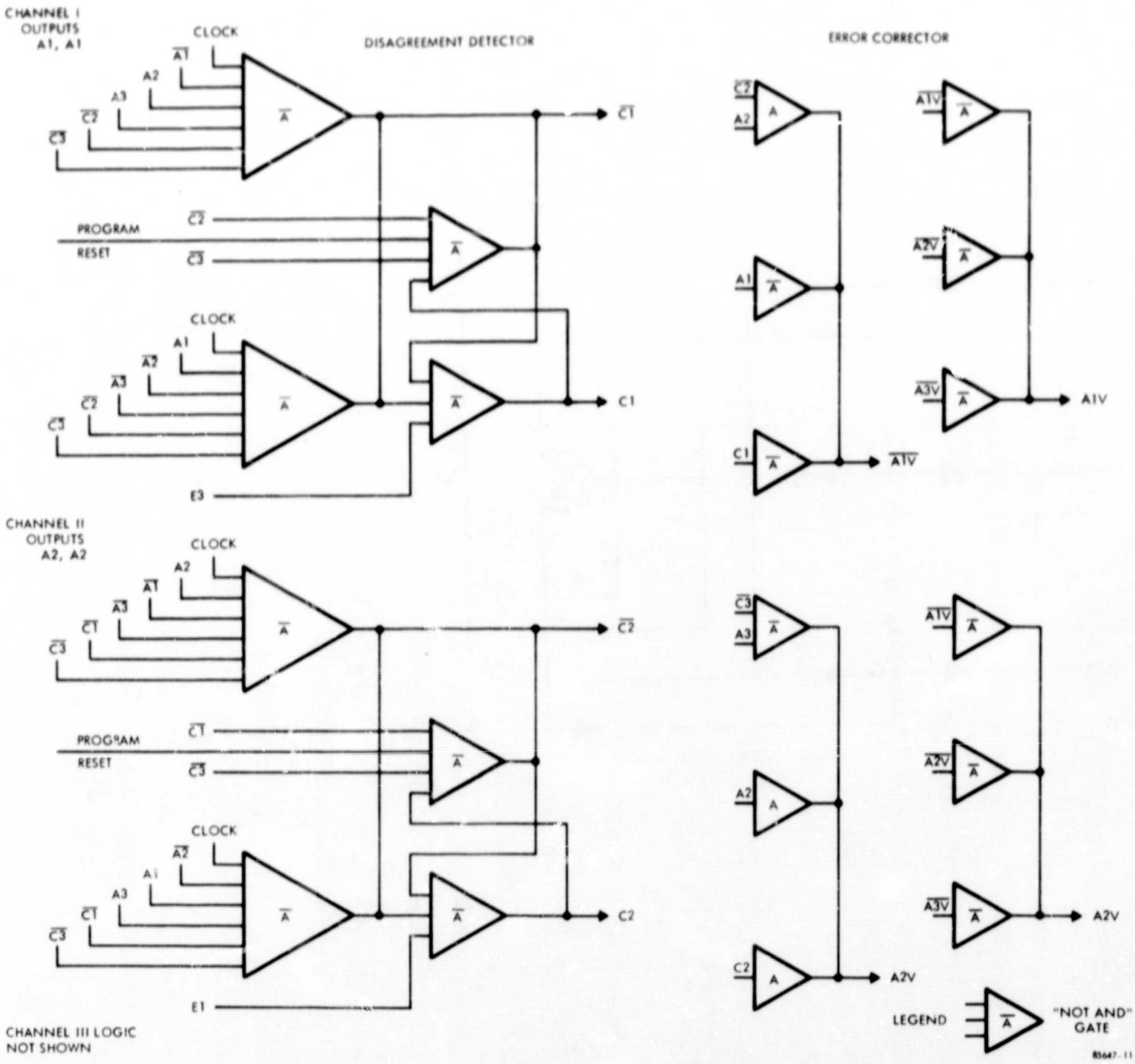


Figure 5.2.2.5.1-6. Switchable Voter, Schematic

Value Check Sequential

In Value Check Sequential the signal values as well as the time order of occurrence both present information regarding status verification. Since this is a monitor method, the values expected would be known and the reference values could be set correspondingly.

Two sequential implementations will be detailed. One will be with direct computer entry with the sequential evaluation performed internally.

In this method, the assumption of a previously stored algorithm or at minimum, a set of threshold values correlated with the sync signal for reference is inherent. Digital inputs are considered, though if signals are analog, A to D conversions could be implemented externally. Refer to Figure 5.2.2.5.2-1.

A second method of implementation consists of an array of differential amplifiers, each fed by analog gates triggered by the sync signal. Each analog gate triggers in series, thus Diff. Amp. 1 will receive the first value; Diff. Amp. 2, second value.

Each Diff. Amp. will receive a reference value corresponding to the Amp. sequence. The status variable of each Diff. Amp. could then be assessed by the Central Processor. Refer to Figure 5.2.2.5.2-2.

Method One is adaptable to both analog and digital input signals while Method Two is adapted to analog inputs solely. Both methods are predicated upon a sequential order of signals.

Value Check Nonsequential

Refer to Figure 5.2.2.5.2-3. This technique is utilized in comparing a signal input with a stored, stable reference. The stored stable reference implies the expected value is known, and this is substantiated by the matrix of Figure 5.2.2.2-5 which mandates a deterministic signal.

The sample and hold circuits are applied to the input signal to alleviate any problems that may be provided by a rather short time duration of e_{in}.

The enable signal and the analog gate are included to prevent the status variable from approaching e_{ref} (the reference voltage) in the absence of e_{in}.

Coding

Parity Checks

In this specialized case of coding, the characteristics and composition of the digital word are evaluated in a rather mild overall error detecting scheme.

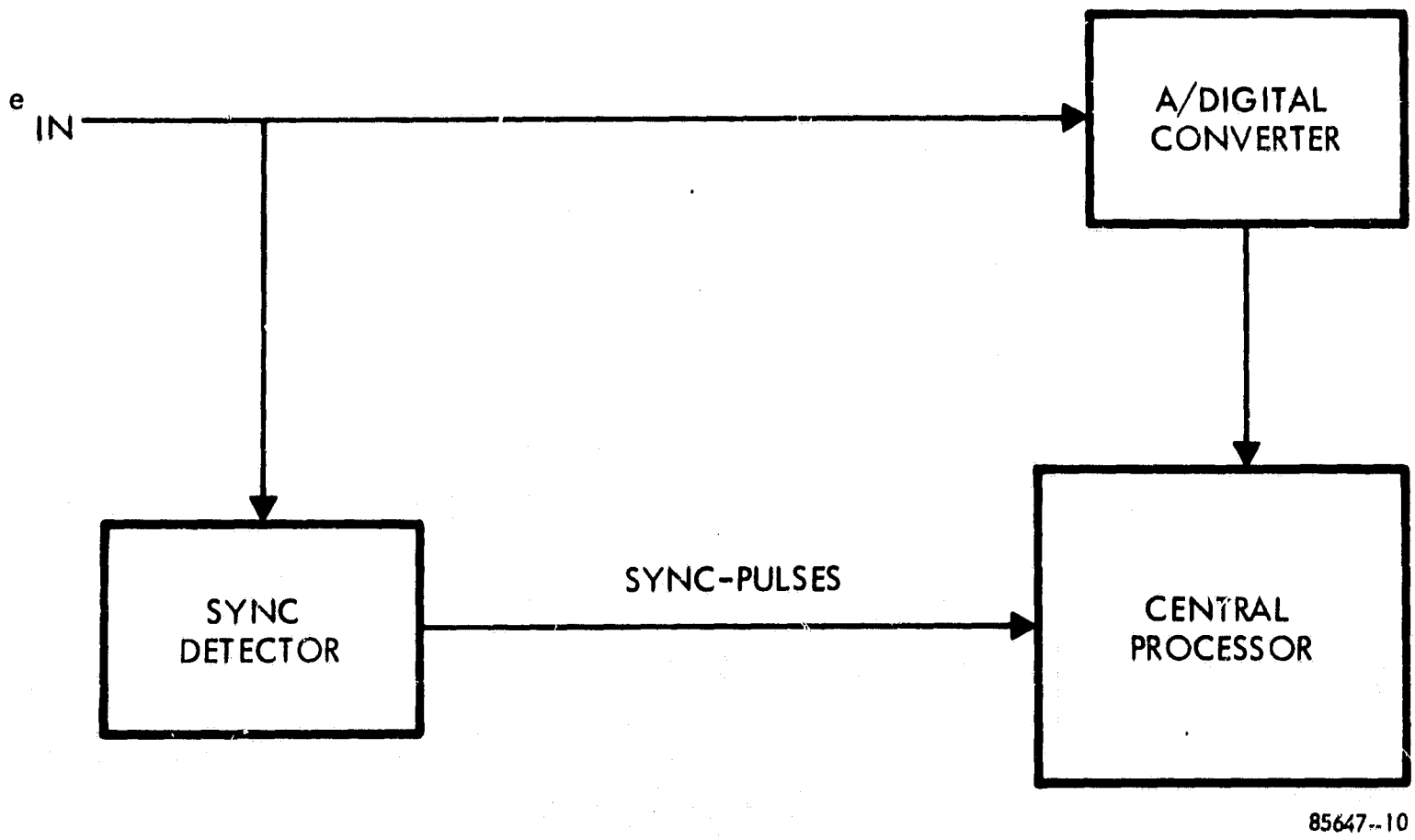


Figure 5.2.2.5.2-1. Valve Check Sequential

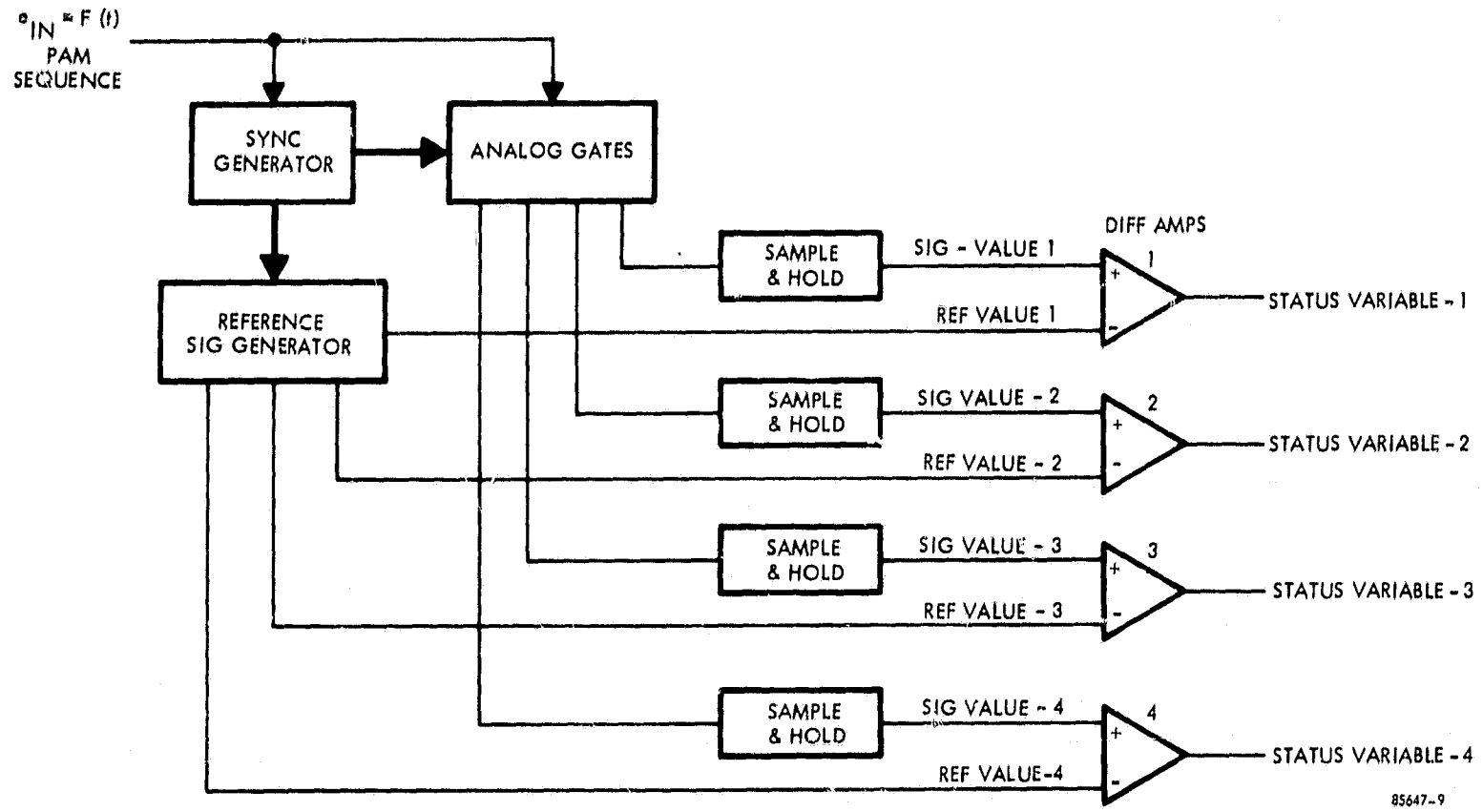


Figure 5.2.2.5.2-2. Valve Check Sequential

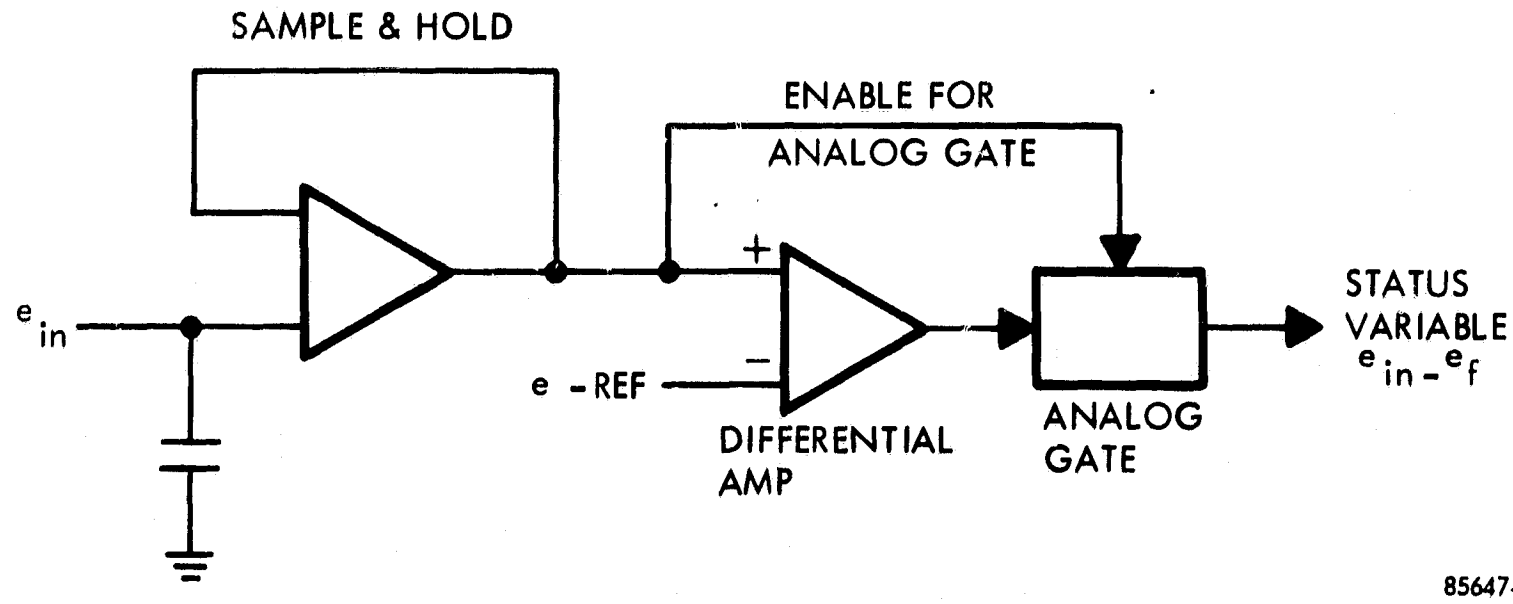


Figure 5.2.2.5.2-3. Valve Checks Nonsequential

The general operation follows. (Please refer to Figure 5.2.2.5.2-4.) The input digital data is directed to a serial shift register, until the digital word length is completed. The L.S.B. (Least significant bit) is previously established, as either a one or a zero, depending upon whether even or odd parity is chosen and the number of ones and zeros in the digital word. For even parity, when the total of ones in the word is odd, then the parity bit is a one. For odd parity when the total of ones is even, the parity bit is a one.

The general operation consists of picking out the transmitted parity bit and routing it to the coincidence detector. Concurrently, the parity generator through an iterative process and the NAND gates (Figure 5.2.2.5.2-5) extracts the actual parity of the digital word in the storage register. The parity generated from this process and the parity transmitted should agree, and thus, both inputs to the coincidence detector should be present, enabling the data storage register output to be shifted out. The failure to achieve coincidence of the transmitted parity bit and the locally generated parity bit will inhibit data storage output and be counted as bad message.

In this method the possibility of two compensating data errors creating a failure condition which goes unnoticed is quite strong as the parity bit and the locally generated parity bit will agree, yet there exist two errors in the data word. It is for this reason that the term mild error detecting scheme is noted above.

The setup in Figure 5.2.2.5.2-6 is designed to check a transmitter-receiver data link. Two identical pseudorandom sequence generators are used. Each generator produces a (2^n-1)-bit sequence of all permutations of n bits, except the all-zero permutation. One generator feeds a transmitter. The received bits are used to synchronize the second generator, so that the received bit sequences should be identical to those of the second generator. The receiver output is compared directly with the sequence generator output, and the error counter stores the number of bad comparisons. This error count is compared with the acceptable maximum to evaluate the system status.

The use of the bit synchronizer allows the transmitter and receiver to be separated, since separate sequence generators may be employed. Thus, the data link may be checked in its normal locations.

The PRN Gen. operates as follows. (Refer to Figure 5.2.2.5.2-7.)

The modulo-2 addition of the shift register output stage (FF_n) and one of the other stages (FF_2) is used to drive the shift register input causing the output to be a sequence of (2^n-1) bits consisting of all permutations of n bits except all zeros.

Conditions

1. PRN Seg. Generators must be synchronized for meaningful operations.

2. Bit Rate of Gen. must be within range of transmission medium.

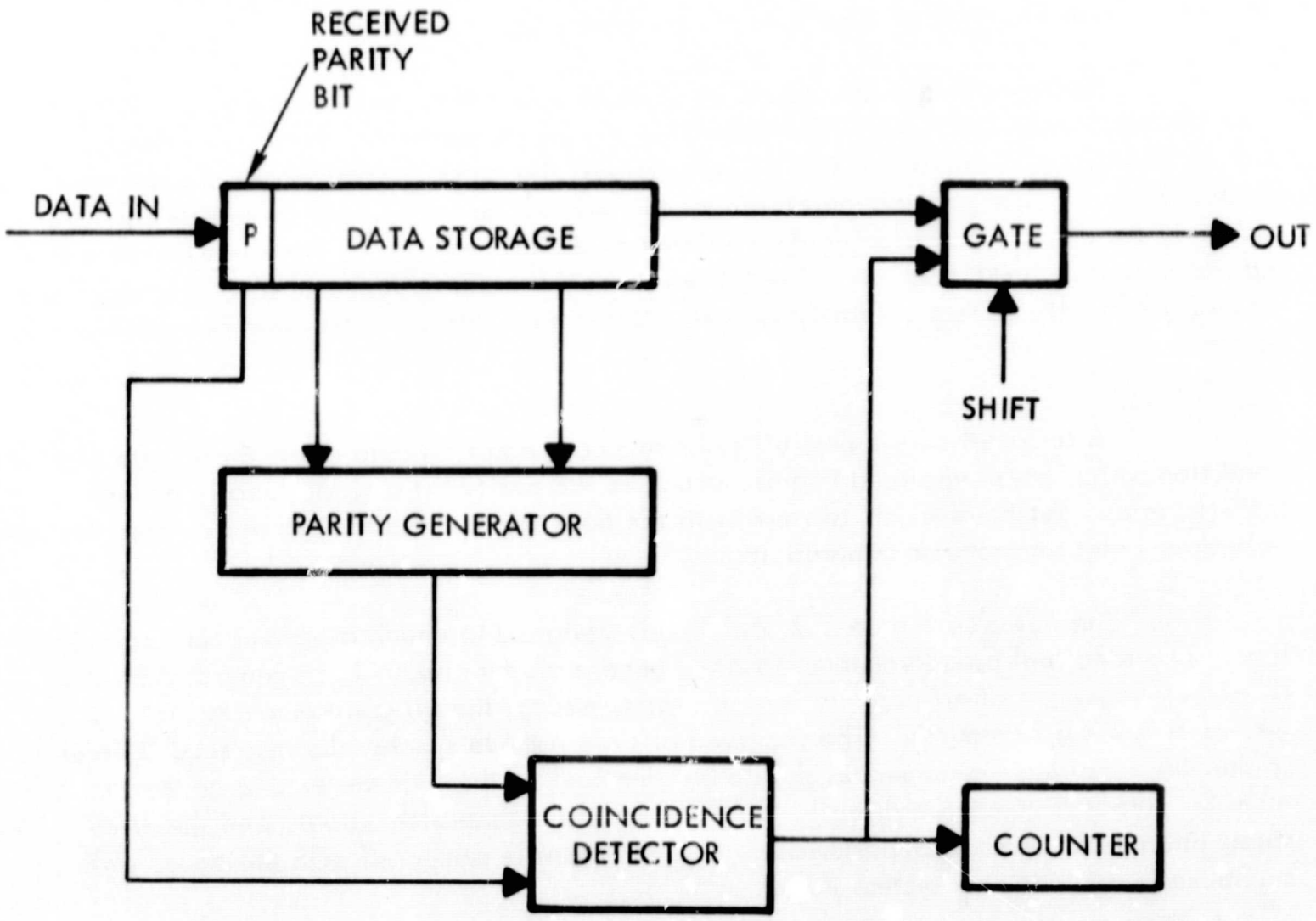
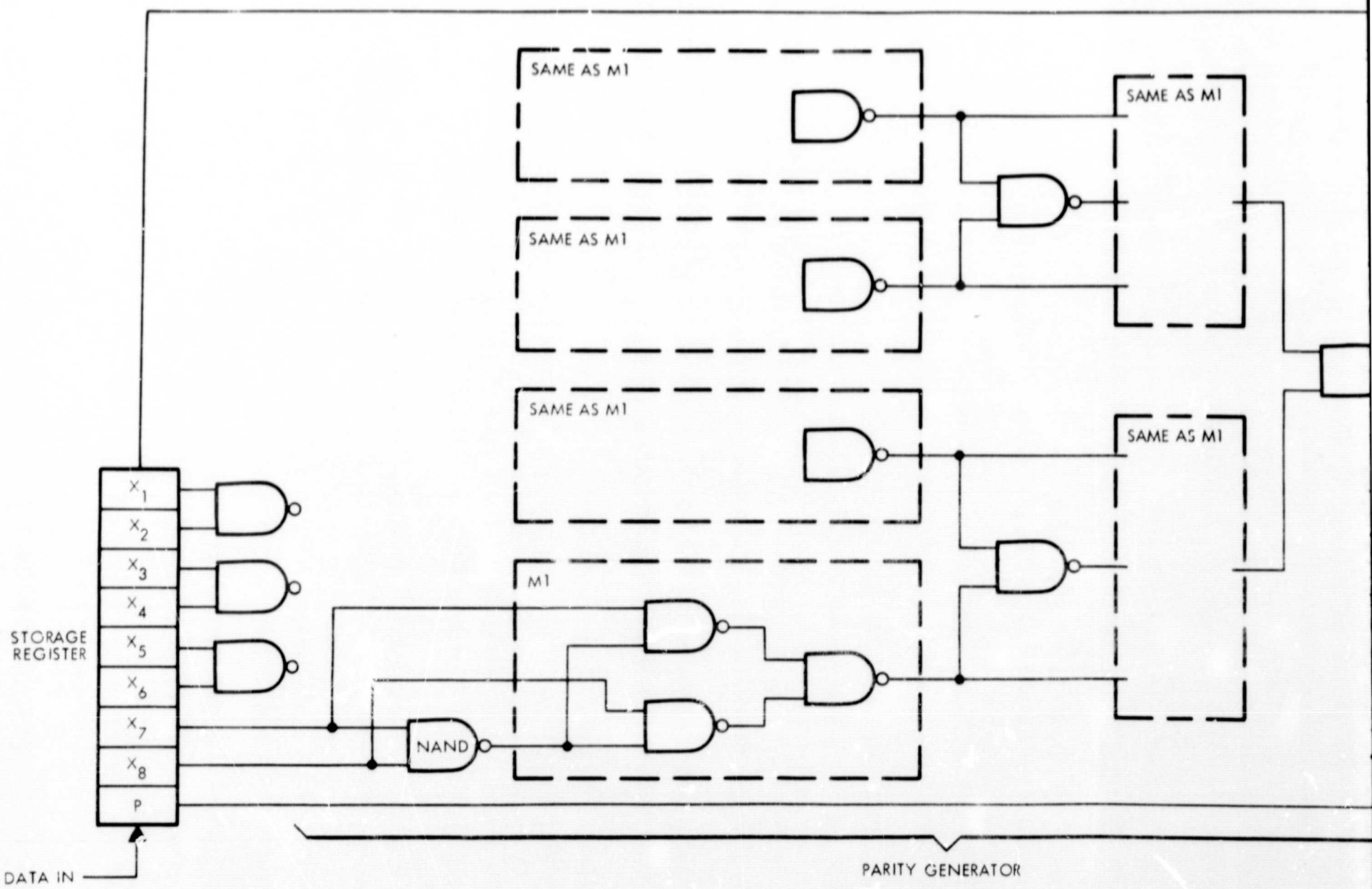


Figure 5.2.2.5.2-4. Coding Parity Checks



FOLDOUT FRAME 7

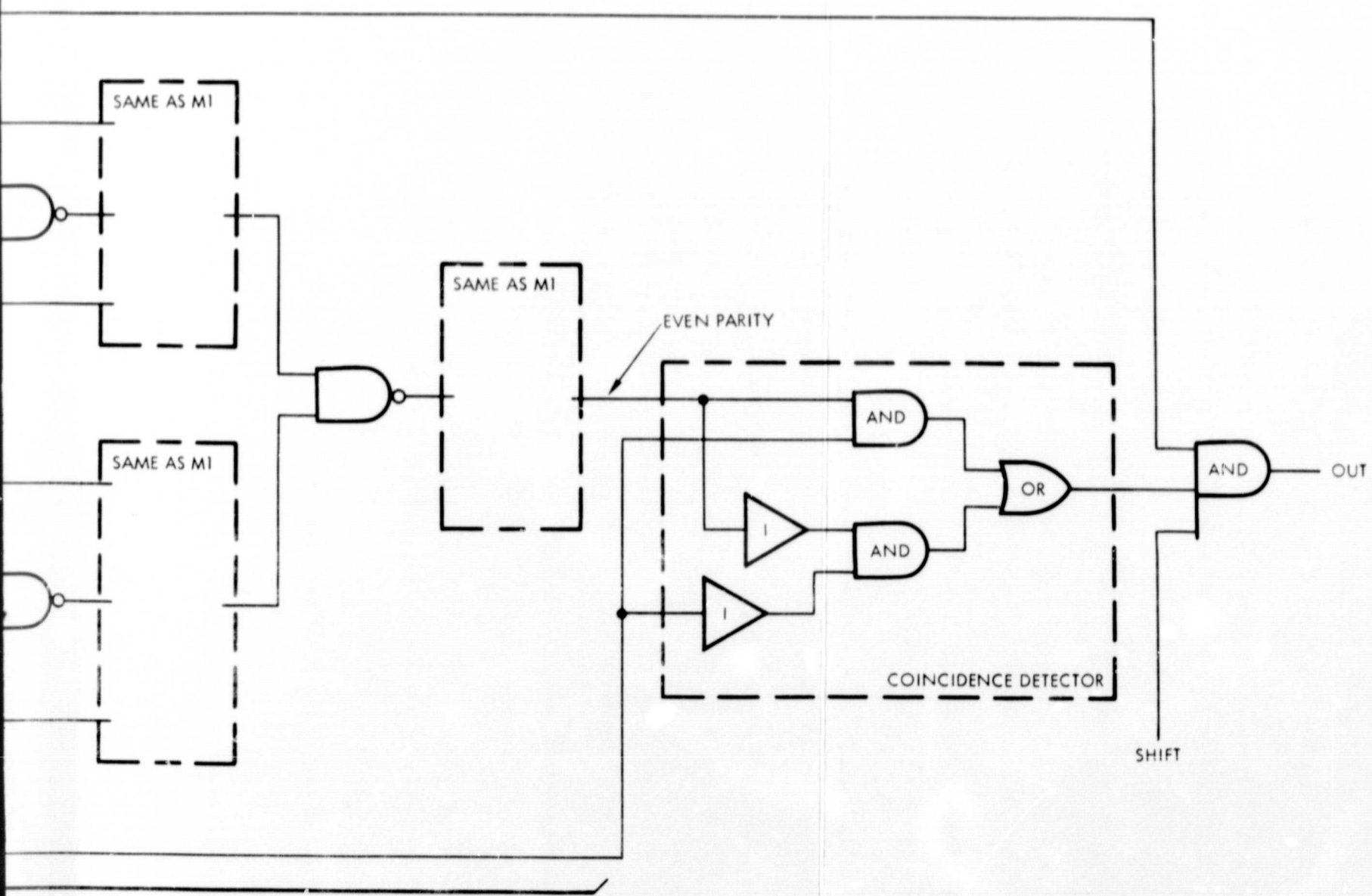


Figure 5.2.2.5.2-5. 1-Bit Parity Check System

FOLDOUT FRAME 2

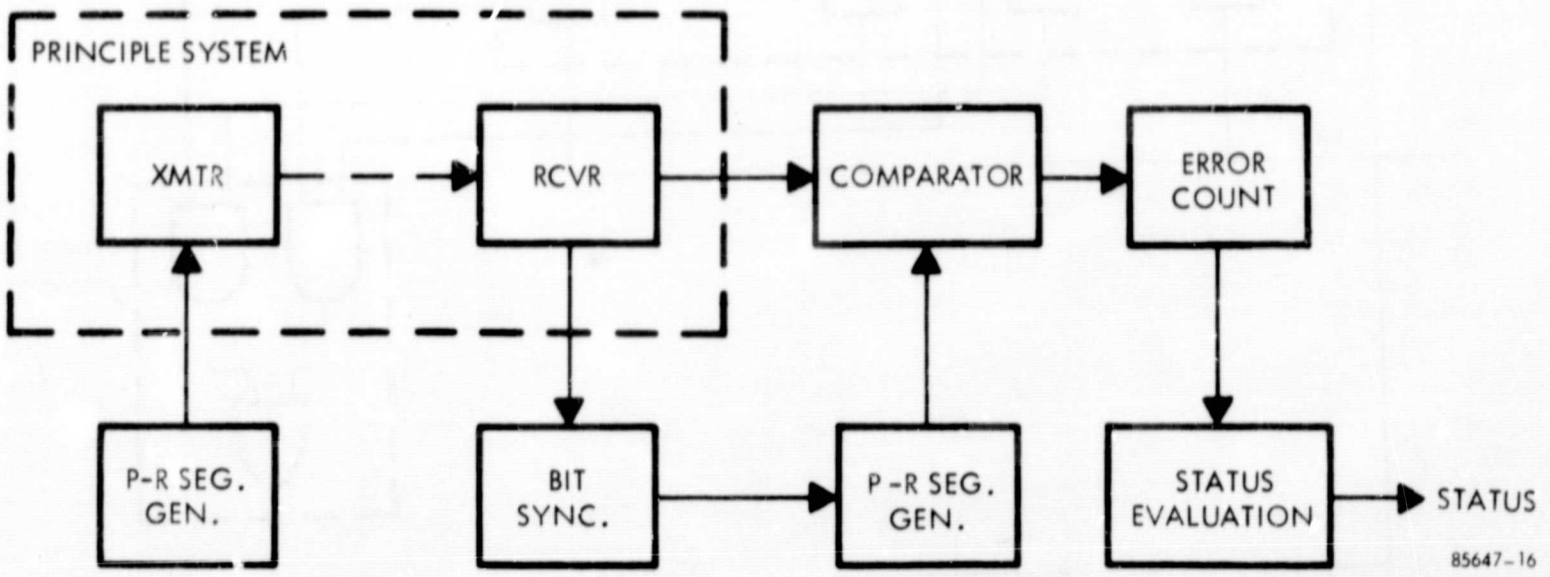


Figure 5.2.2.5.2-6. Coding

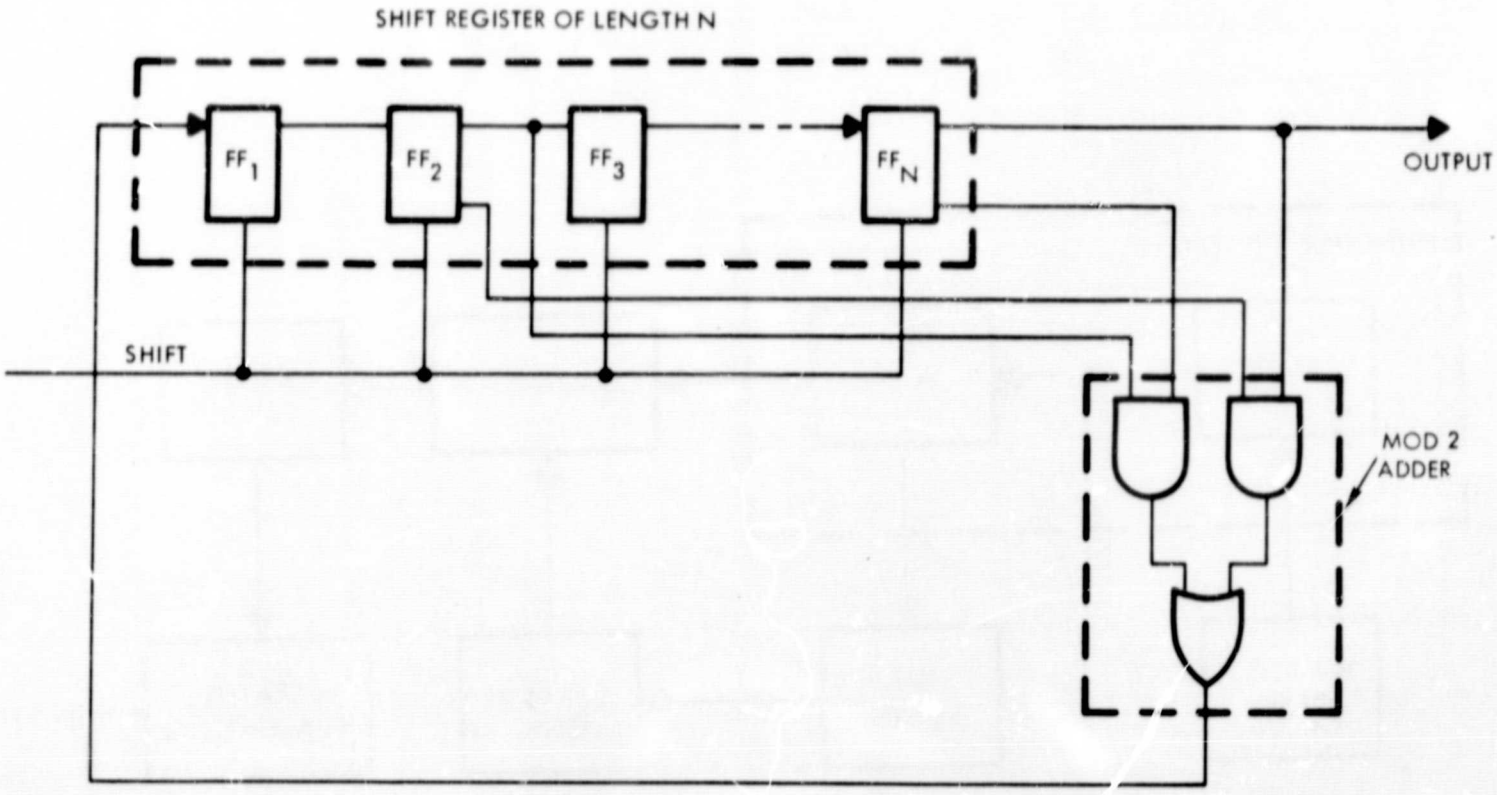


Figure 5.2.2.5.2-7. Pseudorandom Sequence Generator

Applications

1. A2A wideband lines on ACE UL and DL Lines

2. Verification of communications between LUT and Firing Room 110A Launch Computers

3. Verification of Redundancy in PCM/DDAS - 600 KC coaxial cables

All above suggested applications must be performed off-line on a noninterference basis.

Signal Form Analysis

This technique compares the value of some parameter of the input signal to an expected value of that parameter, such as peak, rms or mean value. No time information is conveyed in this verification technique. Figure 5.2.2.5.2-8 shows the block diagram of a sample implementation of the Signal Form Analysis technique. The measurement technique shown may be used on an analog signal (AC or DC) or on a serial digital data train as long as the "ON" signals to the control switches (SCR's) are properly synchronized. The control switches shown just determine which characteristic of the signals (input as well as reference) are to be used for comparison. The "scaler" is a voltage divider which provides an output which is the rms value of the output if sinusoidal signals are assumed. If the rms value of other than a sinusoid is required, the scaler would be replaced by true rms detection device (heating value detector). The arbitrary function generator is a device which generates any waveform by combining individual segments of straight lines. The slope, dc offset, and time length of each segment are variable over an extremely large range. For specialized applications the function generator could be supplanted by a direct reference, such as 6V rms, and this configuration will reduce to 3 basic items, Reference, Holding Circuit and Differential Comparator.

The Mean Machine, Reference Figure 5.2.2.5.2-9, accepts an analog signal, integrates the signal over a unit interval of time, producing an output voltage equal to the mean of the input voltage. This value is then subtracted with a reference voltage, and the difference is compared in a threshold detector. If the difference exceeds the allowed tolerance, the detector will output a no-go status.

The Mean Machine II, Reference Figure 5.2.2.5.2-10, operates in the same manner as the I version, except the resulting mean is processed digitally.

Integrator and Interval Timer, Reference Figure 5.2.2.5.2-11. The flip-flop holds the relay closed until a trigger pulse (indicating the beginning of the sampling interval) is received. The relay is then energized, opening the circuit, and allowing the integration to begin. The next trigger pulse releases the relay, which discharges the capacitor.

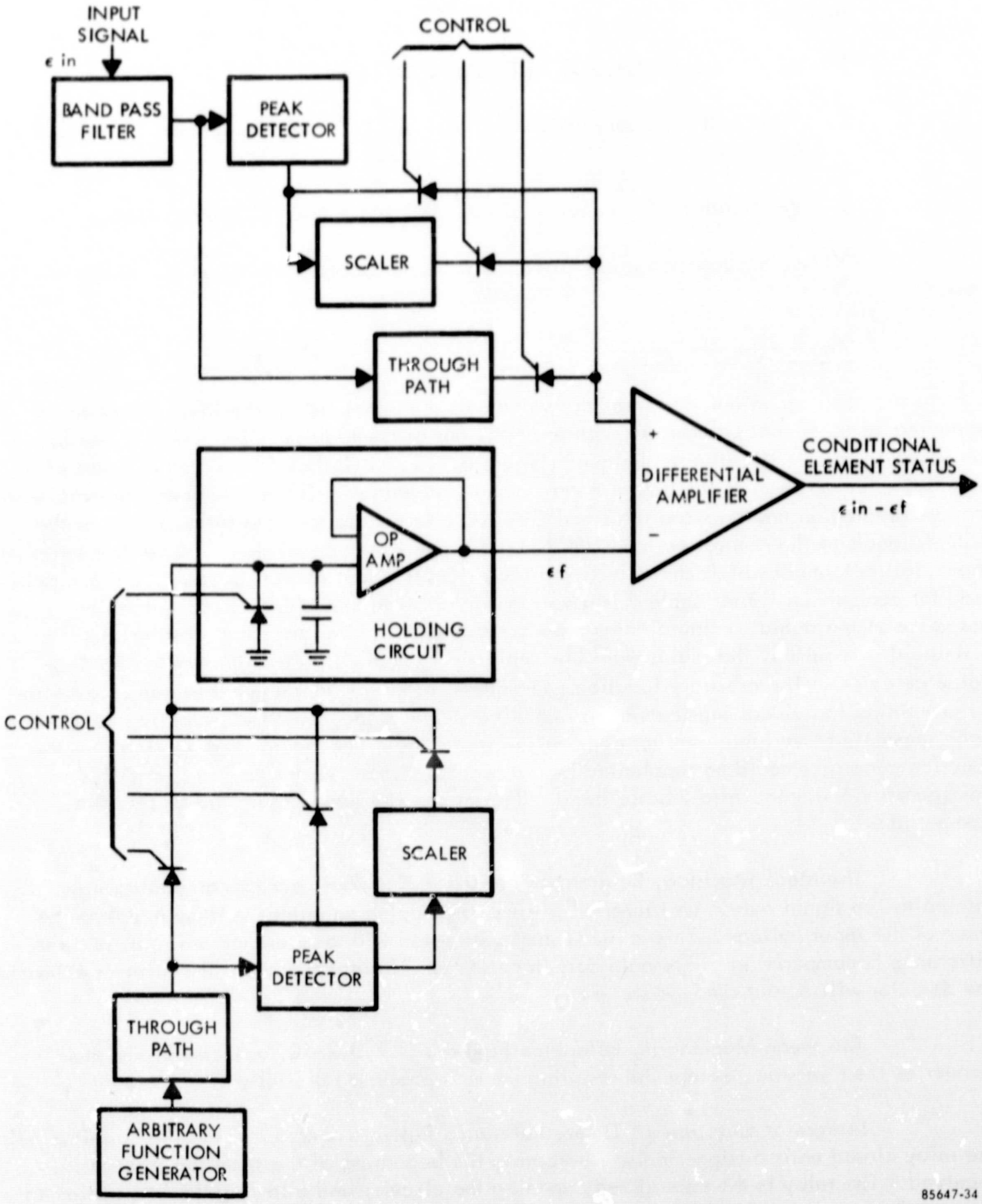


Figure 5.2.2.5.2-8. Signal Form Analysis

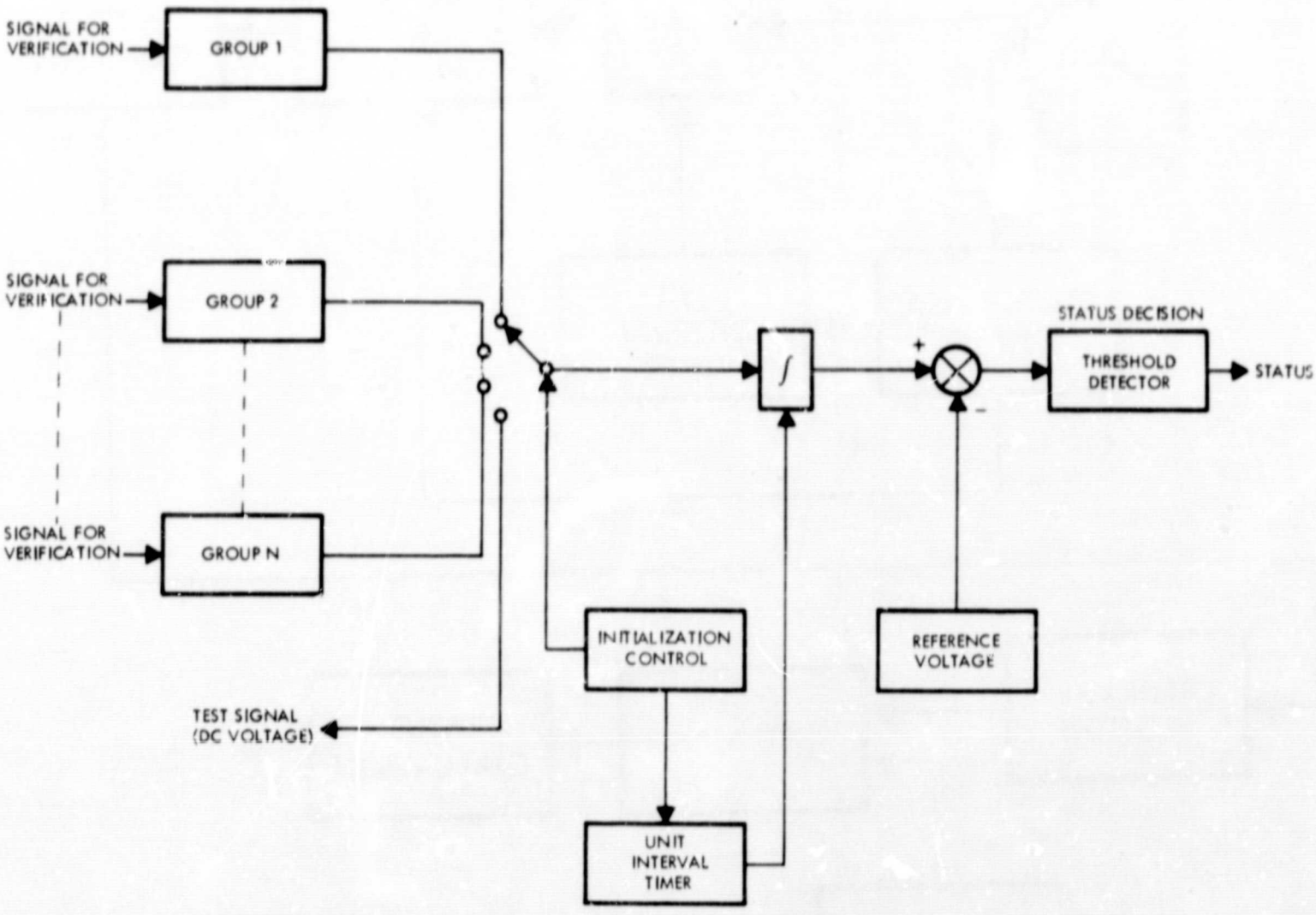
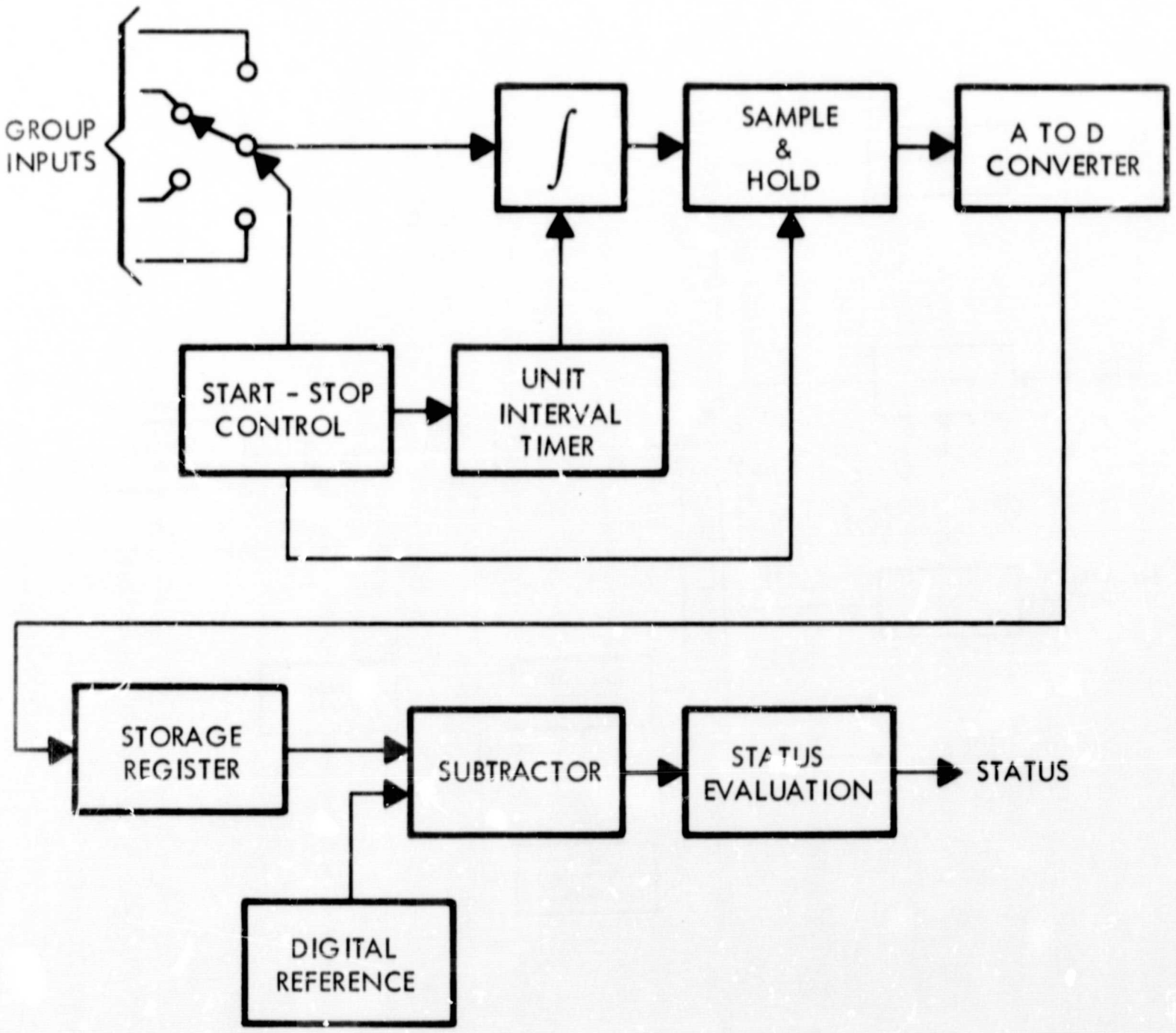


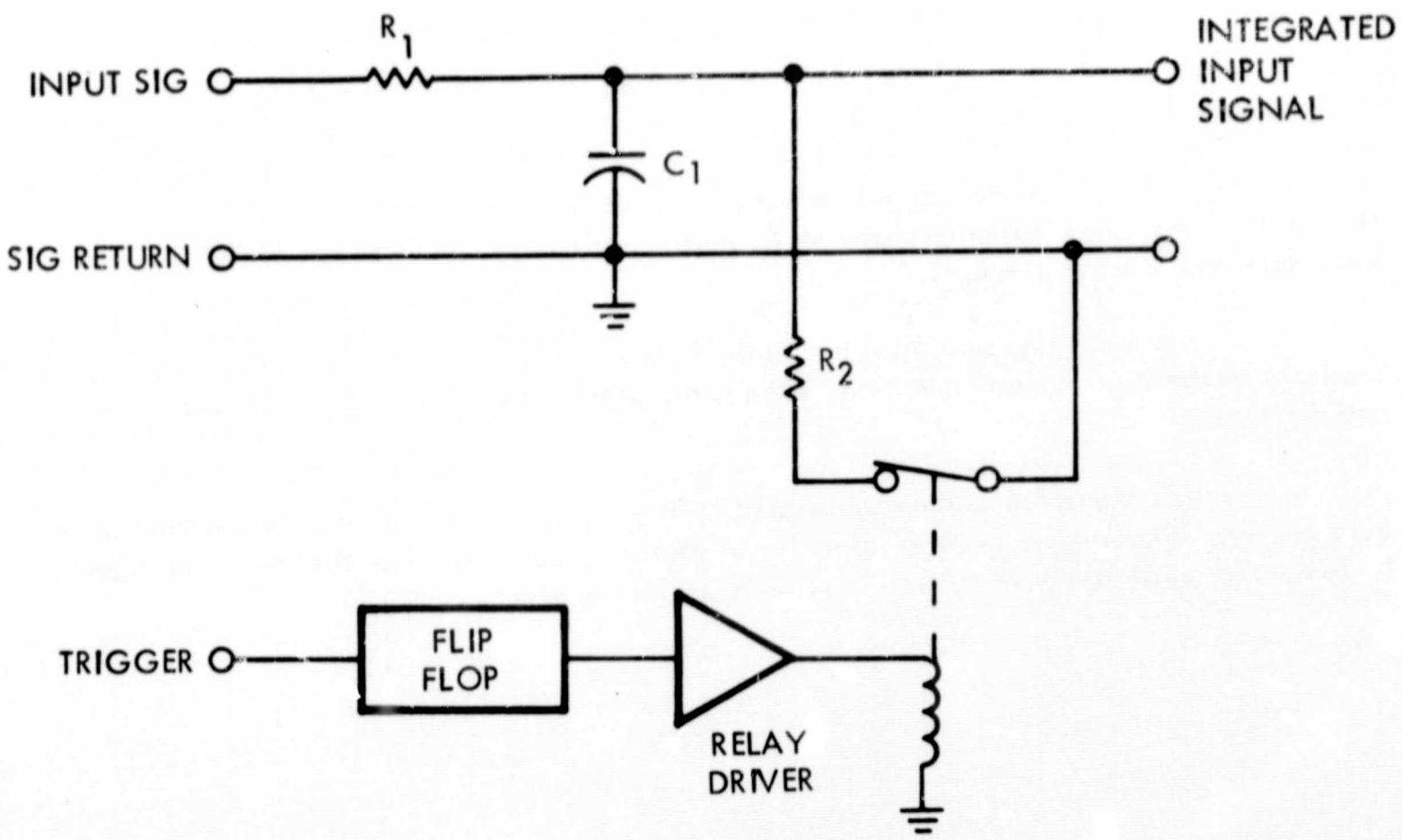
Figure 5.2.2.5.2-9. Mean Machine I



THIS MACHINE OPERATES IN THE SAME MANNER AS THE I VERSION, EXCEPT THAT THE RESULTING MEAN IS PROCESSED DIGITALLY.

85647-27

Figure 5.2.2.5.2-10. Mean Machine II



NOTES: 1. R_1 AND C_1 SHOULD BE CHOSEN TO INTEGRATE THE SIGNAL OVER THE FREQUENCY RANGE OF INTEREST.

2. R_2 IS A CAPACITOR-DISCHARGE RESISTOR. SHOULD BE LOW VALUE.

3. IF MORE SOPHISTICATION IS DESIRED, AN OP-AMP INTEGRATOR MAY BE USED TO REPLACE THE LOW-PASS FILTER INTEGRATOR.

85647-28

Figure 5.2.2.5.2-11. Integrator and Interval Timer

Peak Machine, Reference Figure 5.2.2.5.2-12. The circuit shown follows only negative peaks, but by reversing all the diodes in the switch portion, it can be made to follow positive peaks. Negative-going values of e_{in} cause positive current to rapidly charge C (R_1C should be small compared to $\frac{de_i}{dt}$) until the + output (+e) corresponds to the largest negative peak of e_1, at which time the error voltage at S is zero, and D_d becomes nonconducting. Thus, the largest value of e_{in} will be stored on C, which is prevented from discharging by the back-biased D_d and the open switch. The value of e_{peak} is converted to digital, and a pulse at the end of the sampling period stores it in the storage register. This pulse and the reset pulse come from a timing block (not shown), which also controls the switching of the input for time-sharing purposes.

The mean-squared (MS) machine, Reference Figure 5.2.2.5.2-13, operates similarly to the digital mean machine, except the input signal is first squared, then averaged and digitized.

This MS value is then subtracted with a digital reference and the difference is evaluated to determine the status. This is, in effect, a comparison of the rms value against its expected value but with the root-taking operation omitted.

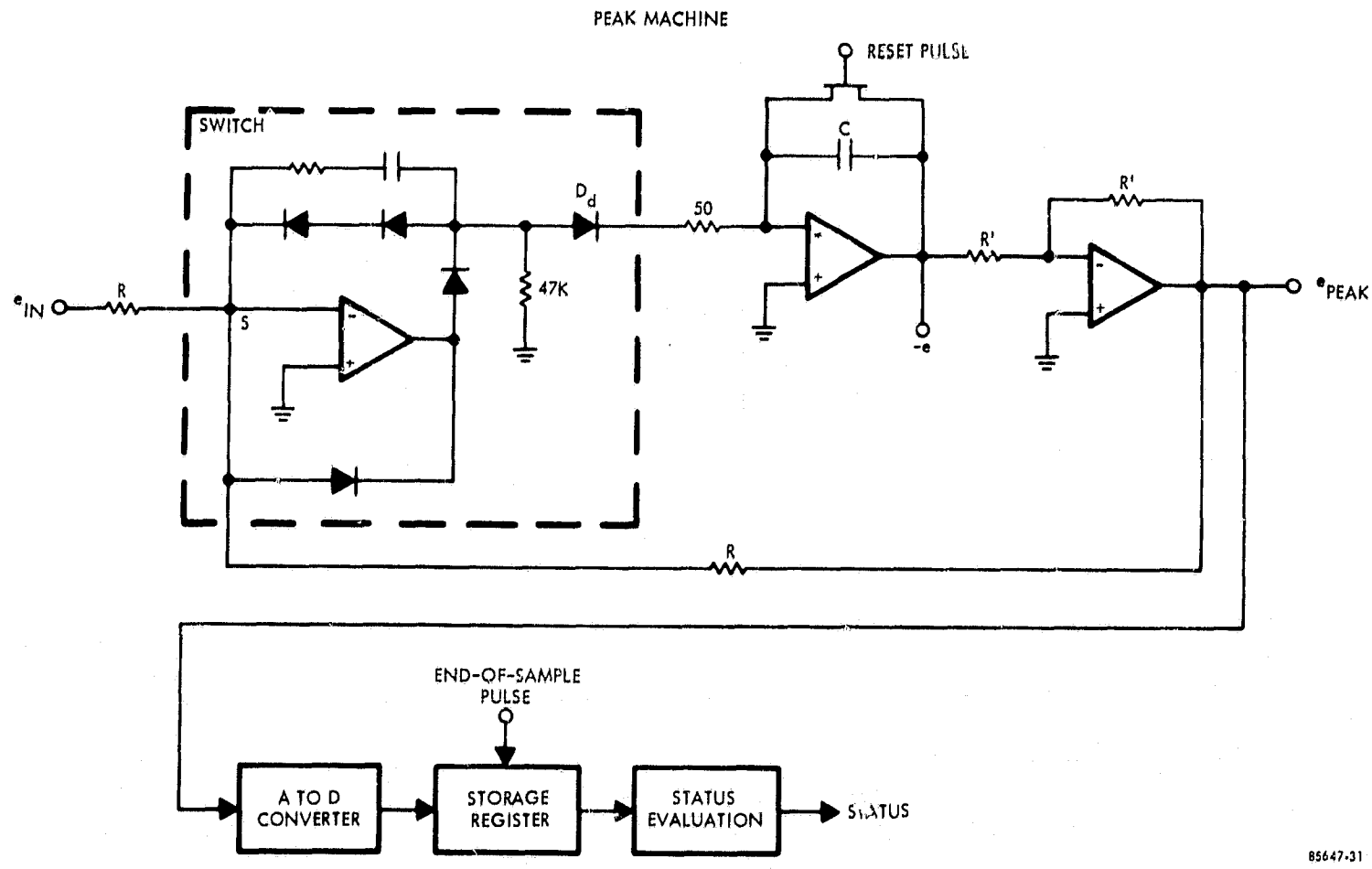


Figure 5.2.2.5.2-12. Peak Machine

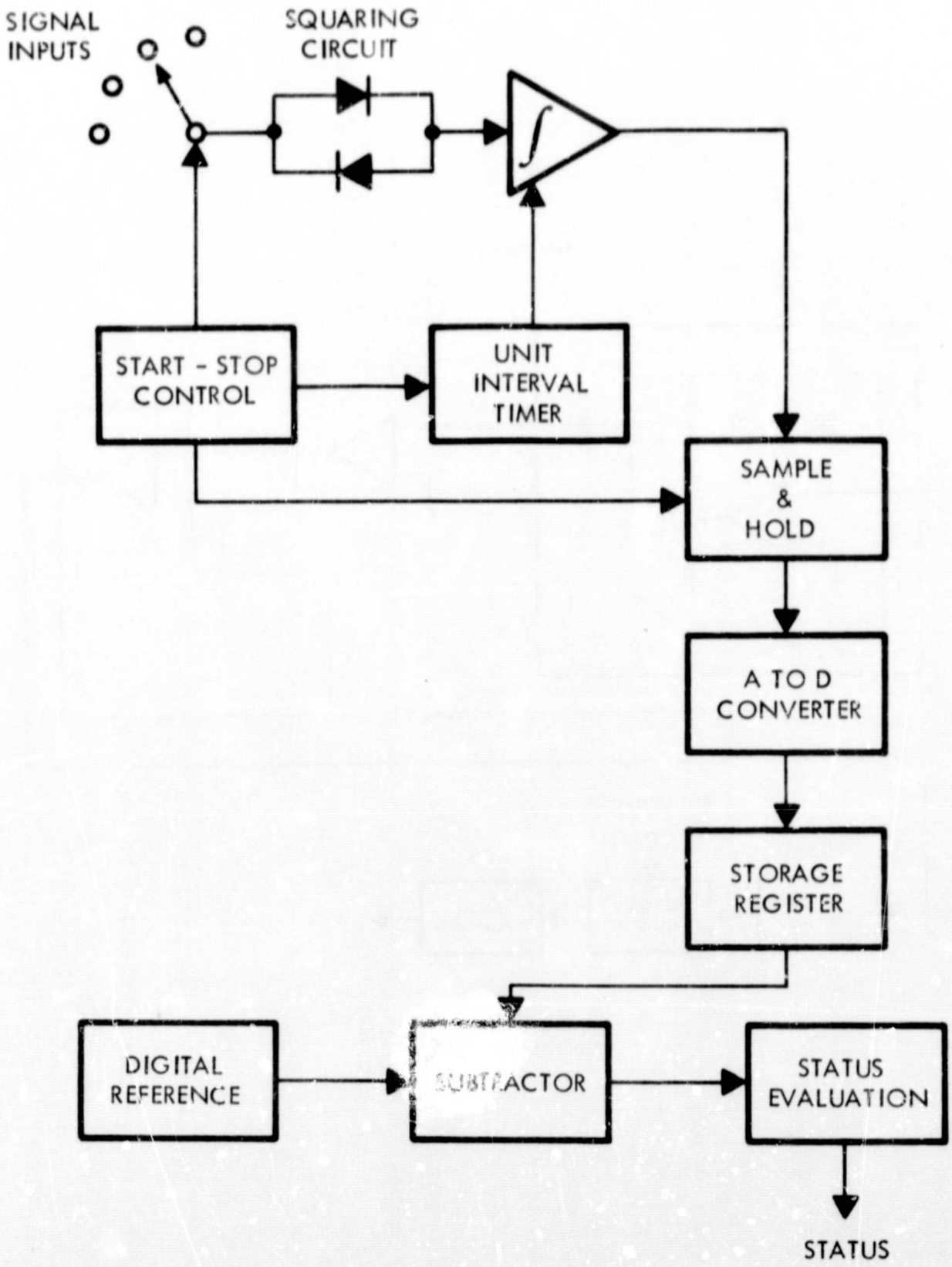


Figure 5.2.2.5.2-13. MS Machine

The Instantaneous Frequency Machine, Reference Figure 5.2.2.5.2-14, accepts an input signal into a wideband discriminator which outputs a voltage proportional to the input frequency. Since this device will normally be used to measure a single-frequency sinusoid, the output voltage of the discriminator will indicate the instantaneous frequency of the signal. This voltage is then sampled at the desired instant, and the voltage measured is converted to frequency. The accuracy of this conversion does not depend on the linearity of the discriminator, since the discriminator may be calibrated in advance. The resultant frequency is then evaluated to determine its acceptability.

Complete Spectrum Analysis

Refer to Figure 5.2.2.5.2-15. The three elements of Group I are sampled on a time division basis, through controls and commands from the central processor. The input signal is applied to the spectrum analysis circuits, via the mixer. The receiver-mixer is tuned by the sawtooth generator driving the voltage controlled oscillator, with the sawtooth sweep simultaneously applied to the horizontal deflection plates of the cathode ray tube. The output signal of the receiver is applied to the vertical deflection plates, thus producing a plot of signal amplitude versus frequency on the screen.

The complete spectrum will be reproduced for visual evaluation. For those applications where the energy level of a frequency of interest is to be ascertained, with automated means, discriminators and analog gates must be incorporated as shown. The video output is applied broadside to these analog gates and gated out to a specific monitoring device where a monitoring technique may be applied to determine absolute levels, excedence of minimum acceptable levels, etc. The gate is triggered by the output of discriminators centered at the frequency of interest. As the VCO sweeps through the spectrum, each discriminator will be exposed to its proper band in a time division sequence. Thus, when f_x is reached, the gate will open and the video amplitude at that instant will be gated out to the monitoring device which consists of a detection measuring device, a differential amp, and a stored reference for evaluation.

For the self test features, the test pattern is included to be utilized randomly or after each failure is encountered, to validate the spectrum analyzer circuits. With the self test, both Type I and Type II errors may be minimized.

The Input Test signal is incorporated for two conditions:

a. In the complete absence of inputs on any elements, a test signal is necessary for determining redundancy of circuits.

b. Under normal operation, where only one element is utilized, the other two may be randomly evaluated on a noninterferring basis.

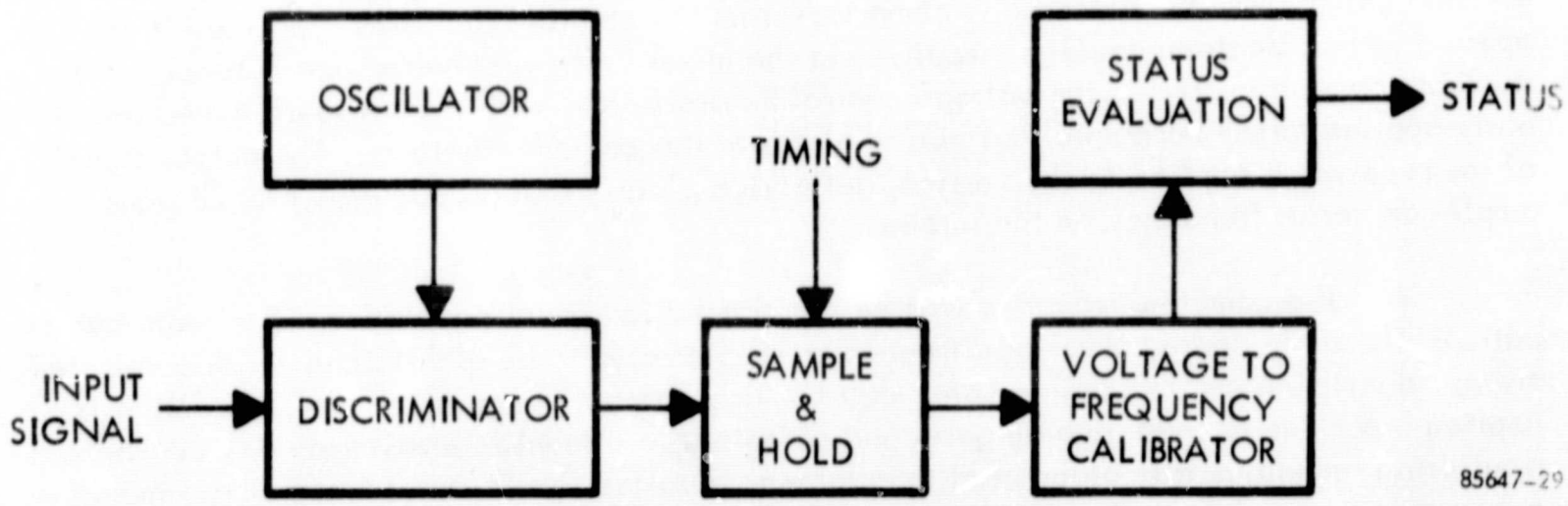


Figure 5.2.2.5.2-14. Instantaneous Frequency Machine

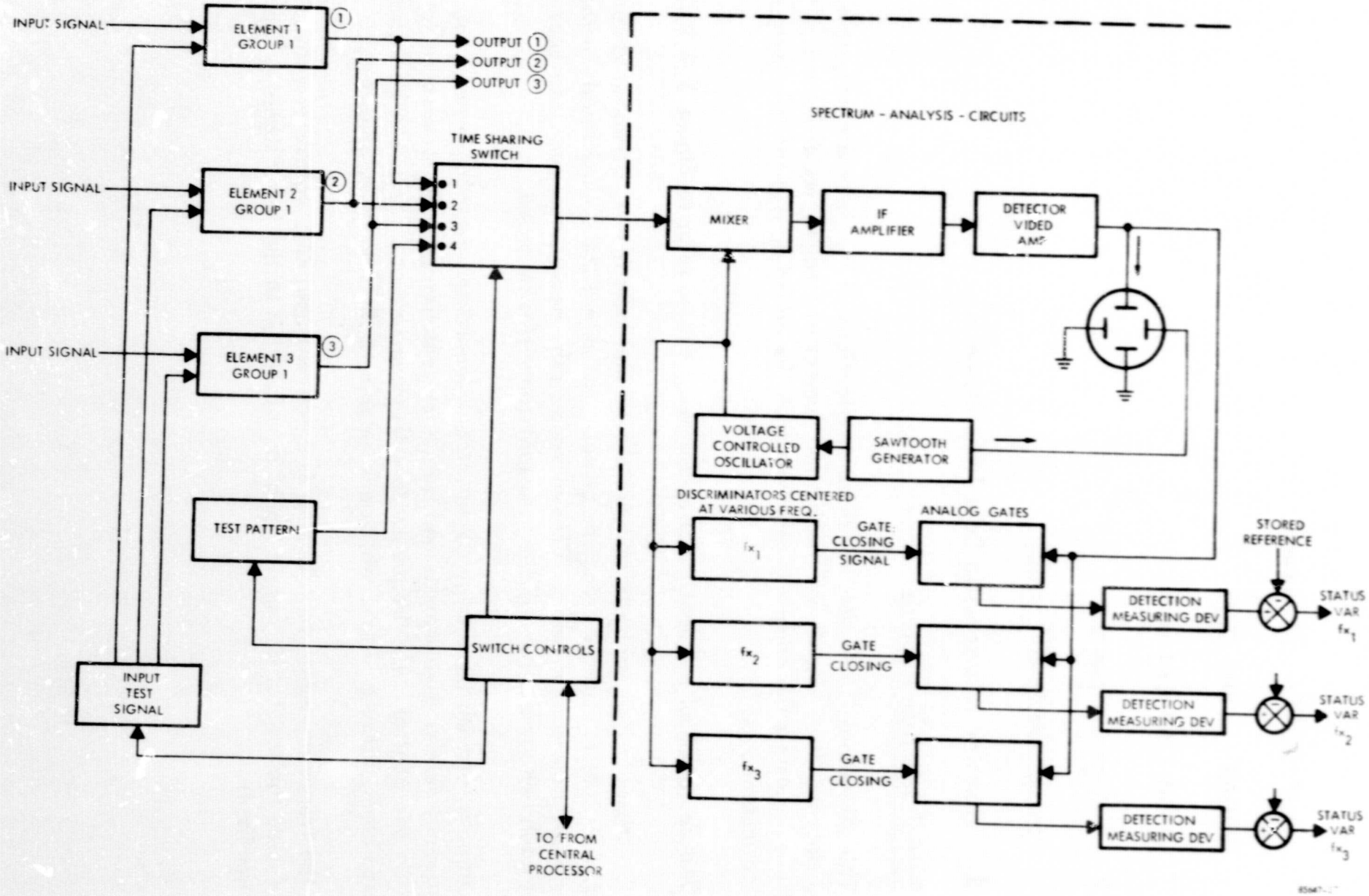


Figure 5.2.2.5.2-15. Complete Spectrum Analysis

Typical tenant signals presently in use at KSC that could be applied to this technique:

1. PCM/DDAS - FSK waves

   DDAS ±35 kHz Dev.

   PCM ±75 kHz Dev.

2. S-Band Composite

   phase modulated carrier

3. Vibration and Acoustic Data Transmission

Partial Spectrum Analysis

This procedure is intended for those applications where there are only selected frequencies of interest or concern. With a limited number of frequencies of interest, it becomes rather superfluous to assess the complete spectrum with the added equipment necessary for this complete spectrum analysis.

The operation of the configuration follows. Please refer to Figure 5.2.2.5.2-16.

On the output of each element are placed bandpass filters, centered about f(x) the frequency of interest. Energy detection circuits, to detect the energy levels in the bandwidth under a prescribed criteria, (RMS in bandwidth, peak level, etc.) are placed on the output of each bandpass filter and the resultant quantities recorded.

In parallel with the energy detecting and recording, the filter outputs are time shared to frequency sensitive voltmeters and frequency sensitive comparator circuits for real time evaluation and control. The frequency sensitive comparator circuits can be instrument servos, demodulators, circuits, etc., which are tunable to the frequency of interest.

The frequency sensitive voltmeter is a conventional RMS voltmeter with selectable filters placed upon the input. An output signal as a function of the input signal is included for direct computer input.

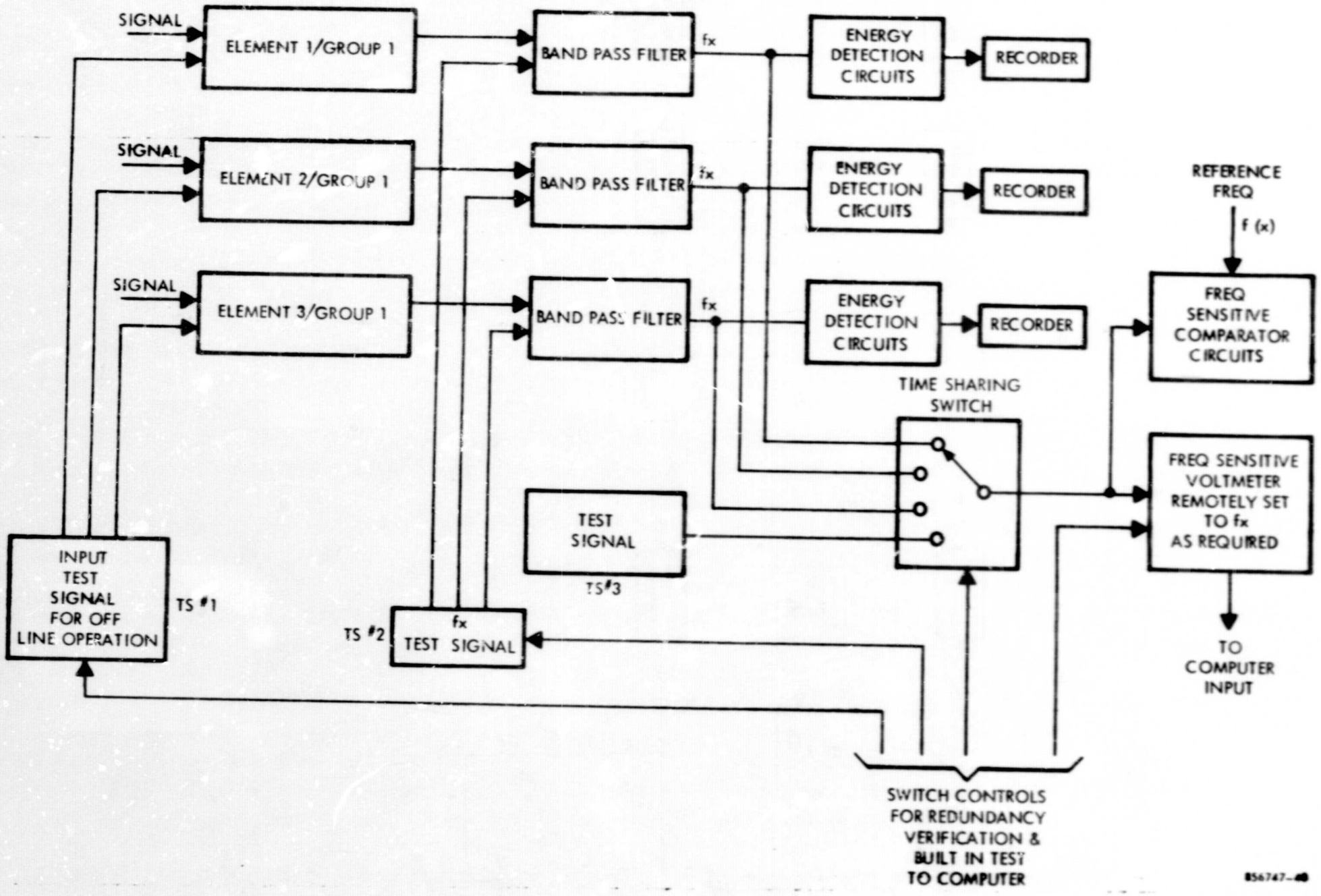


Figure 5.2.2.5.2-16. Partial Spectrum Analysis

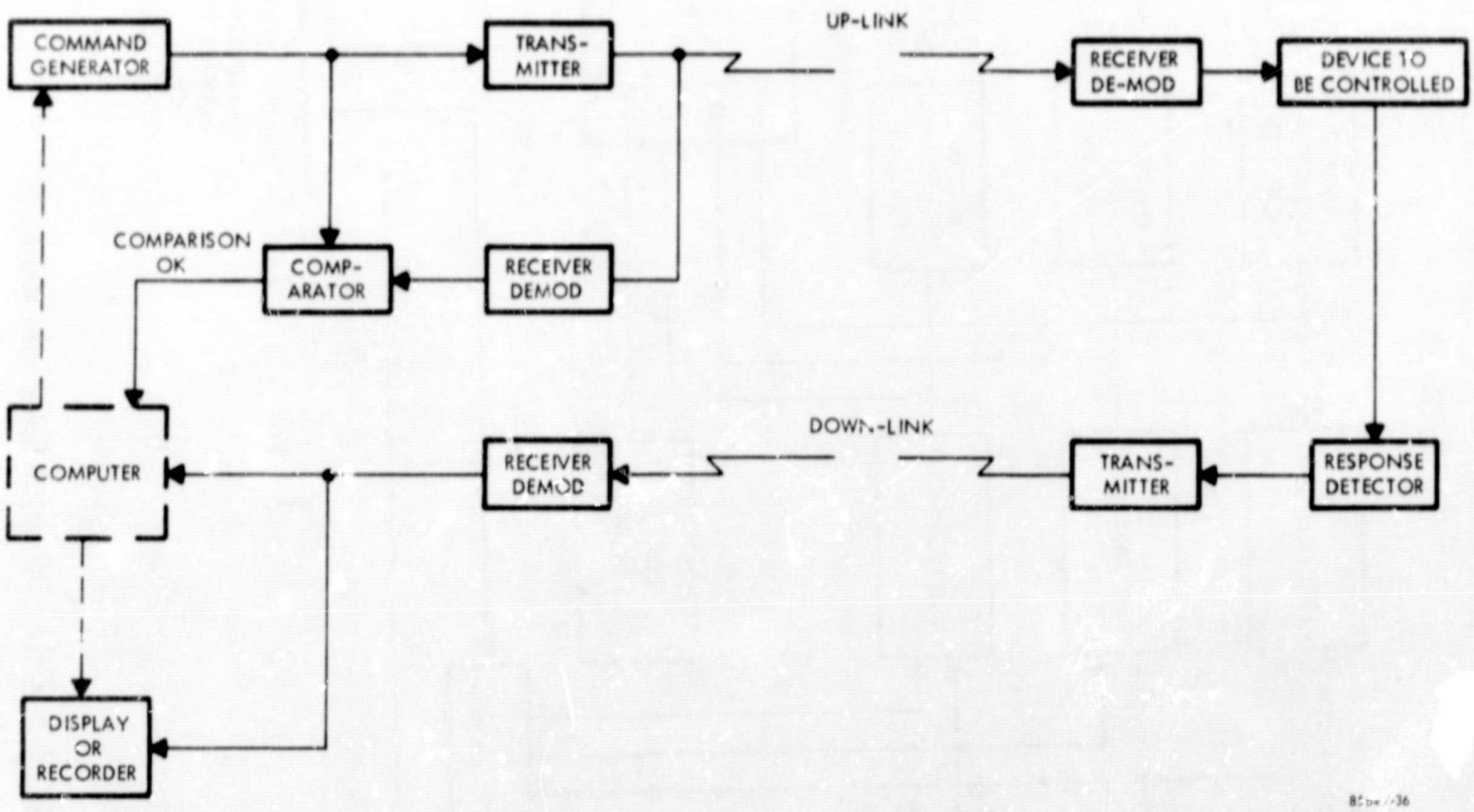


Figure 5.2.2.5.2-17. Acknowledgment

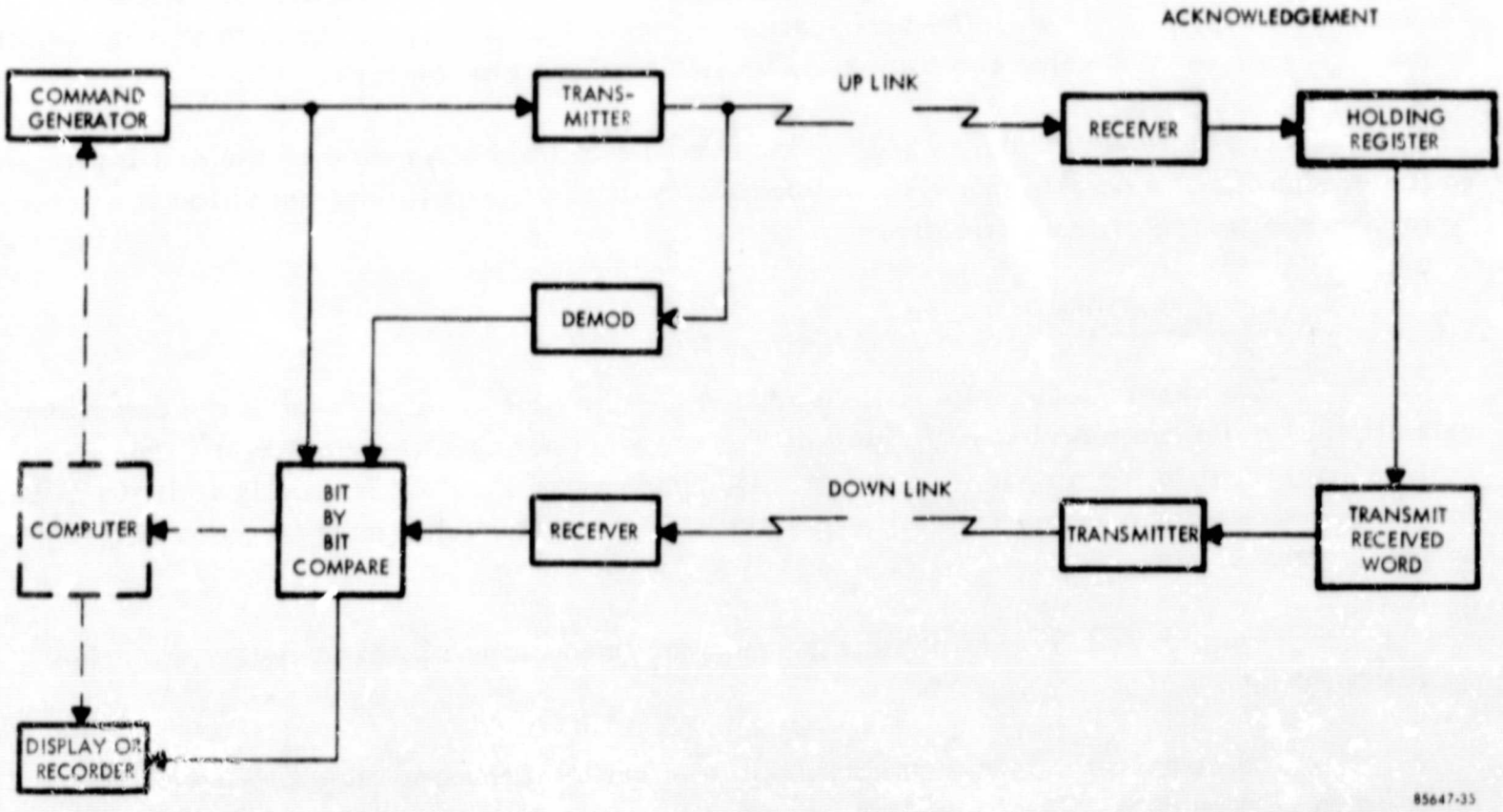


Figure 5.2.2.5.2-18. Acknowledgment

The operation of the verification equipment follows. The external control lines, from a centralized computer, are noted. An input Test Signal Generator is present for (1) OFF line testing of the group, or (2) selective testing of elements not in use at that moment. The spectrum of the TS#1 signal will be analogous to the spectrum of the tenant signal. With the external controls and the time sharing switch, evaluation of the f(x) component may be performed on all elements in the group on a nondisrupting basis, presuming sufficient isolation of the verification equipment.

A second test signal is present, TS#2, the f(x) test signal which is included to quantitatively evaluate both the throughput circuits, (Filter Energy detection circuits and the recorder) concurrently with the verification equipment consisting of the time sharing switch, frequency sensitive voltmeter and frequency sensitive comparator circuits.

The third test signal, TS#3, is included for a rapid assessment of the end instruments of the equipment and can be called up automatically after each deficient condition is discovered to resolve the source of the difficulty.

Acknowledgment

Two general cases of acknowledgment will be noted. Both involve the command and execution of a desired function with the only variance consisting of the type of affirming indicator returned to the command location. This positive affirmation is usually utilized as an enabling function for a highly critical sequential string of events that must be performed in perfect order.

Figure 5.2.2.5.2-17 depicts the more common usage of Acknowledgment. The operation follows:

The computer activates a command, through the command generator, for a desired function to be executed. The transmitter receives the command, modulates a RF carrier where a signal extractor samples the RF signal, is demodulated and compared locally to the command generated for an exact bit by bit comparison. A comparison OK signal enters the computer for evaluation and further processing. Concurrently with this local check at the transmitter, the command signal is received at the device to be controlled and the command control function performed. Once the control function has been implemented, a response detector senses the change of state, motion or other discernible action and transmits back to the computer control station, a highly distinguishable signal with an equally low probability of misinterpretation. This response signal is received, evaluated and utilized in the computer as an Enable for a succeeding function.

The second general type of acknowledgment is illustrated in Figure 5.2.2.5.2-18.

Operation is detailed as follows: the computer activates the command generator, which drives the transmitter. The transmitter output is demodulated and compared on a bit-by-bit basis with the command generator output. Concurrently, the transmitter output (UPLINK) is received, demodulated and placed in a holding register. At this point, the major divergency

with the first method appears. The entire contents of the holding register are transmitted on the downlink back to the command control station, where a second bit-by-bit comparison is performed, this time between the downlink word and the command generator. After the comparison is acceptable, a function enable is transmitted and the command actually executed.

Applications of Acknowledgment

1. Command Control
2. Command Separation
3. Critical Electromechanical Verification
   A. Thrust Vector Control
   B. Aerodynamic Control Surfaces
   C. Hydraulic Valves
4. Remote Auto Calibration System (RACS)

User Complaint

User Complaint can be considered a special case of acknowledgment where the human element provides the decision criteria concerning the unacceptable status of the element/set output signal.

This verification method is circuitwise open-ended as only an indication of signal is provided with no automatic remedial action.

Implementation can consist of common indicating devices;

Meters - Digital words representing signal levels,

Electromechanical Motion Detectors

5.2.2.5.3 Output to Input Comparisons

Inverse Transform and Correlation methods for output to input comparisons are detailed in this subsection.

Inverse Transform

Inverse Transform is generally applied to a complex analog function. Restrictions include the admissibility of the input and the criticality of the delay network and differential amplifier. Refer to Figure 5.2.2.5.3-1.

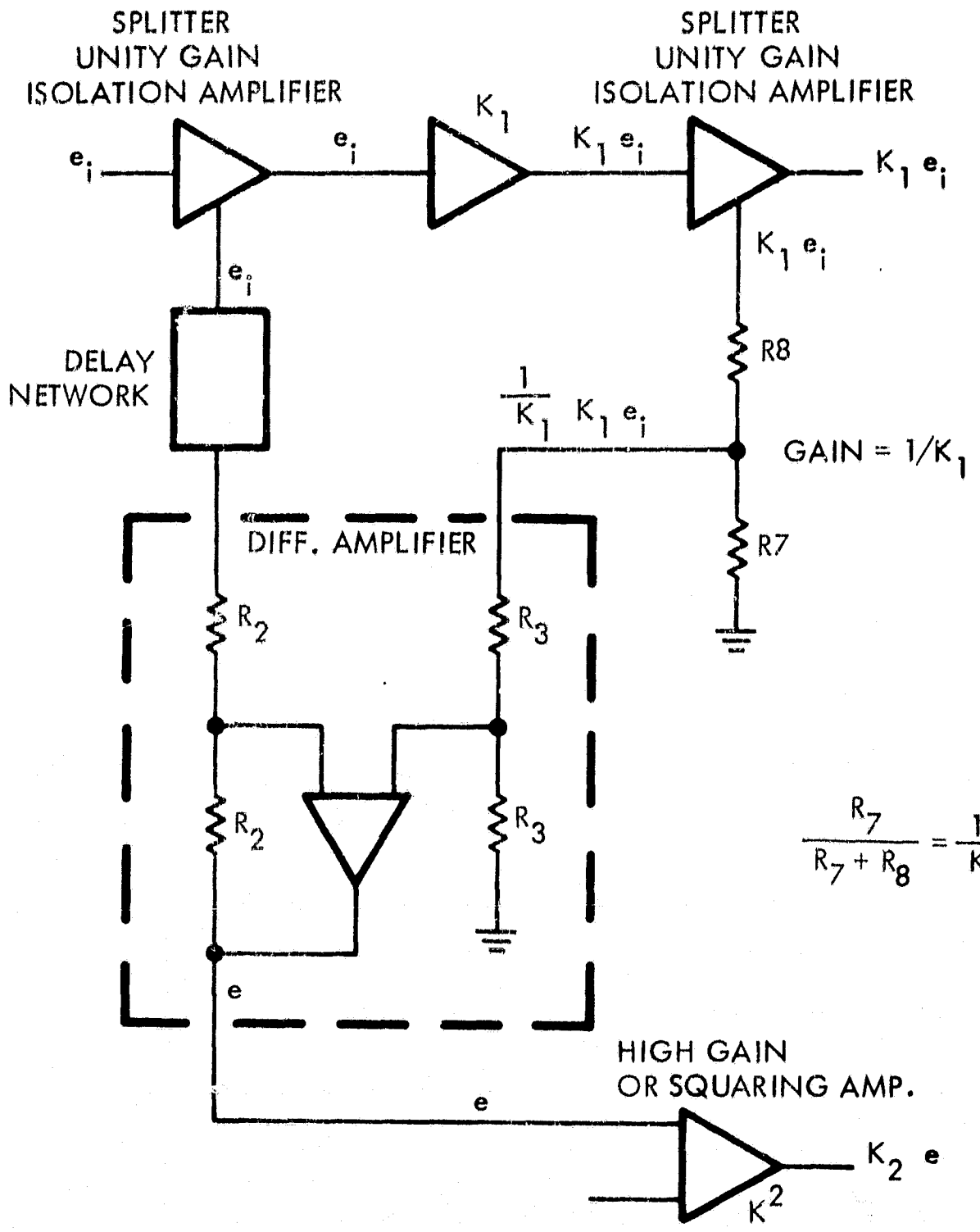


Figure 5.2.2.5.3-1. Inverse Transform

The status variable, e,should present a null condition, subject to external noise and EMI, thus amplifier K_2 should be a highly accurate wideband amplifier with a gain consisting of either

1. Linear High Gain

2. Squaring

In either case the S/N level will be raised to levels precluding the adverse effects of noise.

Typical functions presently in use at KSC that this method could be applied to consist of:

1. G&C

   Inertial platform parameters

2. Servo-Controls on movable nozzles

3. PTCS Propellant tanking and computer system

4. Antenna Drive Servos

The technique illustrated in Figure 5.2.2.5.3-2 is generally classified as Inverse Transform though it does employ some coding techniques through a tandem transmission configuration and a bit by bit comparison of the transmitted and received codes.

The operation follows: A digital code is generated and transmitted on Line 1. Line 1 is looped through to Line 2 and retransmitted to the signal source area. The transmitted code is delayed in time equivalent to the sum of the Line 1 and Line 2 delays and fed into a bit comparator where a distinct bit by bit comparison of the locally generated and retransmitted bits is performed.

Differences between bits are cumulatively counted as errors. The high S/N of the locally generated code enables the local code to be acceptable as a standard, thus the probability of both Type I and Type II errors is minimized.

Geographical considerations of nonproximity between ends of a transmission link make the utilization of this method feasible. A source of ambiguity does exist as to culpability when the error rate becomes excessive. With two transmitters, two receivers, two lines and a loop through in series, further localized testing would be necessary to isolate the indicated error source.

Applications

A2A lines between Pads and MSOB

Two way testing of D.T.S. (Data Transmission System with Prop. Tank Comp. Sys.

The Cross Correlator, Reference Figure 5.2.2.5.3-3, is capable of calculating the cross correlation function, $R_{ab}(\gamma)$ between the input and output of a set/element. The signals to be correlated are first digitized. Then the output signal is sampled n times at $\Delta\tau$ -second intervals. On the final sample, the value of a(t) is also sampled and stored. After sampling, the unit switches to the processing mode, in which each delayed value of $b(t-m\Delta\tau)$, $m = 0, 1, \ldots n-1$, is multiplied by the value of a(t), forming the cross-correlation function, $R_{ab}(\tau)$. These newest values are used to update the previous values in the average and store register. After a sufficient number of process cycles, the averages in this register should approach a final value.

Once the cross correlation is computed, it may be displayed on a CRT, or recorded, or processed. One form of processing might be to compute the power density spectrum by Fourier-transforming the correlation function.

Cross Correlation

Time Domain Reflectometry

A very special case of cross correlation, useful for limited special purposes in the off-line conditions is time domain reflectometry (TDR). (Refer to Figure 5.2.2.5.3-4.)

This method consists of applying a very sharp rise time pulse in the nanosecond range to an element/set and evaluating the reflected pulse.

The distance L is included to calculate the time between successive echoes and thus aid in the determination of the second and third echoes.

The high impedance probe also attenuates these secondary pulse echoes further negating error possibilities.

The reflected wave will be:

1. Delayed
2. Reshaped
3. Discontinuous (possibly)

as a function of series and parallel impedance elements, and circuit discontinuities.

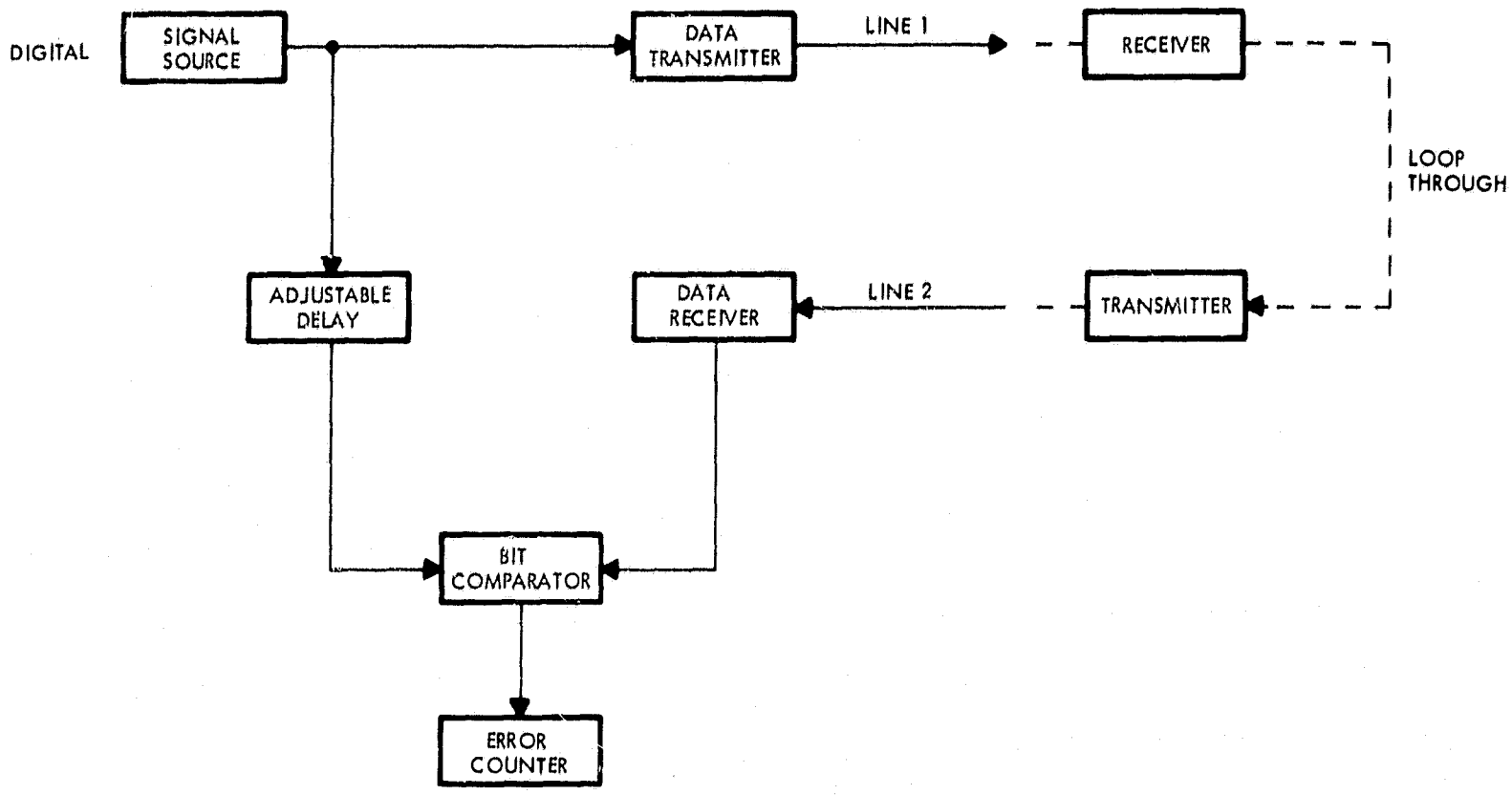


Figure 5.2.2.5.3-2. Inverse Transform

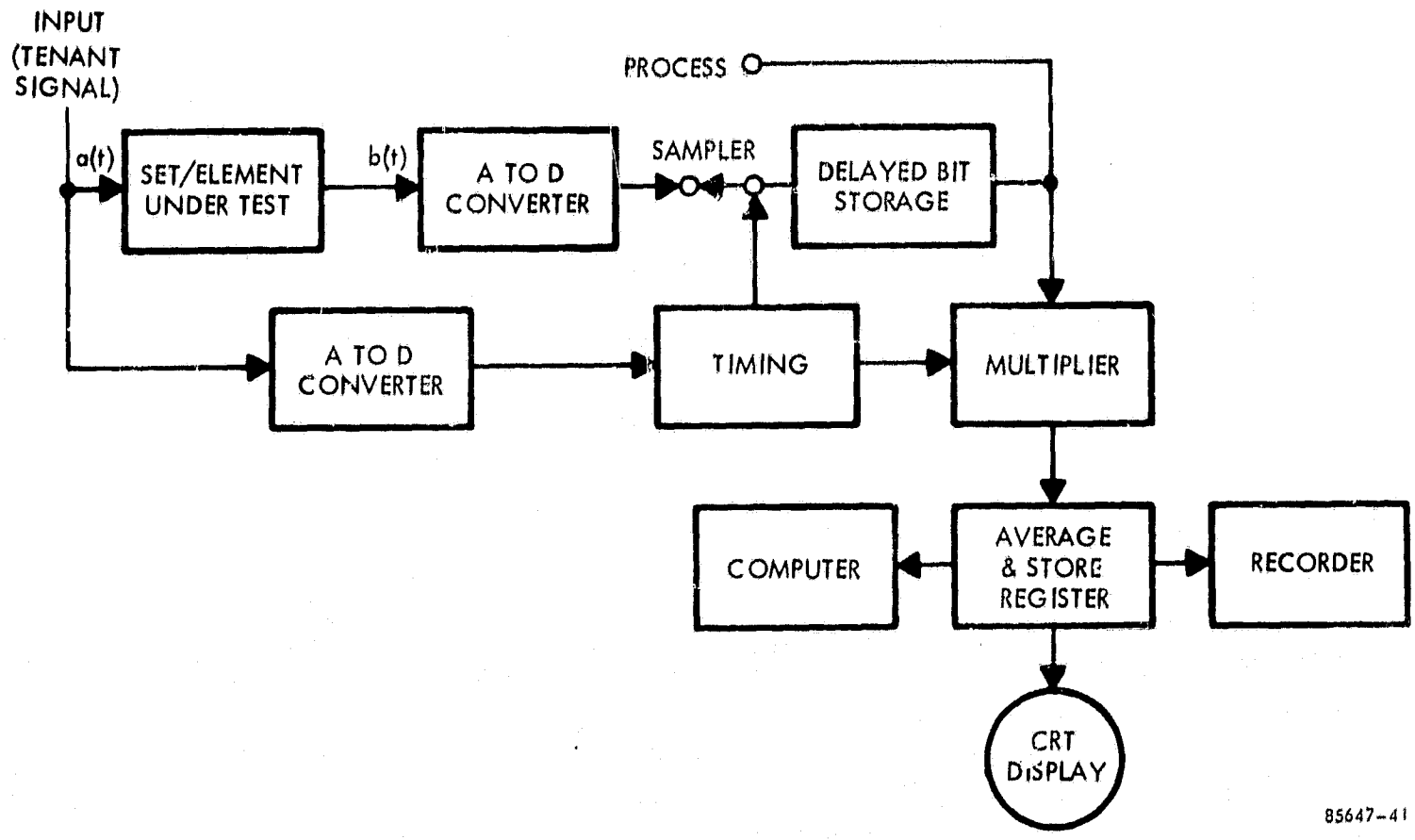


Figure 5.2.2.5.3-3. Cross Correlation

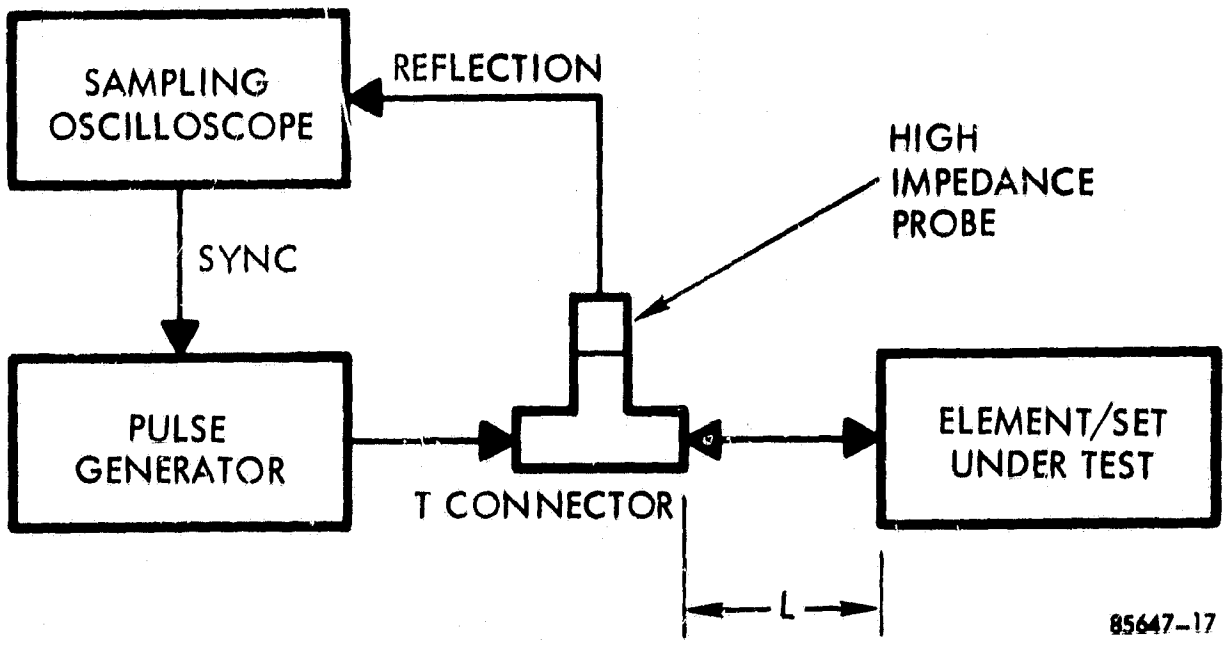


Figure 5.2.2.5.3-4. Time Domain Reflectometry

Possible Applications

1. Testing of Wideband transmission cables of the coaxial, triaxial, and balanced twin types

2. Antenna Testing

3. Ordnance Devices - Such as exploding Bridge Wires (EBW) with the built-in air gap and discontinuity

4. Dielectric changes in multilayered fluids

5. Dielectric changes when fluid levels recede (Fuel tank level indicators)

6. Impedance Measurements

Cross Correlation - Applications

1. Servos in inertial

2. Thrust vector control servos

3. Antennae drive servos

4. Measuring time delays through units or through transmission mediums (ranging equations).

Reference figure.

5.2.3 The Group Problem

Having examined the details of the set problem, let us see how verification is performed when the sets are put together to form a system and how level one groups are addressed. The heart of the group problem is the method of identifying the status of elements within the group. Recall that a group may consist of simple sets and lower level groups as well as being an identifiable entity which does not possess the attractive properties of a simple set (a level one group). The implication may have been drawn from Section 5.2.2 that verification of all sets must be approached in the method described. This is not necessarily true. From the group problem standpoint, these methods apply if verification of a particular set must be accomplished.* Let us explain. There are other methods of verifying on-line elements. One such method is identifying the element using status information about inter-related elements which is sufficient to reason the status of the element under contention. We

*This statement may seem anachronistic after the previous treatment of sets. The set problem was addressed first in the belief that the principles are more straightforward than those of groups.

shall call this process logical deduction. If uniqueness and completeness apply to the situation, this process is quite feasible and usually at a reduced cost. A second method of identifying an on-line element which is not performing satisfactorily is simply to switch it out and replace it with another element in the set. (We are assuming this action is performed on an automated basis.) If the unsatisfactory condition disappeared, the element switched out must have been unsatisfactory. To realize the full benefits of this approach, it would be applied to an entire group (of any level). When an unsatisfactory condition developed, the verification equipment would simply commence switching until the condition was corrected. We shall call this process iterative deduction. When the status of each element in a group is determined by the techniques of Section 5.2.2, we shall term the process exhaustive deduction.*

What has been gained by the processes of iterative and logical deduction? In answering this question, we should first point out that in each case we still described a mechanism for detecting unsatisfactory operation. The primary gain has been in the number of detecting mechanisms required. Conceptually, the iterative process would require only knowledge of the conditional status of the group (at its output) and the status of the input. No status of the intervening elements would be directly required. If the group is quite large, this could be a significant savings in cost and weight - provided the switching time is acceptable. Logical deduction realizes the same benefits, but typically on a much smaller scale. It is important to note that neither approach does away with verification techniques and whenever a verification technique is required, the material of Section 5.2.2 applies.

The group deduction processes are addressed in more detail in the following sections. Before we consider this detail, however, it may be fruitful to summarize some of the differences between sets and groups.

- By their nature, the status of a group (analogous to status of a set) will typically have no meaning, for knowing 3 of 5 elements in a group are up will seldom tell the desired story. However, it may be possible to attribute a status statement of the form - all elements up, not all elements up - to a group.

- Unlike the simple set where (usually) one element is on line and we may have the option of using simulative input signals to the remaining elements, the interconnection of elements in a group will require (usually) that more than one element use the tenant signal.

- In a simple set, knowing the status of one input (although it may be many independent information paths) will confirm the conditional status of an element. In a group this will typically not be so.

*It should be noted that, as described in Section 5.2.1.3, exhaustive deduction can also be achieved by injecting a signal at the input of every element.

5.2.3.1 Exhaustive Deduction

Exhaustive deduction as an approach to the group problem is the determination of status on a set-by-set basis, in essence being the simultaneous or sequential application of the simple set techniques discussed. With this statement it becomes obvious that the major limiting factor on the use of this approach will be accessibility, for the application of the simple set techniques requires that distinguishable element outputs or, at the least, observable element effects in a set output be made available for verification.

Because of the degree of penetration into the group which is afforded by an approach of this kind, the degree of comprehensiveness attainable through the use of exhaustive deduction will exceed that due to iterative or logical deduction. The ability to verify an operation independent of others will always offer the potential for a greater understanding of that operation. It would not, for example, be expected that offsetting failures or out-of-tolerance conditions in successive sets would go undetected.

Exhaustive deduction would naturally require the greatest amount of equipment exclusive of command-and-control functions. If the same provisions and usages which allowed continuous verification in the simple set case (noninterruptive sensing of signals for verification, use of tenant, symbiotic or idle signal for verification, etc.) continuous verification will be possible for the group problem. This is a capability unique to the exhaustive approach. Another unique feature of exhaustive deduction is that the advantages of requiring only an admissible input for status resolution, a feature attributed to certain of the coincidence development techniques, can be passed on to the group problem when the same techniques are employed for exhaustive deduction. As an example, a group problem for which exhaustive deduction was carried out by voting on each set of element outputs might well require no knowledge of set inputs to resolve conditional status into status. It may be additionally noted that wherever simple sets appear in a serial configuration, exhaustive deduction may establish conditional status for the first set and input status for the second set simultaneously, thus facilitating status resolution.

The results of "exercising" an element will be more readily observed than will be the case for the other deductive schemes wherein the element's output may have to pass through successive elements prior to its observation.

The amount of verification equipment required to implement an exhaustive scheme will increase in rather direct proportion to the complexity of the group under scrutiny. (We shall for the moment ignore equipment savings by time-sharing). Exclusive of command and control functions, the exhaustive approach will demand the most verification equipment. Where the possibility of verifying in a continuous fashion by the coincidence methods which facilitate status resolution (output/output and output/input comparisons) the exhaustive approach, not needing command and control, may require the least total amount of equipment.

With proper design of principal system equipment, such as the provision of a second, isolated input from each element, or the use of noninterruptive signal sensing techniques, exhaustive deduction could be accomplished with a total lack of switching in the principal system equipment. This is an advantage over iterative deduction.

The possibility exists that, when output/input coincidence development techniques are applied to a series of equipments, a tolerance buildup in the chain could go undetected unless the group output were in some fashion checked against this possibility. For example, a chain of Inverse Transform checks might all show good yet the group output be bad.

The ability to check many sets simultaneously makes exhaustive methods faster than iterative. The advantage is multiplied if it is necessary to use exercising signals.

The occurrence of a majority voting set within a group will not affect the applicability of exhaustive deduction nor complicate its implementation so long as element outputs are made accessible. The same may not be said for iterative and logical deduction.

5.2.3.2 Iterative Deduction

Iterative deduction implies the ascertaining of group status by performing iterative switching of redundant elements. This can be achieved through two basic approaches which essentially amount to continuous verification on the one hand and noncontinuous verification on the other. Considering the continuous verification approach first, the play here is to approach verification of on-line and off-line elements in two distinct ways. (See Section 5.2.1.2.) The on-line elements are obviously all connected to perform the intended group function and these elements are verified as a collection by observing only the group output on a continuous basis. The off-line elements are configured in whatever fashion proves convenient for their continuous verification. So long as the technique does not involve the on-line elements, virtually any, in any combination, of the techniques described in Section 5.2.2.2 can be used. For example, inverse transform may be used on one off-line element and any one of the monitoring methods could be used on the remaining off-line elements. Or, the off-line elements could be configured serially, as described in Section 5.2.1.2, to form a second parallel collection of elements.

The above will accomplish continuous verification. However, what will happen when an on-line element fails? How is the status resolved? When the on-line verification technique determines that the on-line string has experienced a failure, it will initiate a search routine which begins switching in off-line elements, according to some algorithm, until the failure indication is removed.* The last switching occurrence, the one that removed the failure, is identified with the failed element. Since the off-line elements are being verified continuously, elements of known status are being substituted at all times. Should an off-line element be in a failed state, the iteration processor is informed of this condition and skips this substitution. Should all other substitutions fail to correct the failure, the skipped element is identified as failed. From this discussion it can be observed that this approach to iterative deduction enjoys its greatest utility when used on maintained principal systems.

The noncontinuous verification approach differs from the continuous in one important respect: the off-line elements are not independently verified. Verification of the group is still

*It is important to note that this process is based on the principle of single instances of failure. If the iteration time is short, typically within minutes, this assumption is valid.

based on the group on-line output but periodically the group must be released from its operating function while off-line elements are sequentially switched into the on-line stream for verification. By using a technique which will switch in one new element of each set for each output observation, (i.e., each new observation constitutes a completely different collection of off-line elements) redundancy verification can be accomplished quite rapidly if no unsatisfactory condition is indicated in the process. For then, the number of system configurations for observation will be a minimum. However, if an unsatisfactory output is observed for one or more of the configurations, the only information gained is that some one element which is on line in that configuration is bad. A switching sequence must then be undertaken to identify the faulty element and, even though an optimum sequence can probably be developed, the location of the culprit will usually be time consuming.

If the design confidence requirements are such that the input for verification must be varied over some range in frequency, amplitude, etc., the necessity of doing this in all the different system configurations could be a lengthy procedure.

Iterative deduction must fail to match exhaustive deduction in the degree of comprehensiveness attainable. It would be unreasonable to expect to gain as much information on an element buried within a group from, say, a spectral analysis of the group output as could be gained from a similar analysis of the element's output.

Iterative deduction will require knowledge of group input status, at the least, to allow status resolution.

This approach will be economical in the use of equipment performing the five basic functions of verification, since the only signal observation will be made at the group output. The degree of command and control equipment used for this approach will exceed that required for most exhaustive implementations, however. Logical deduction would be expected to use less command and control equipment but more observation equipment than would iterative deduction.

When design confidence demands that a simulative signal be used to exercise an element, the ability to employ iterative deduction will depend on accessibility of the point at which the signal will be injected. Consider that the group under scrutiny will have as its output that signal(s) under observation. Its input, though, may be located earlier in the signal path than is the signal injection point and sequential switching may occur between input and injection points. As an example, consider simple sets 1.1 and 1.2 of Figure 5.1.3 to be a group for verification and assume that it is necessary to exercise the elements of simple set 1.2. The concept of iterative deduction would be compatible with the need for exercising if the switching of simple set 1.1 were such that all elements of that set could be switched out simultaneously.

If it happens that elements are designed to give a second, isolated output for the purpose of verification, this second output will not be useful for iterative deduction, since the output used for the verification of an element must pass through succeeding elements if this

approach is to be used. The one exception is for a simple set whose output is the output of the group.

The danger of a tolerance buildup going undetected is not present as it may be in an exhaustive arrangement using output/input comparisons on each set.

The occurrence of a majority voting set within a group should usually be handled by some means other than iterative deduction; in fact, exhaustive deduction will be the best choice.

5.2.3.3 Logical Deduction

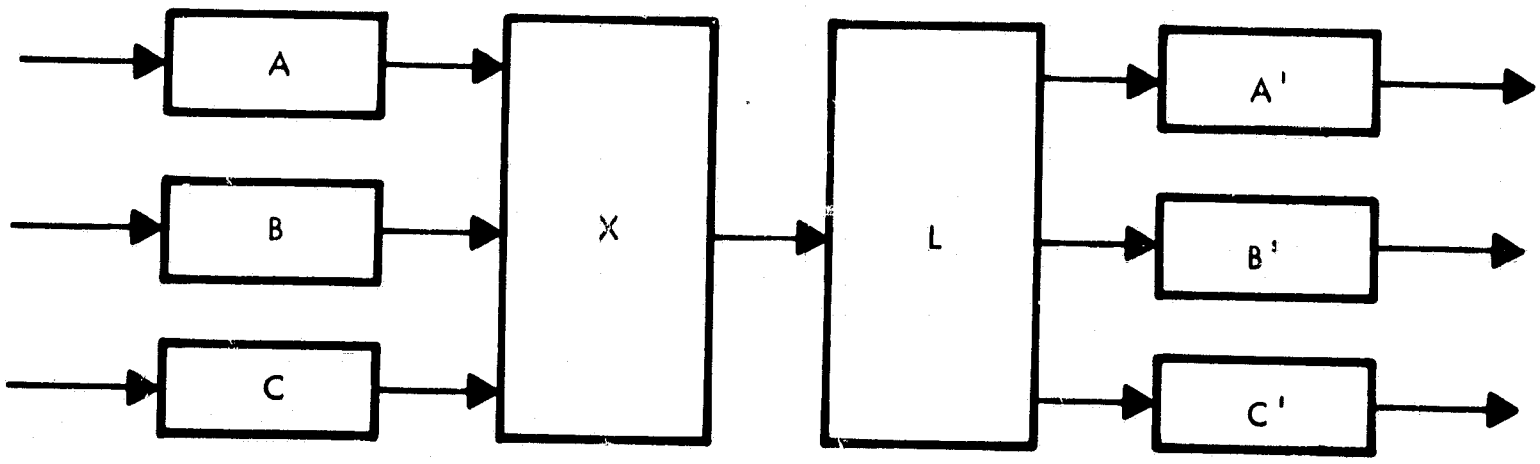
The concept of logical deduction, when applied to redundancy verification, implies the use of knowledge concerning system configuration and signal flow to minimize the number of points which must be observed to deduce status. We are then talking about deriving a maximum amount of status information by intelligently choosing a minimum number of observation points. A simple example is in order. Consider Figure 5.2.3.3 where the input at A' corresponds uniquely to the output at A, B' to B, and C' to C. Suppose, then that an "unsatisfactory" output was observed at A' while outputs at B' and C' looked good. A logical conclusion might be that box A is at fault, since any failure in X or L would have shown up at B' or C'. (We must be willing to make such an assumption in this example.)

The one general statement which can easily be made concerning logical deduction is that it will, to the utmost, be specialized to the equipment it is designed to verify. The advantages gained in reducing the number of observation points and the attendant reductions in observing equipment will be traded off against loss in flexibility. If logical deduction is chosen for extensive use in a complex system, any change in system configuration could lead to the major revision, probably in both hardware and software areas of the verification scheme.

The "exercising" of elements will not necessarily be complicated by the use of logical deduction. The only important consideration will be whether points for signal injection remain accessible.

The complexity of a logical deduction system will vary strongly with the complexity of the group to be verified, though sometimes this complexity may appear entirely in the software portion of the system.

The amount of switching required by a logical deduction approach will be less than that required by iterative deduction. A comparison of switching requirements between the logical and exhaustive techniques is not possible since exhaustive techniques may be achieved with no switching at all or may involve a great deal of switching. Certainly any switching activity in a logical deduction scheme must be well coordinated. This is in contrast to the case for some imaginable exhaustive deduction implementations.



85647-74

Figure 5.2.3.3. Logical Deduction - An Illustrative Example

The time required for a complete verification process under logical deduction will be less, in some cases far less, than that required by iterative deduction. Exhaustive deduction schemes may be made faster than those employing logical deduction, though equipment sharing and the necessity of switching to obtain distinguishable element outputs may result in the exhaustive scheme being slower.

Logical deduction will not evidence the same ease of status resolution that may be realized by using other than monitor methods in an exhaustive deduction implementation. In practice, combinations of exhaustive and logical deduction will be common. It would be prudent to exploit logical deduction to its fullest and use exhaustive deduction to resolve any remaining ambiguities.

No coincidence development technique may be ruled out for use with a logical deduction scheme, but element output would have to be observable at the output side of the group if Compare Two and Voting were to be used. Monitor methods are by far the most likely candidates for use here.

If a majority voting (for the achievement of redundancy or error correction) set appeared within a group and the element outputs were neither accessible nor switchable/ logical deduction would be at a loss.

5.3 Other Design Considerations

In addition to the areas discussed earlier as design inputs, the final determination of verification equipment configuration must consider the important areas of the need for continuous verification, the requirement of dedicating equipment to verification, and the implications of sharing verification devices.

5.3.1 Continuous Verification and the Dedication of Equipment to Verification

In some imaginable redundant configurations, the desire to achieve continuous redundancy verification may be stymied by the inability of the tenant signal to "exercise" the redundant elements to the extent necessary for the establishment of design confidence. The same impasse may be reached if the tenant signal "exercises" the elements on an occasional basis but without the assurance that the period between these occasions will be sufficiently small. As one example, the verification of a diode would undoubtedly require the back-biasing of that device. Unless this condition resulted under the influence of the tenant signal and with reasonable frequency, it would be necessary to provide a signal, simulative or idle, to perform the exercising. One might consider also an audio amplifier in a communications link as a redundant element. A requirement for design confidence here could well be a minimum signal distortion for a signal of given bandwidth. If the tenant signal lacked sufficient bandwidth to exercise the amplifier there would again arise the necessity of providing a signal.

An important point to keep in mind is that the use of simulative, idle, or symbiotic signals may facilitate status resolution, the presumption being that the status of the injected signal will be known.

The importance of exercising redundant equipment is one to be carefully evaluated by the designer. The tradeoff between the loss of flexibility and comprehensiveness implied by a requirement for continuous verification and a sacrifice in system confidence because of noncontinuous verification has been addressed by questioning the quantitative relationship between system confidence and the period between verifications.

As a first approach, consider the case where the set will succeed in its mission if at least one of its elements succeeds.

For the sake of simplicity, it is assumed that the elements are capable of taking on two states during the time required to operate; a failed state and a success state. Intermittent failures are not considered which precludes transitions from a failed state to a success state. If the probability of the i^{th} element working is P_i then the probability of the n element set working is:

$$P_s = 1 - \prod_{i=1}^{n} (1 - P_i) \qquad (5.3.1\text{-}1)$$

when the elements are statistically independent.

Through verification the set can be inspected at predetermined points in time which has the effect of producing time intervals in which the set must operate without observation. In the normal operation of systems, care is taken to avoid failures due to wearout, hence, it is reasonable to assume that wearout will not be a cause of set element failure. Each element in the set is modelled as following an exponential failure law. The exponential model allows for ease in mathematical tractability and is not a requirement imposed upon the elements. Then in the exponential case $P_i = e^{-T/M_i}$ for each element in the time interval of length T, where M_i is the MTBF of the i^{th} element.

A measure of risk can be associated with sets in the following way. Let α be the risk that one is willing to assume that the set will fail in T, or, stated conversely $1-\alpha$ is the probability that a set will work in the time interval T. It is therefore necessary that the following relation holds:

$$P_s = 1-\alpha \qquad (5.3.1\text{-}2)$$

where P_s is defined by Equation 5.3.1-1 and α is the acceptable risk or an acceptable value for the probability of set failure in the time interval T. Using Equation (5.3.1-1) and the exponential model for each element, Equation (5.3.1-2) becomes:

$$1 - \prod_{i=1}^{n} (1 - e^{-T/M_i}) = 1-\alpha \qquad (5.3.1\text{-}3)$$

Under the condition of identical elements $M_e = M_1 = M_2 = \ldots = M_n$, Equation 5.3.1-3 becomes

$$1 - (1 - e^{-T/M_e})^n = 1-\alpha \qquad (5.3.1\text{-}4)$$

where M_e is the MTBF of an individual element of the simple set consisting of n elements. The next step is to investigate simple sets and their behavior under some values of acceptable risk. In essence this amounts to fixing α and the number of elements in the set (n) and solving Equation 5.3.1-4 for the ratio T/M_e. One, two and three element sets were investigated with $\alpha = .01$, .05 and .10. Equation 5.3.1-4 then becomes:

$$e^{-T/M_e} = 1-\alpha;\ n=1 \qquad (5.3.1\text{-}5)$$

$$2e^{-T/M_e} - e^{-2T/M_e} = 1-\alpha;\ n=2 \qquad (5.3.1\text{-}6)$$

$$3e^{-T/M_e} - 3e^{-2T/M_e} + e^{-3T/M_e} = 1-\alpha;\ n=3 \qquad (5.3.1\text{-}7)$$

Figures 5.3.1-1 through 5.3.1-3 graphically depict Equations (5.3.1-5) through (5.3.1-7) for $\alpha = .01$, .05 and .10.

Figure 5.3.1-1, for instance, shows that if one is willing to accept a risk of $\alpha = .10$, then any single element set with M_e on the line marked $1-\alpha = .90$ presents the same risk provided that T is chosen as indicated. For $M_e = 200$ hours one would have to set T = 20 hours for $1-\alpha = .90$ (i.e., $\alpha = .10$) and for $M_e = 150$ hours, T must be equal to 15 hours for $\alpha = .10$.

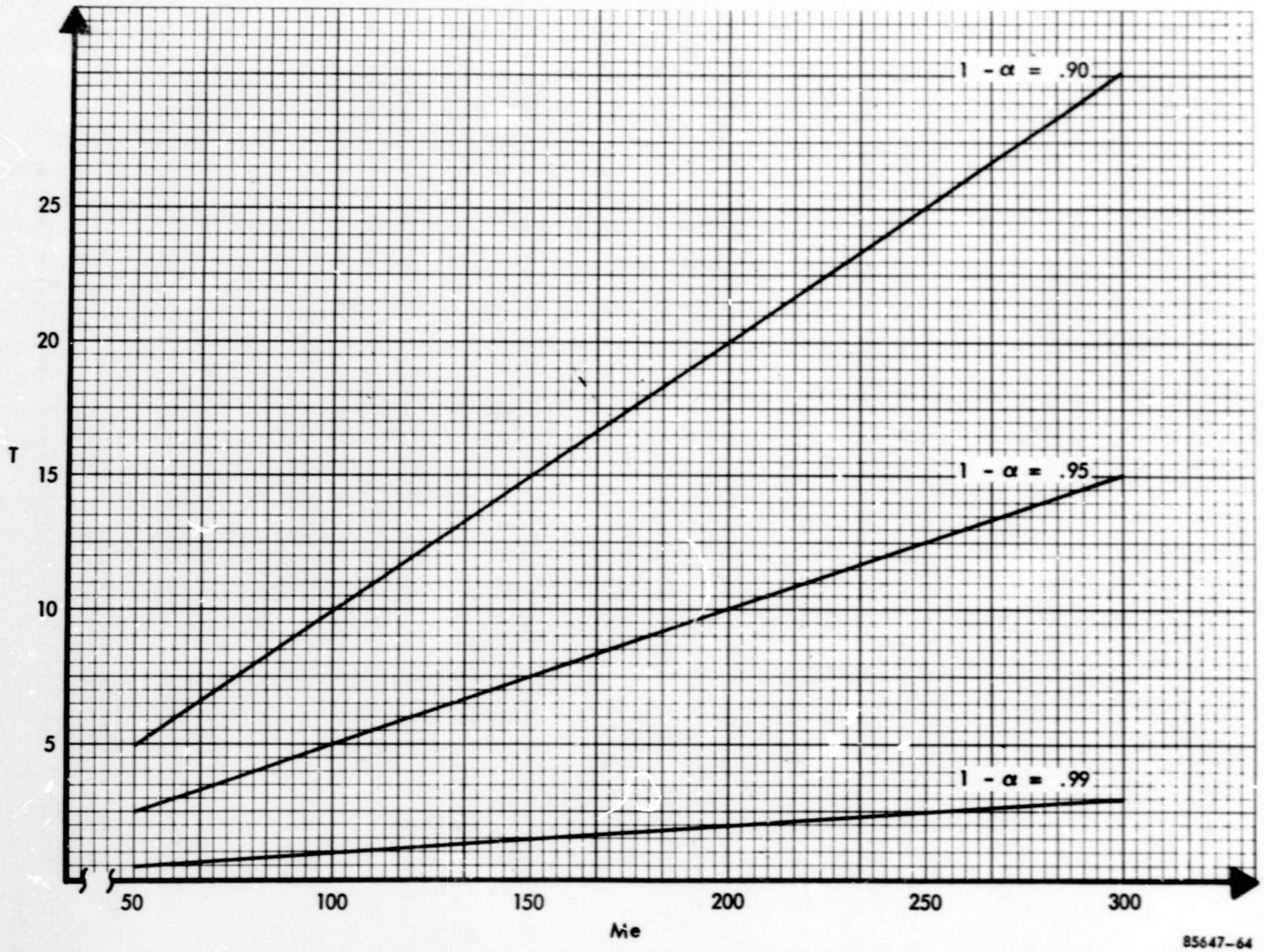


Figure 5.3.1-1. Single Element Sets Lines of Equal Probability

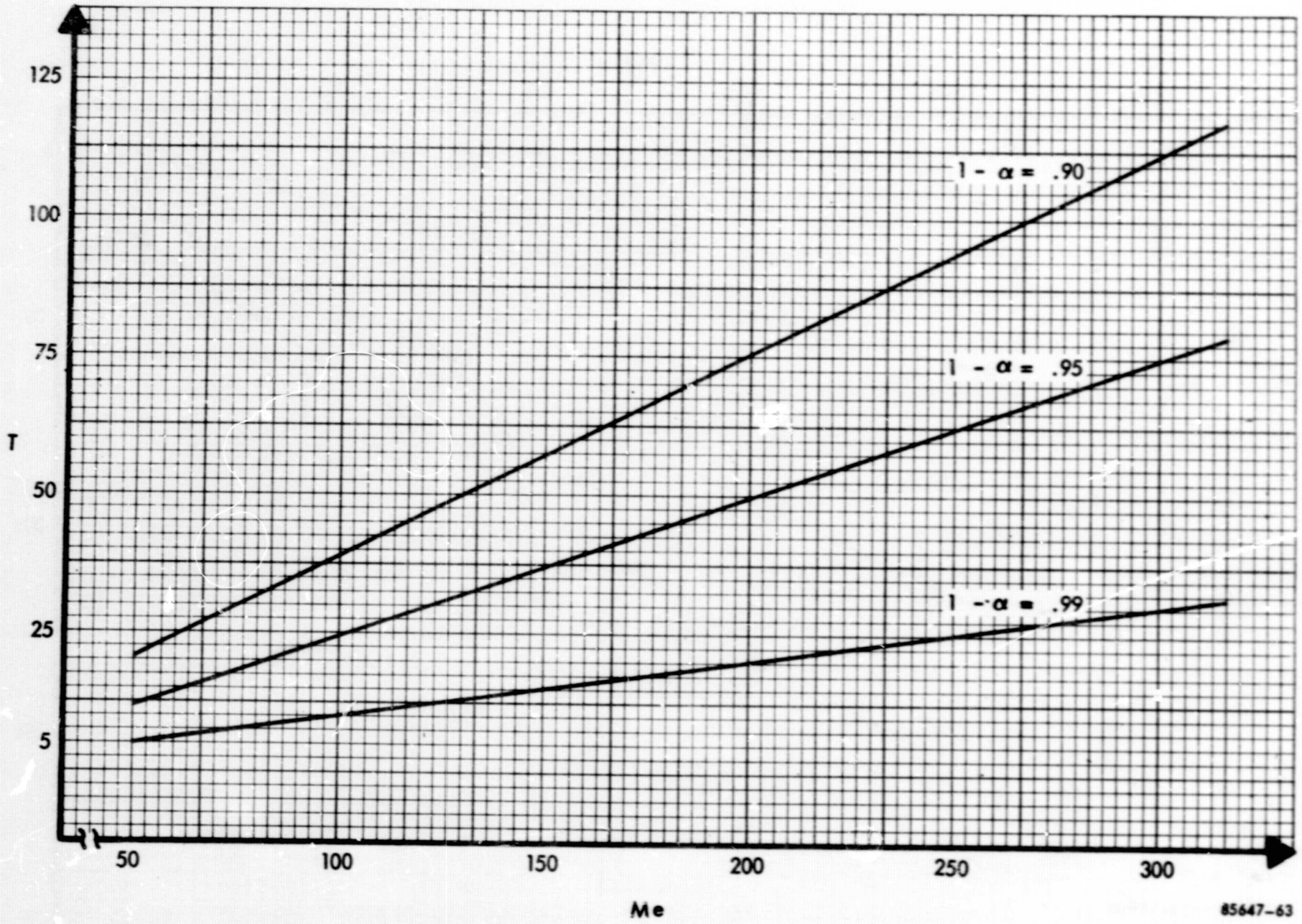


Figure 5.3.1-2. Two Element Simple Sets Lines of Equal Probability (II)

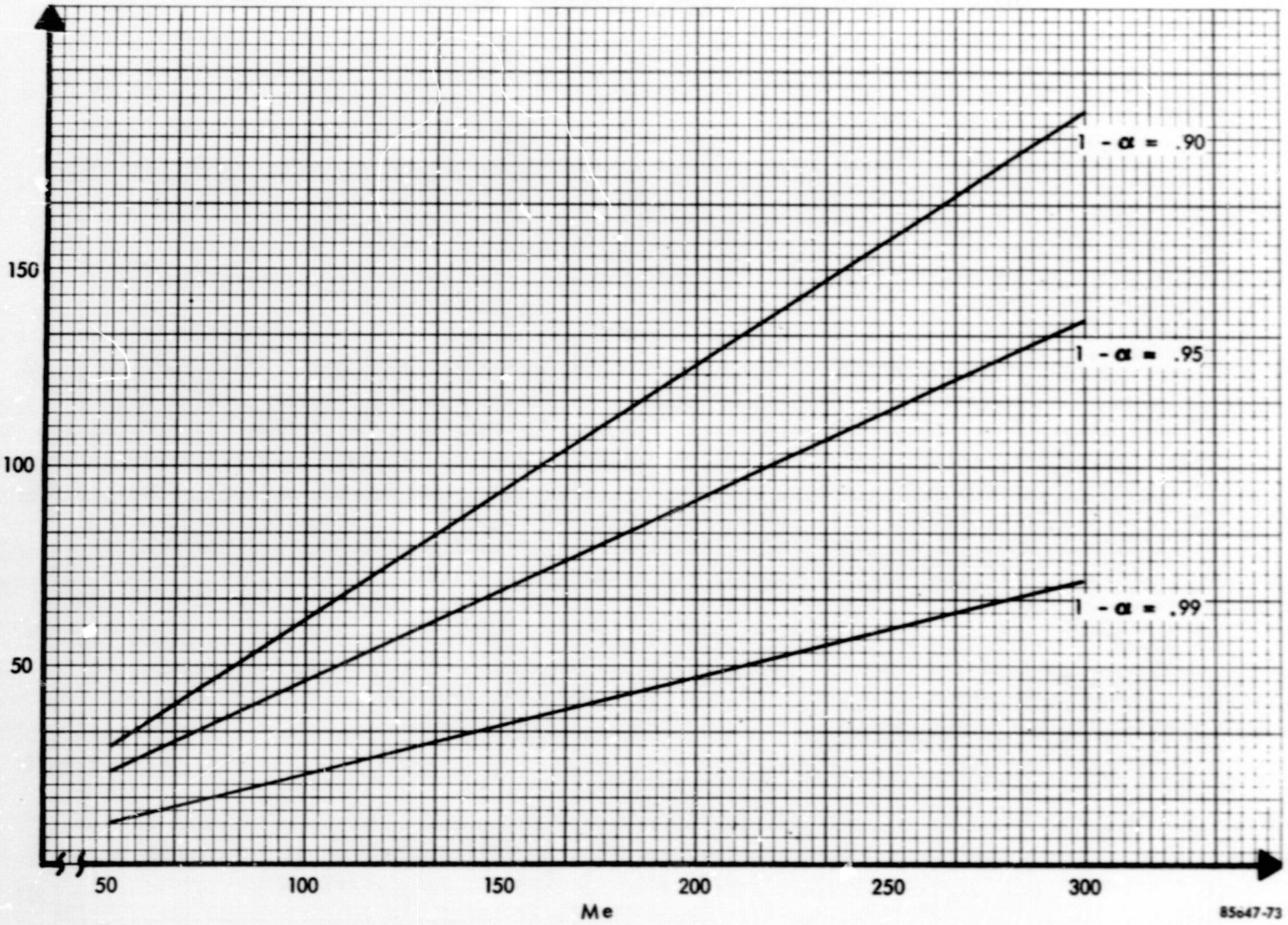


Figure 5.3.1-3. Three Element Simple Sets Lines of Equal Probability (III)

If T is known and α is fixed, then it is a simple matter to determine the M_e which must be met. An example would be when T = 25 hours and α = .10, then one would need to select a M_e = 250 hours. In the case of a fixed M_e, one would have to adjust T accordingly each time α was changed.

To decrease the risk α from .10 to .01 it would be necessary to decrease T from 25 to 2.5 hours for M_e = 250 as seen from Figure 5.3.1-1.

Figure 5.3.1-2 provides for similar observations but represents a two element simple set. For M_e = 200 hours and α = .10 then T must be equal to 75 hours. Said in a different manner, a two element set with the MTBF of an individual element equal to 200 hours, will have a probability of failing equal to .10 for a time interval of 75 hours. To decrease the risk to .01 for M_e = 200 hours it is necessary to decrease T from 75 hours to 20 hours.

Figure 5.3.1-3 represents a three element set and can be used in the same manner as Figures 5.3.1-1 and 5.3.1-2.

The figures can be used as vehicles for performing various tradeoffs such as acceptable risks versus time intervals in which the set musr operate unobserved (T).

Since three elements can be arranged in such a manner as to result in other requirements of element success for the assurance of set success, it is constructive to investigate the behavior of a majority vote set. A majority vote set is defined to consist of three equal elements (i.e., $M_e = M_1 = M_2 = M_3$) such that the set will succeed if at least two of three elements succeed; the assumption being that the voter is perfectly reliable. Mathematically, for statistically independent elements:

$$P_s = \sum_{k=2}^{3} \binom{3}{k} p^k (1-p)^{3-k}. \qquad (5.3.1\text{-}8)$$

Introducing α in the same manner as before and setting $P = e^{-T/M_e}$, Equation (5.3.1-8) becomes

$$P_s = 3e^{-2T/M_e} - 2e^{-3T/M_e} \qquad (5.3.1\text{-}9)$$

where P_s is the probability that the majority vote set will succeed in the time interval T. Figure 5.3.1-4 is a graph of Equation (5.3.1-9) for α = .10, .05 and .01 as a function of T and M_e. Figure 5.3.1-4 can be used in the same manner as Figures 5.3.1-1 through 5.3.1-3. For example, assume that α = .05 (1-α = .95) and that it is known that T must be 20 hours then a majority vote set must be selected such that M_e equals 140 hours.

Comparisons of sets for which the success of a single element means set success and the three element majority vote (MV) set are presented in Figures 5.3.1-5 through 5.3.1-7. Note that the MV set lies between the one and two element parallel sets. The figures can be used to compare or decide on the proper set configuration for a given α and M_e in the following way: Let α = .10 (Figure 5.3.1-5 is used since 1-α = .90) and M_e = 200 hours then T must be

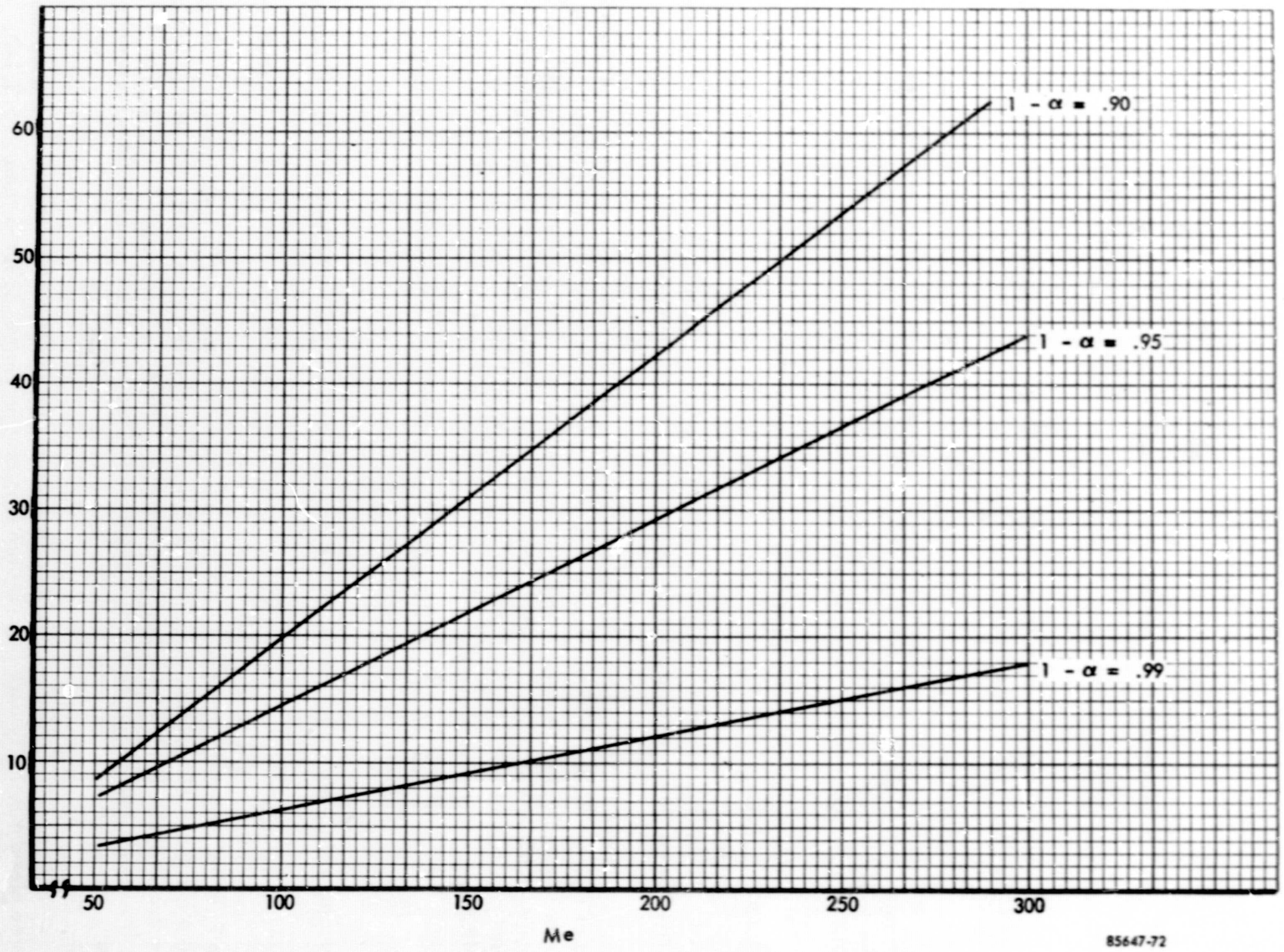


Figure 5.3.1-4. Majority Vote Set 2 out of 3 (MV) Lines of Equal Probability (MV)

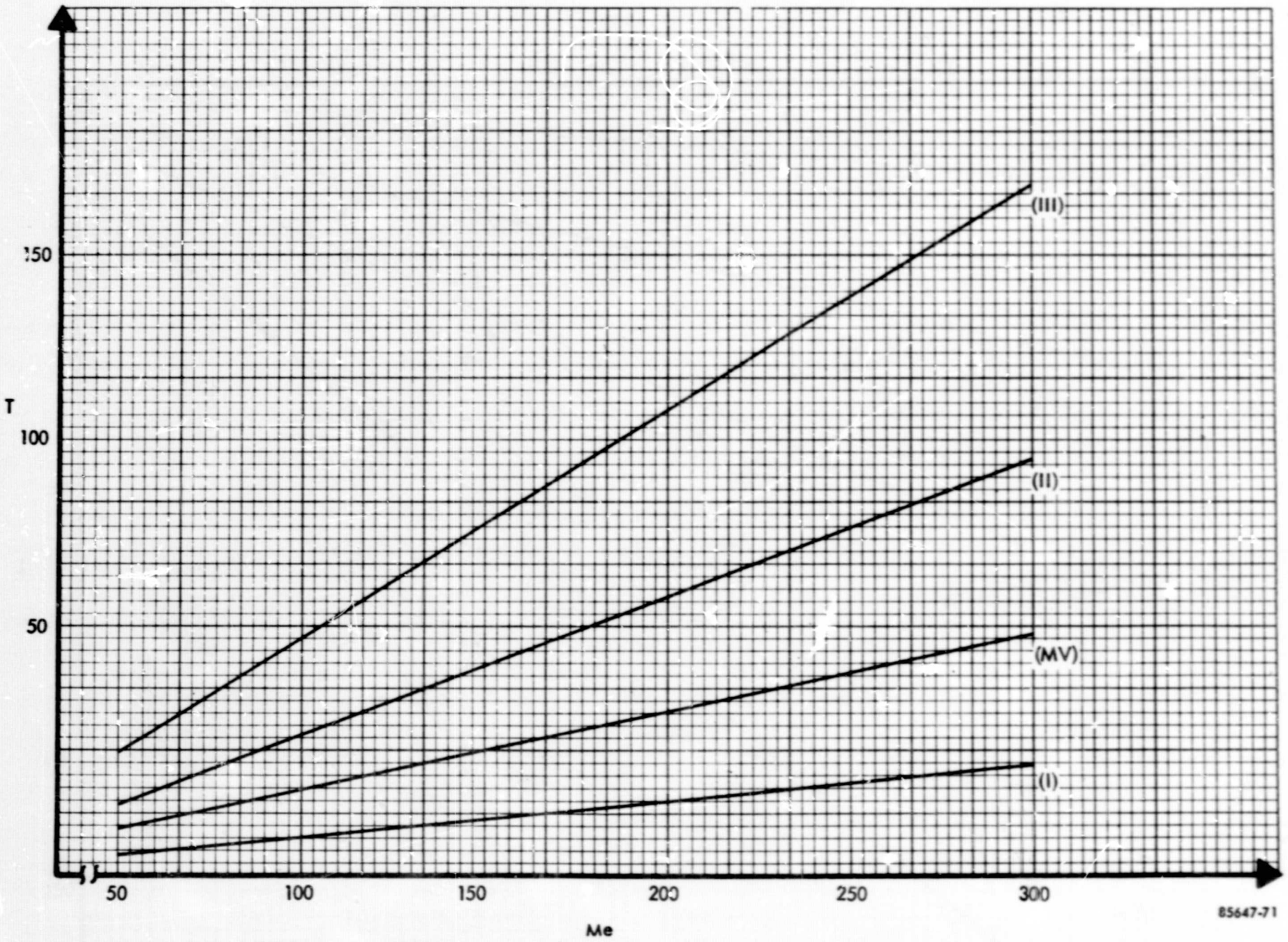
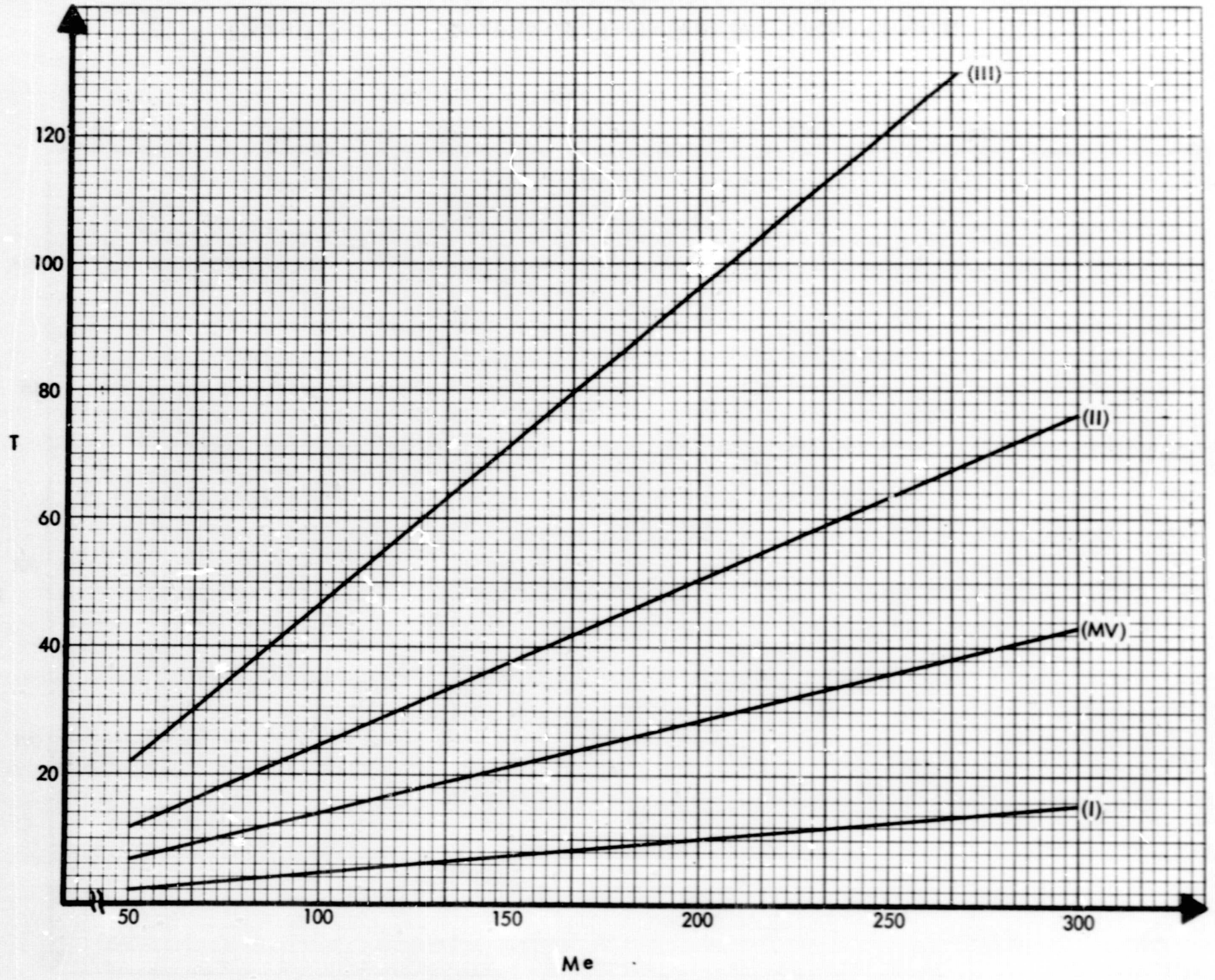


Figure 5.3.1-5. Comparison of Simple Sets; Two Success Criteria. Lines of Equal Probability $1 - \alpha = .90$



85647-70

Figure 5.3.1-6. Comparison of Simple Sets; Two Success Criteria
Lines of Equal Probability $1-\alpha =$,

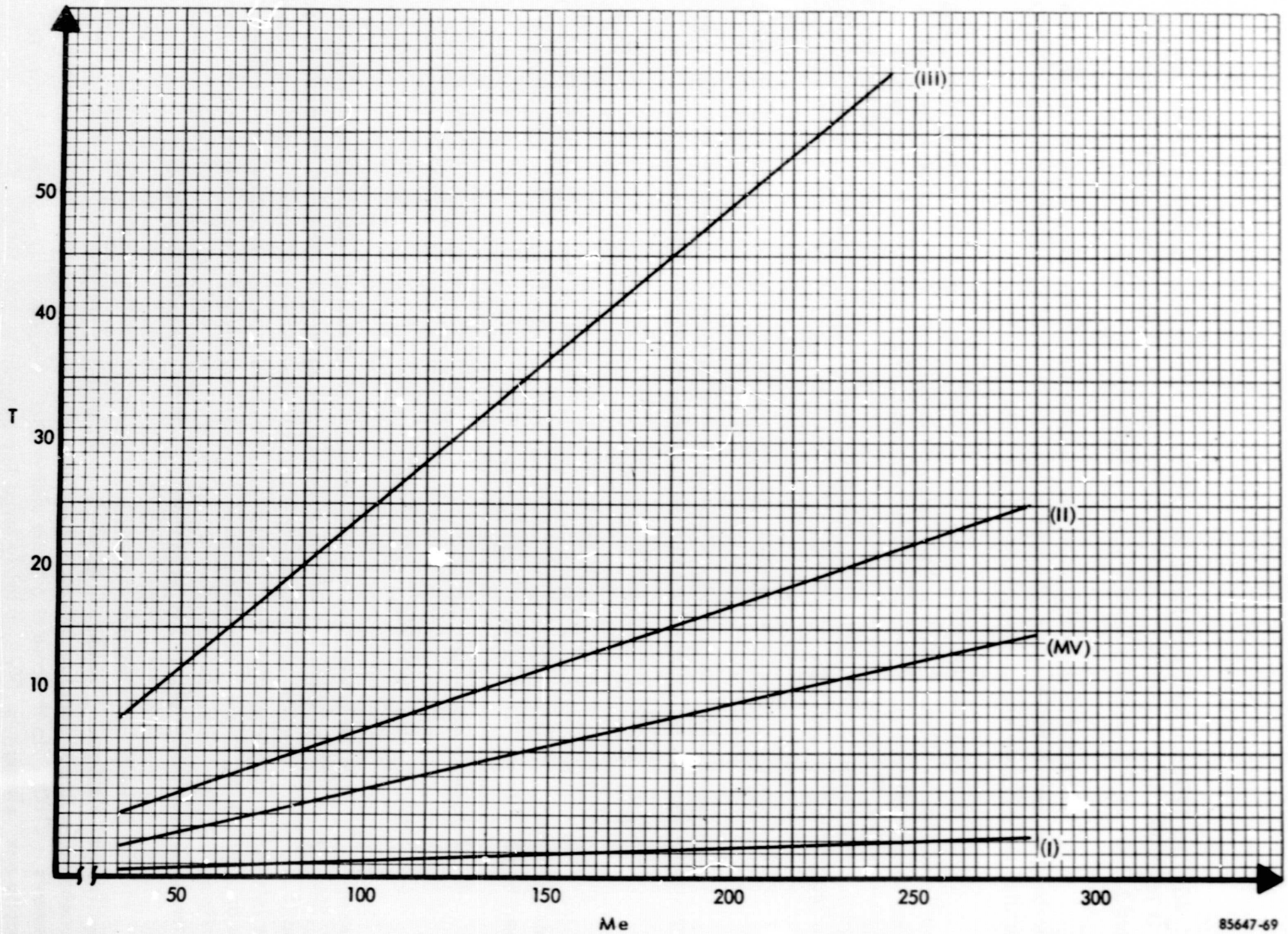


Figure 5.3.1-7. Comparison of Simple Sets; Two Success Criteria.
Lines of Equal Probability $1-\alpha = .99$

20, 45, 75 or 125 hours for one element, majority vote, two-element or three-element sets. Hence, if it is known that T is greater than 50 hours but less than 100, at least a two element set must be used to provide the desired probability of success for the interval T.

While the designation of α leads to determining the probability of set success in T, another pertinent question arises concerning the time interval T. What is the probability that the parallel set will lose all but one element in the interval T?*

This question will be of particular interest when loss of redundancy during a mission could result in an abort. If this is the mission philosophy, the first reaction is to stipulate continuous verification so that the user may be alarmed to the fact that he has lost one (for first degree) or two (for second degree) elements. However, if it should happen that periodic verification can establish a sufficiently low likelihood that a redundant set will degrade to this point, the requirement for continuous verification may be relaxed.

Two sets are of interest here, namely the three-element and the two-element sets.

Consider the three-element case where all elements are operating at the start of the interval T, then according to the set and element models defined previously.

$$P\,(2\,|\,3;\,P) = 3(1-e^{-T/M_e})^2(e^{-T/M_e}) \qquad (5.3.1\text{-}10)$$

where $P = e^{-T/M_e}$ and $P(2\,|\,3;\,P)$ gives the probability of two of three elements failing in the time interval T, or the probability that the three-element set will have only one element operating in the time interval T.

In the two element set:

$$P(1\,|\,2,\,P) = 2e^{-T/M_e}\,(1-e^{-T/M_e}) \qquad (5.3.1\text{-}11)$$

where $P(1\,|\,2,\,P)$ is the probability that one element out of two elements will fail in the interval T. Since $P = e^{-T/M_e}$, then it is sufficient to select a value of P and solve Equations (5.3.1-10) and (5.3.1-11) for the desired probability of being "down to exactly one" operating element in the interval T. Once a value of P is selected, then Figure 5.3.1-1 can be used to determine the appropriate M_e and T. For instance, if P = .95 then any point on the line marked $1-\alpha = .95$ in Figure 5.3.1-1 has a corresponding M_e and T; if M_e is fixed along with P, then T can be determined from the graph, if T is fixed then M_e can be read off the graph.

Table 5.3.1 compares the two and three element sets with respect to being "down to exactly one" element. Consider a two element set with the probability of an individual element succeeding in time T equal to .90 then the probability that the set will lose one out of two elements is .1800. In the case of a three element set, the probability of being "down to exactly one" element is .0270, a fairly large improvement.

* This is equivalent to asking for the probability of exactly one element surviving.

Figures 5.3.1-8 through 5.3.1-11 are graphs of Equations (5.3.1-5) (5.3.1-6), (5.3.1-7) and (5.3.1-9) solved for a range of values on α from .20 to .0001 and some selected values of M_e. These graphs can be used to determine the point at which, for a given M_e, a decreasing T would not be very profitable for the set in question. Figure 5.3.1-10 for example, shows that to go from a risk of .005 to .0001 for $M_e = 300$, T has to decrease from 56 to 14.

More complex situations can be modelled and investigated in a manner similar to that employed here. The mathematics become somewhat more complicated but in general probability bounds can be derived for these complex structures.

For sets which do not have statistically independent elements, bounds can be determined from the probabilities of the individual elements.

Table 5.3.1. Probability of being Down to Exactly One Element for the Two and Three Element Sets

PROBABILITY OF INDIVIDUAL ELEMENT WORKING (P)	PROBABILITY OF BEING DOWN TO EXACTLY ONE ELEMENT	
	TWO ELEMENT SET	THREE ELEMENT SET
.80	03.20×10^{-1}	0.96×10^{-1}
.85	25.25×10^{-2}	5.74×10^{-2}
.90	18.00×10^{-2}	2.70×10^{-2}
.92	14.72×10^{-2}	1.77×10^{-2}
.95	09.50×10^{-2}	0.71×10^{-2}
.99	01.98×10^{-2}	0.03×10^{-2}
.995	09.95×10^{-3}	0.07×10^{-3}
.999	19.98×10^{-4}	0.03×10^{-4}
.9995	99.95×10^{-5}	0.08×10^{-5}
.9999	19.99×10^{-5}	0.003×10^{-5}

Consider a group of sets instead of a single set; then the preceding discussion and approach can be used to arrive at an overall risk or conversely the probability that some member(s) of the group will fail where group success is possible only if all sets work properly.

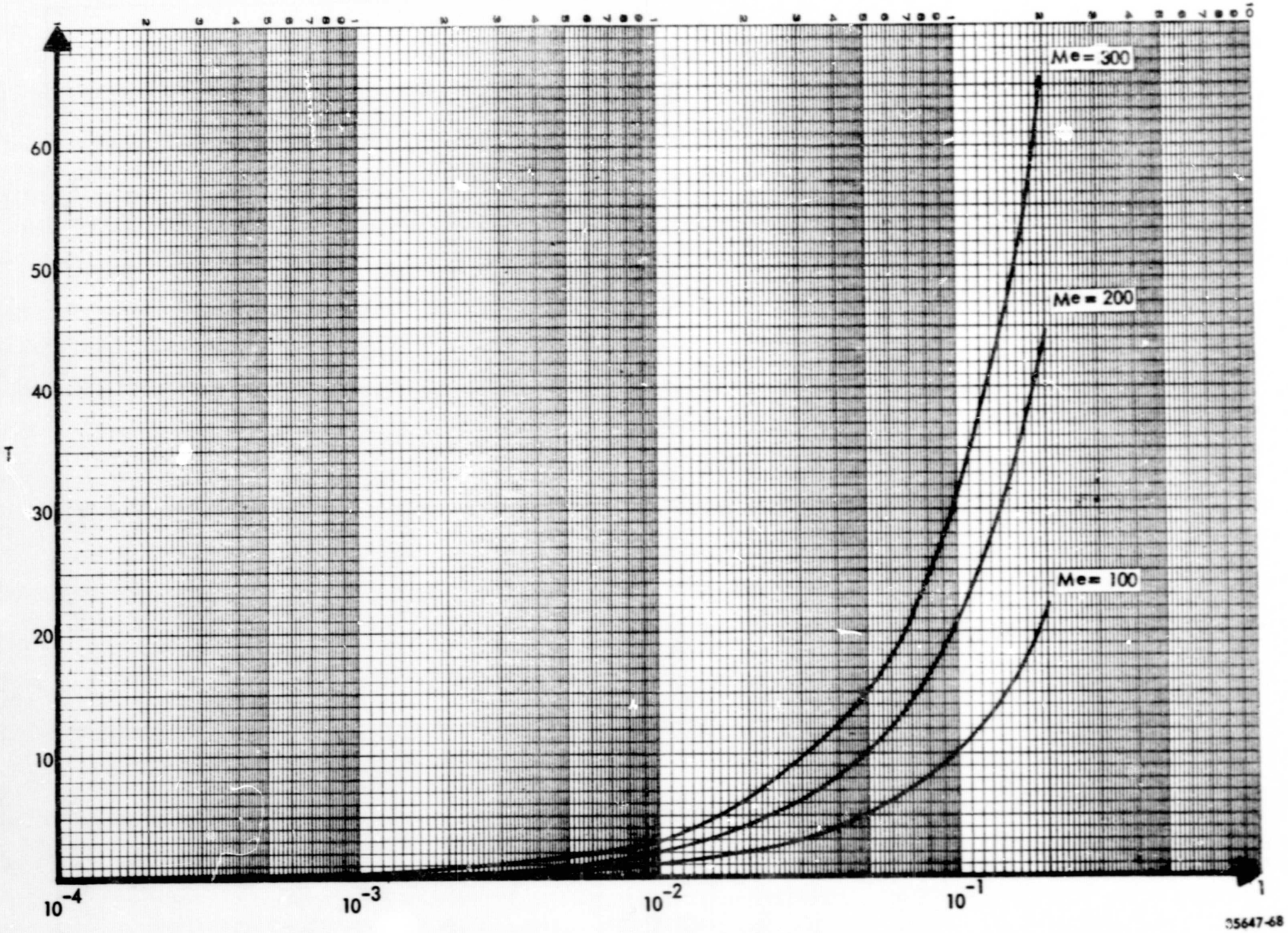


Figure 5.3.1-8. Single Element Set - T vs. Risk (1)

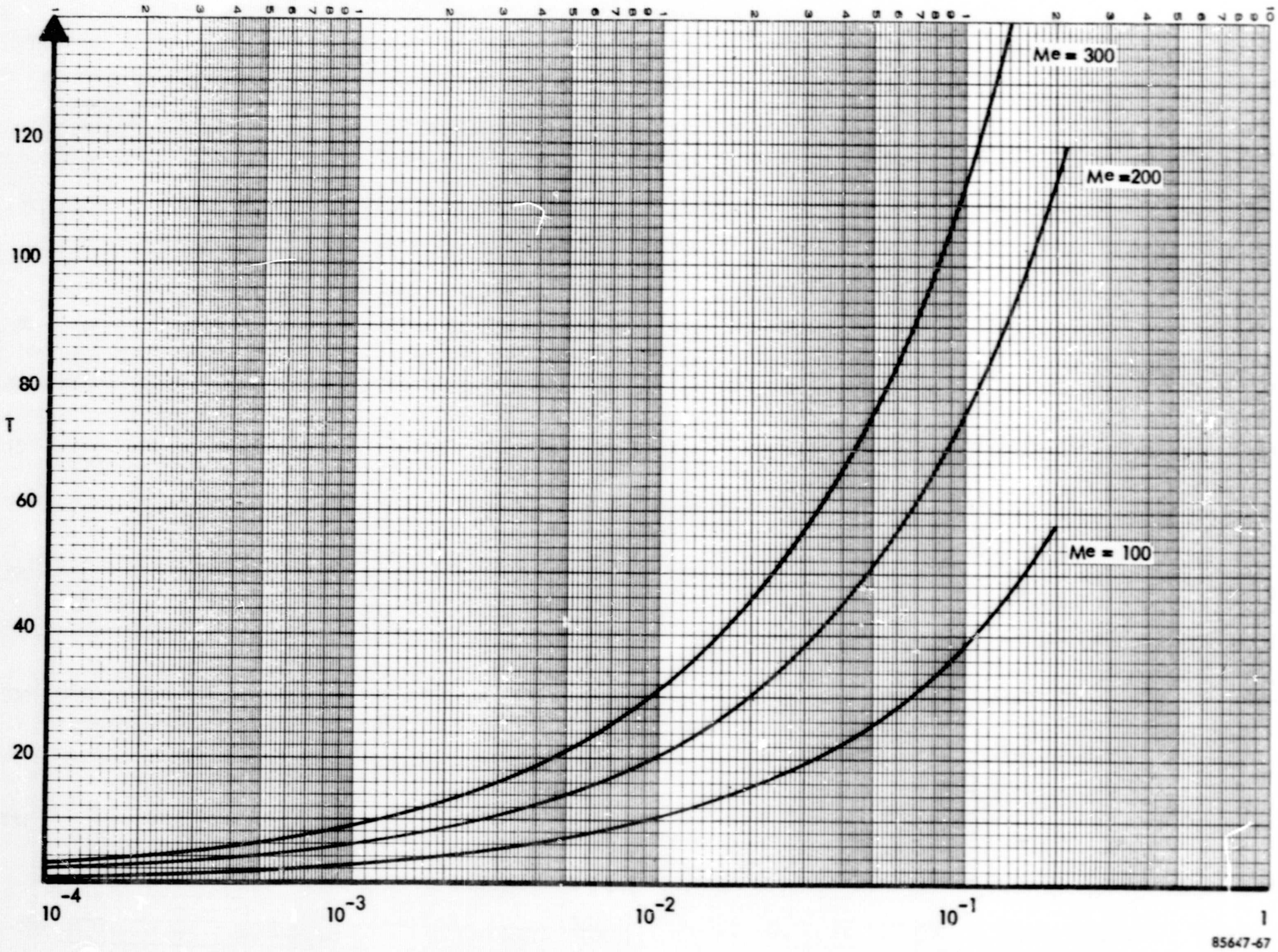


Figure 5.3.1-9. Two Element Simple Set - T vs. Risk (II)

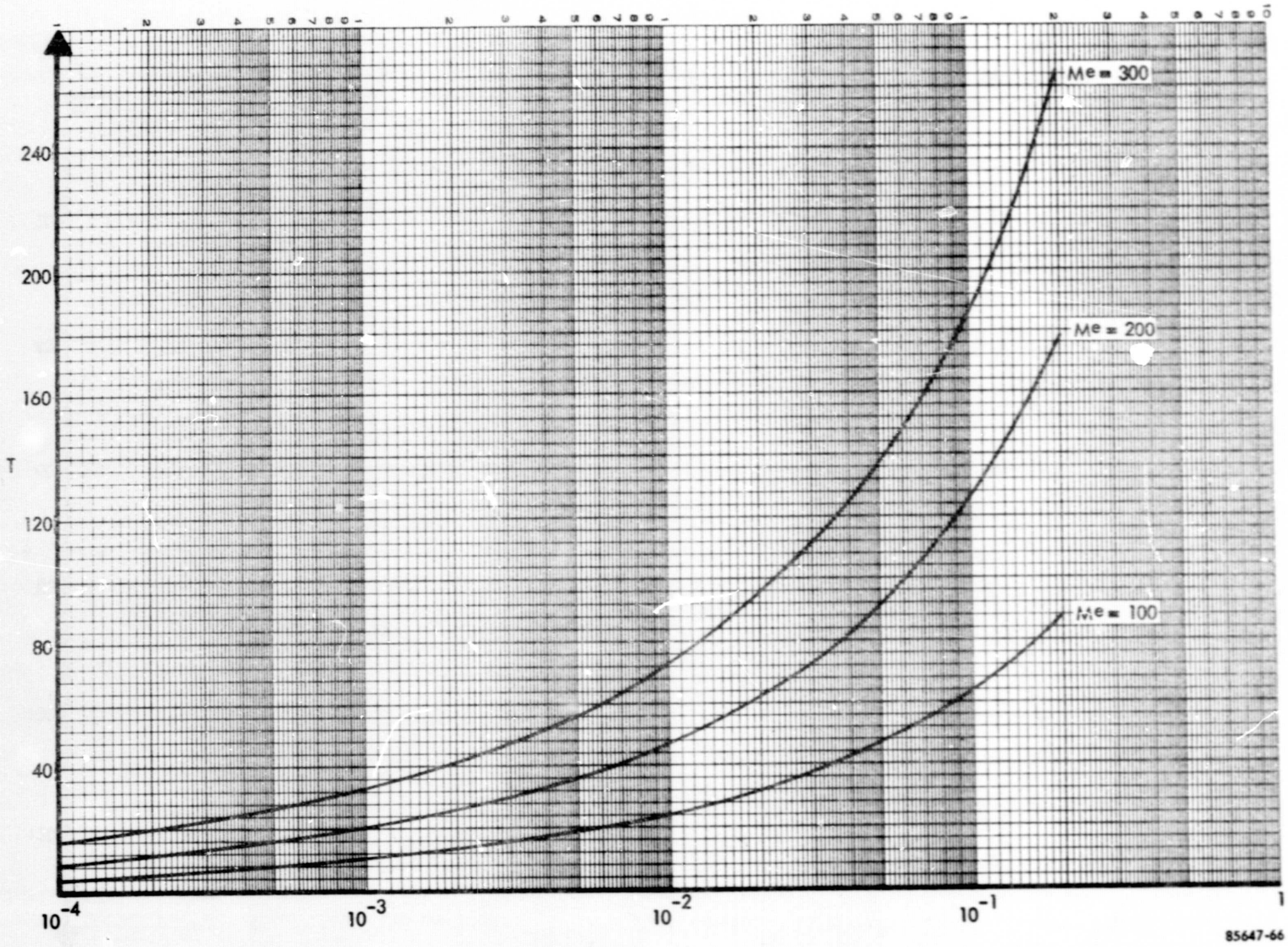


Figure 5.3.1-10. Three Element Simple Set - T vs. Risk (III)

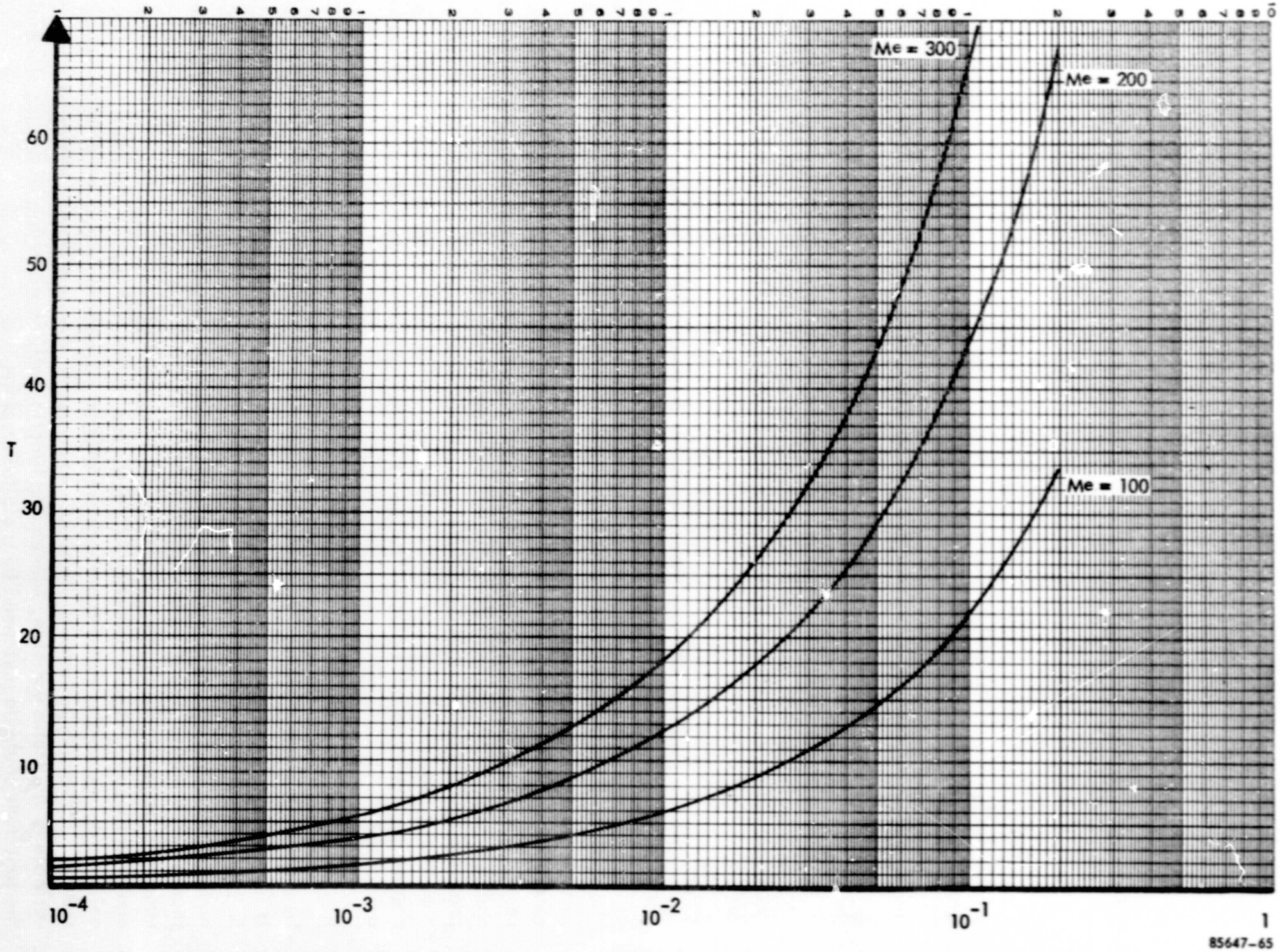


Figure 5.3.1-11. MV Set - T vs. Risk

If the probability of the i^{th} set working is P_{si} then the probability that at least one member of the group failing is:

$$Q_g = 1 - \prod_{i=1}^{n} P_{si} \qquad (5.3.1\text{-}12)$$

where the P_{si} are statistically independent sets. As noted previously, if the members of the group are not statistically independent then bounds would be derived to replace Q_g. Equation (5.3.1-12) in turn gives the overall probability of at least one set failing in a group of N sets and Q_g can be interpreted as the overall group risk.

5.3.2 Implications of Sharing Verification Devices

Because of the cost of implementing some verification methods and because of the possibility of an on-line/off-line situation arising in the achievement of redundancy, it is pertinent to question the implications of sharing verification equipment.

Probably most important to consider is the impact of equipment sharing on time partitioning requirements and design confidence. It could easily arise, with extensive sharing of equipment and automatic command and control of the verification process, that the times between the updates of status of a given set are not frequent enough to satisfy the user. This is particularly likely to happen if a central processing function is handling numerous verification inputs on a priority-interrupt basis. A point that appears here is that conditional status determination requires the simultaneous presence of the proper signal and the proper equipment. Status resolution may have to await other information such as the status or conditional status of preceeding equipment. It is the specified maximum times between completions of this process that must be satisfactory to the user. In terms of verification equipment, this requires a certain degree of rapidity in the status resolution function as well as an avoidance of oversharing equipment.

In the question of which of the verification functions may be shared, it is found to be a good rule that the closer the function is to the equipment being verified, the less sharable it is. This is an extension of a point made in the discussions of Appendix A and in Section 5.2.2. For most of the coincidence development techniques a degree of specialization to the equipment being verified is mandatory. The characteristics of each technique with regard to sharability are discussed in Appendix A, but it is clear at first glance that verification equipment will be restricted in the type and range of signal that it can handle. It is not likely that equipment would compare two sets of signals, one in the 100v range and the other in the millivolt range. Parameter estimation functions will be more sharable and mapping functions still more so. Naturally, wherever digitization occurs, on the signal being observed, the coincidence variable or the status variable, succeeding function will be amenable to sharing since almost all the functions could be performed by a digital machine.

Wherever time-sharing is used the deletion of equipment to perform the basic functions will be traded off for command and control implementations. If the rule-of-thumb is

accepted that the cost and complexity of command and control equipment should not exceed that of the equipment it is deleting, it is obvious that the sharing of the more complicated functions is most attractive.

A tradeoff between the sharability of a particular piece of verification equipment and accuracy is likely to arise. The designer may well be tempted to "open up" a function in order to allow its sharing among a larger set of preceeding functions. It should be borne in mind that this will probably affect the accuracy of verification and a careful assessment must be made of the implications.

The proper approach to the design of a sharing verification system will be to identify the points in the principal system from which information for verification will be drawn and outline the functions to be performed on the extracted information. The set of functions to be performed may then be partitioned into groups which have similar outputs; coincidence variables of the same form, status variables of the same form, etc. These groups then identify where sharing can begin.

After the decisions have been made concerning which functions are to be shared, several areas must be considered in the design of verification equipment to be shared. The output of the shared equipment must be inhibited during switching to avoid an output which may be interpreted by succeeding equipment as an inference of operational integrity. In digital implementations, this is likely to be less of a problem than in analog implementations, since data can be "clocked out" in an orderly fashion and is not required to have a real-time relationship with the input.

Verification equipment must not overload, saturate, or drift excessively during switchover. This consideration will in some instances require the provision to the verification equipment of dummy loads or signals, remembering that for large-scale sharing systems the duty cycle on a particular piece of equipment may be low.

The sharing of verification equipment must never disturb the characteristics of a tenant signal when such a signal is being used for verification. Furthermore, if simulative, symbiotic or idle signals are to be used "downstream" in a system verification problem, any effect on these signals of switching verification equipment will complicate the status resolution of succeeding equipment.

Time-shared equipment must not provide the means for crosstalk between different portions of the system.

Means for identifying information sources must be provided. This may be done either by tagging the information itself or by obtaining routing information from the command and control equipment.

5.4 Relationships To a Central Processor and Existing Ace Techniques

The intent of this section is to present the general role which a digital processor may play in an automated redundancy verification scheme and to briefly discuss the relatedness and applicability of automatic checkout equipment (ACE) techniques as applied to complex electronic/electromechanical systems.

Since the exact configuration and characteristics of a futuristic complex system can only at best be surmised, a well defined set of guidelines for definitizing processor design and function is beyond the scope of this report. However, this does not preclude a generalized treatment of the universal problem. To this end, an introductory paragraph is presented to establish some considerations that are relevant to any application of digital processing equipments in such an environment. Digital processing applicability is discussed to pose certain questions relevant to the system design process. Following this is a brief reiteration of the general functional flow of the redundancy verification process. This is done to maintain logical continuity of the discussion and to lead into further argument. The central processor's role is then discussed relative to four functional configurations of verification processing. The treatment of the central processor is concluded with a paragraph concerned with programming considerations. Finally, existing ACE techniques are discussed to present a related technology which involves techniques similar to those to be encountered in automation of redundancy verification.

5.4.1 Automation Considerations

The role played by a central processor in a complex electronic/electromechanical system is influenced by many factors. Some of the salient factors to be considered are:

- Operational Requirements
- Performance Criteria
- Reliability Criteria
- State-of-the-art Technology
- Digital Data Base Volume and Diversity
- Digital Data Base Acquisition Interface
- Data Transmission Rates and Timing
- Raw Data Formats
- Measurement Timing and Accuracy

- Processing Requirements
- Computational Accuracy
- Data Storage and Recording
- Information Display
- Man/Machine Interface
- System Expandability

The selection or design of any real time digital processor should never be considered before the overall digital processing functions have been determined. Operational requirements, performance criteria and reliability criteria are the cornerstones of the system design process.

The primary factors to be considered in the central processor design are digital data base volume and diversity, data transmission rates and timing, processing requirements, and man/machine interface. These factors when properly evaluated will set the general structural boundaries of the processor design.

5.4.2 Digital Processing Applicability

The applicability of digital processing to the automation (or partial automation) of redundancy verification in a complex electronic/electromechanical system environment is discussed here from the viewpoint of conceptual design considerations. Consider the following questions:

- What is the scope of the automation problem?
- What functions can be accomplished by digital processing?
- What functions can be time shared?
- What functions require central processing?
- Can one central processor handle the total digital processing workload?

To answer these questions in detail could easily result in a study in its own right. They are presented here to remind the reader of the general line of thinking that must be devoted to determination of digital processing applicability in any real time system.

5.4.3 Redundancy Verification Functional Flow

We may summarize the results of Sections 5.2.1.3 and 5.2.2.1 into five functions required for redundancy verification.

1. Coincidence Development
2. Parameter Estimation
3. Mapping and Decision
4. Status Resolution
5. Status Recording and Display

Figure 5.4.3 depicts the functional flow and illustrates this flow from the simple set level to the group level. These concepts have been discussed previously in detail and will not be belabored here. It is necessary at this level of perspective; however, to view the overall process as this is the theme of the following sections.

5.4.4 Central Processing Options

The role of a central processor in the total automated redundancy verification scheme can be determined precisely only by a design process based on a specific system configuration and established operational and performance requirements. But in general, that role can be represented by four candidate system configuration options. Figure 5.4.4 depicts the system configurator for these options. This figure is an extension of the redundancy verification functional flow as shown in Figure 5.4.3. The status resolution function in all four options to be discussed is relegated to the central processor. But before proceeding with discussion of the four options, consider the structure of the configurator and the functions of each of the entities depicted.

The central processor is the focal point of automation. Its function and design can range from a special purpose digital processor with limited arithmetic and input/output capability to a giant computer with multiple environments, extensive instruction repertoire, buffered and multiplexed input/output capability, microprogrammed macro instructions, multiport memory, and many other features. The basic functions to be performed by the central processor are as follows:

- Executive (command, control, sequencing)
- Data Acquisition
- Data Storage and Retrieval

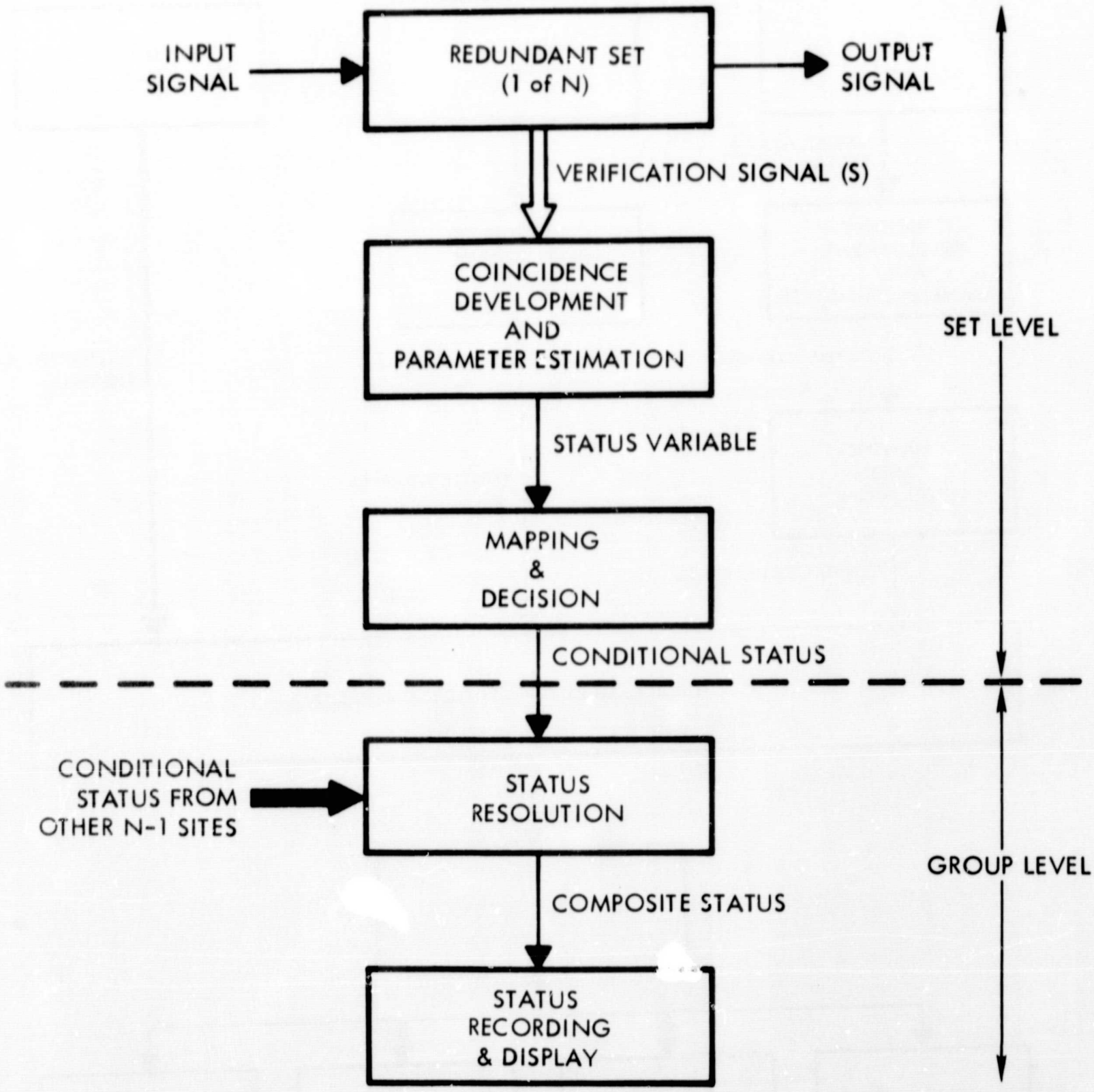


Figure 5.4.3. Redundancy Verification Functional Flow

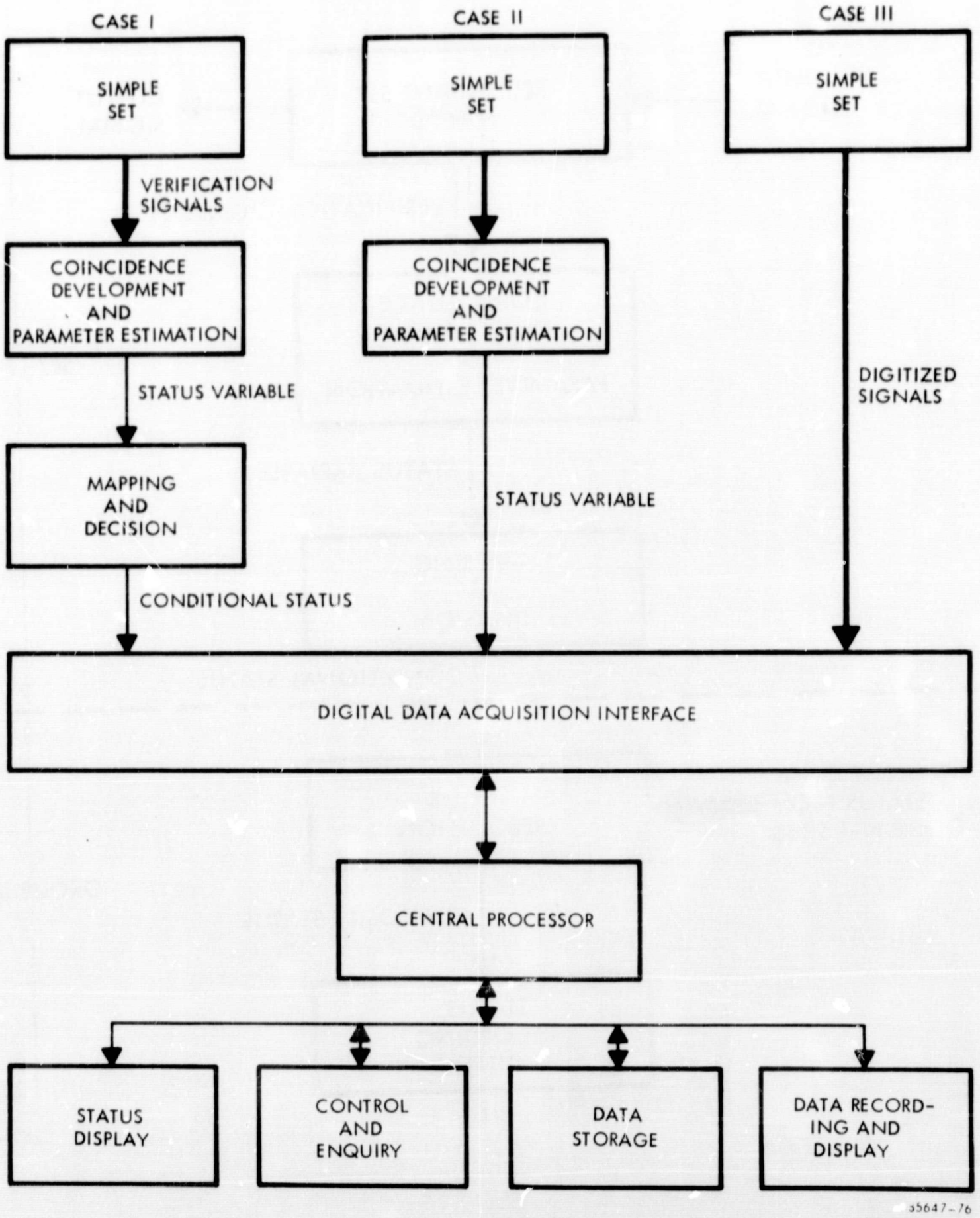


Figure 5.4.4. Central Processing Configuration

- Data Recording and Display
- Processing (mapping, decision, formatting)
- Reporting

The Digital Data Acquisition Interface provides the communications link between the central processor and the special peripheral hardware which performs all necessary verification functions on the principal system.

The interface problem can be divided into three cases (see Figure 5.4.4).

Case I - In this case all signal processing (coincidence development and parameter estimation) and mapping are performed by special purpose equipments. The conditional status for each simple set is presented to the data acquisition interface in digital form. The interface may be comprised of a combination of multiplexed or buffered channels depending on the data rates and volumes to be transferred.

Case II - In this case special purpose peripheral equipment performs the signal processing function. A status variable for each simple set is presented to the data acquisition interface. The form of the status variables may be either analog or digital. All digital inputs will be handled as in Case I. However, analog signals must be digitized and formatted. These digitized quantities may then be handled as in Case I.

Case III - In this case virtually all the verification functions have been relegated to the processor. With few exceptions, all the pertinent tenant signals or transducer signals have been digitized and routed directly to the Acquisition Interface. Under these circumstances, the Acquisition Interface must be capable of handling a wide variety of word lengths, word rates and, if the tenant signals are digital, varying formats.

The Data Storage function provides the mechanism for storing all digital information associated with the redundancy verification process. This includes buffer storage for data acquisition and transmission, program storage for all processing programs, bulk storage for raw data and reference data, and output buffer storage for display data.

The status display function presents in real time the current system redundancy status. The standard elements of the display mechanism are display boards, CRT displays, and aural transducers.

The control and inquiry function allows the operator to communicate with the central processor executive to initiate actions and retrieve information. The standard elements of the control and inquiry mechanism are keyboards, switches, teletypewriters, and CRT terminals.

The data recording and display function provides the mechanism for permanently recording data requested by the operator or as a result of programmed output and for displaying

any data in permanent form output as a result of programming or operator inquiry. The standard units associated with this function are magnetic tape recorders, line printers, stripchart recorders, photographic film, and digital plotters.

It will be instructive to examine each of the above interface cases in the light of the central processor. This is the subject of the following subsections.

5.4.4.1 Case I

This option is defined to be a configuration of functional elements represented by Figure 5.4.4 that requires the central processor to perform status resolution and status recording and display. Signal processing and mapping functions are performed by special peripheral equipment(s) which resolve the verification signals to a conditional status signal and input to a Case I data acquisition interface. The primary processing algorithm is, therefore, concerned with a logical decision process of resolving composite status, an unambiguous statement of system redundancy state. This case places a minimum processing load on the central processor. Computational speed and accuracy will not be a critical factor in selecting a processor for this option. Since most of the data processing is performed external to the central processor the overall data base will be relatively small and will consequently require less storage and produce a minimum load on the input/output channels.

5.4.4.2 Case II

This option is defined to be a configuration like Case I that relegates the Mapping and Decision function into the central processor as well as status resolution and status recording and display functions. This configuration requires a Case II data acquisition interface. The addition of more and different computational requirements on the central processor will require possibly more precision, speed, and instruction types. The increased data base and processing will significantly effect the throughput rate and may require expanded input/output capability. Data storage, recording and display requirements will expand proportionally.

5.4.4.3 Case III

This case represents a quantum leap in central processing requirements. This case requires that all verification signals be inputted directly to a Case III data acquisition interface. The data acquisition and storage problem is compounded by the many types and varied rates of signals to be processed and stored. The signal processing algorithms will be many and time sharing of all processing functions will certainly be necessary for any sizable principal system. This type of requirement could very easily accommodate a large scale multienvironment real time computer system with sophisticated input/output structure mass random access storage and a full blown real time multiprogramming operating system. Large random access storage will probably be necessary to contain the data base and the full complement of processing programs.

5.4.4.4 Case IV

Case IV is an added, compromise option defined to be an optimum combination of Cases I, II and III to take advantage of the good points of each. In reality, Case IV is the most typical. By proper selection of off-the-shelf hardware, many of the signal processing tasks can be accomplished with proven equipment. In other cases, signal processing can be accomplished only through special designs. Still others can be accomplished by direct input to standard multiplexed processing channels in the data acquisition interface. The same holds true for mapping. By judicious system design, the central processor can be reduced substantially from that typically required for Case III implementation.

5.4.5 Programming Considerations

The type of programming encountered in this type of system configuration will be highly specialized real time programming. The size and scope of the programming task is, of course, dependent on the complexity of the central processor and the type of processing to be accomplished. In Section 5.4.4 four central processing options were discussed. Each of these options entails an entirely different configuration of central processor, peripheral equipments, and processing tasks. The total programming task is also influenced by such factors as:

- What off-line processing equipments are available and are they compatible with the on-line system?
- What vendor-supplied system software is directly applicable to the problem?
- What programming aids such as operating systems, compilers, assemblers, emulators, and simulators are available?

Selection of a central processor that is compatible with off-line equipment is a very significant factor in reducing the prime equipment configuration. Often off-line equipment can possess capabilities far beyond the prime equipment and provide for programming aids and services that sometimes spell the difference between a superior and marginal software system. If the central processor has a very limited capability some programming development problems may be insurmountable without good support equipment.

Selection of a digital processor or computer of any significant scale should be made bearing in mind the direct applicability of vendor supplied software. This is particularly true if the computer is to be a large scale multienvironment real time machine with a complex input/output structure. In this case a monitor system capable of performing complex compilation and synthesization is a must for program development. Further, the vendor can readily incorporate changes to the system corresponding to increased hardware and software requirements with minimum impact on the operational programs.

The availability and applicability of special programming aids such as emulators and simulators should be given careful consideration. Emulators can significantly reduce programming

development time by providing debug capability not dependent on prime equipment availability. Simulation on the other hand can be quite effective in evaluating hardware system design, developing and evaluating optimum processing algorithms, and determining system feasibility. Simulation can also be utilized to select and configure the central processor.

5.4.6 Existing ACE Techniques

Applications for real-time digital processing technology have evolved in many fields of science, engineering, and commercial enterprises. The one most closely related to the problem of automated redundancy verification is Automatic Testing.

Over the past decade military and aerospace requirements for more sophisticated, more compact, and more reliable modular electronic/electromechanical systems have required innovations in design, packaging, and testing. Testing of such systems must be conducted during research and development to validate and improve system design, during production to maintain quality control, and in the field to perform routine preventative maintenance and fault isolation in case of failure. Initially this testing was performed manually by a test engineer using laboratory equipments. But, as test articles became faster, more complex, more compact, and the volume of testing increased, manual checkout became infeasible.

Digital processors provided the ideal solution to keeping pace with state-of-the-art developments in electronic systems since digital techniques are largely employed in space flight and ground based equipments. Further, digital processing enables man to take advantage of the speed, decision making, consistency, repeatability, and other of its attributes as described in Paragraph 5.4.1.

The number and types of automatic checkout equipments are many but all have a very basic common functional design and operation. Figure 5.4.6 illustrates this design. The test environment consists of a test article, test equipment, and man. The man/machine interface enables the man to select, setup, initiate, monitor and control the test sequence. The control and decision function performs a precisely timed sequence of stimuli and measurements designed to exercise the test article according to performance and acceptance criteria. The stimuli and measurement interfaces respond to commands from the control and decision unit to produce stimuli and perform measurements respectively. The measurements are evaluated by the control and decision unit. Out-of-tolerance conditions are recorded and displayed via the man/machine interface. Usually the first level of testing is a general functional test. When out-of-tolerance conditions are detected, special fault isolation programs are envoked to resolve the problem. Fault isolation equates somewhat to status resolution in redundancy verification.

Most automatic test sets today are designed around a general purpose real time digital computer. The type of computer is determined by such requirements as:

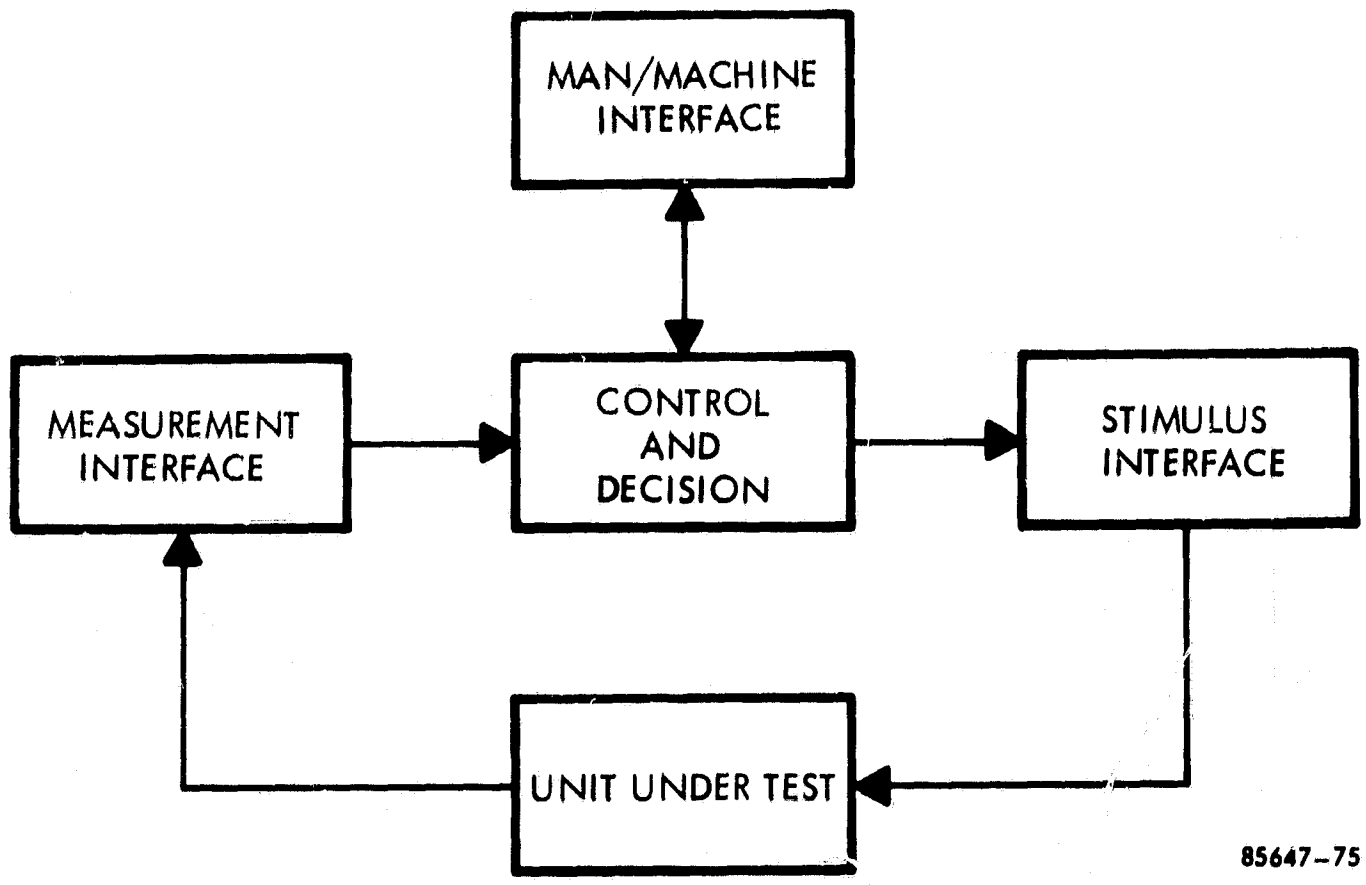


Figure 5.4.6. Automatic Testing Functional Flow

- Memory Access Time
- Word Length
- Instruction Repertoire
- Input/Output Characteristics
- Standard Peripheral Equipments Available
- Support Systems Software Available

The special peripheral hardware that comprises the stimilus/measurement subsystem is usually comprised of commercially available off-the-shelf hardware; universal computer interfaces, channel multiplexers, digital-to-analog converters, analog-to-digital converters, digital voltmeters and programmable power supplies are but a few.

Digital CRT display and keyboard terminals, teletypewriter units, and control panels provide the usual operator interface.

Core memory, disc file, and magnetic tape provide the data and program storage media.

Programming aids for automatic testing have been developed but are generally highly specialized. The development of automatic checkout languages has evolved around the idea of providing the test engineer with an on-line capability to write and execute short test programs in a test oriented interpretive macro language.

5.5 Summary of the Process

A great deal of material has been covered in this section and before beginning a new subject it is important that this material be coalesced. In addition, the preceding sections have not necessarily followed a chronological development, for clarity of presentation was given precedence over chronology in the order of presentation. This section will take into account the time dependence of the various activities. The reader is also referred to a case study in Section 7.0 for an example of the process.

5.5.1 Establishing the Framework

Initial efforts in the design will consist of two parallel activities: partitioning the principal system and resolution of the higher level group problem. Principal system partitioning is identified as an initial activity, for it is here that the problem can first be divided into smaller, more manageable problems and the true scope of the process is first manifested. Together with the required design confidence, the quantity of different confidence levels to be considered and the general group level guidelines; the partitioned system marks the definition of the

set and group problems. Having identified groups and sets, the design can now concentrate on specific points within the principal system for signal characteristic identification and properties indicative of operation. In addition, with the groups and sets parceled out, the status relationship of output properties and time profile information can be directly related to the functions of interest. This will allow assessment of each set and group on its own merits.

Resolution of the higher level group problem provides the verification design an overview and initial, gross direction. This activity establishes the method of status reporting and four general design philosophies: method of status resolution, use of, and relationship to, a central processor (and/or satellite processors), policy of treating off-line equipments and plans for achieving isolation/independence of the verification equipment.

5.5.2 The General Group Problem

With the groups identified by partitioning and the general policies and philosophies established, verification design of the groups can begin. Drawing on this information, verification design for a group essentially amounts to selecting the deductive process or combination of the deductive process, viz., exhaustive, iterative, logical deduction. These processes are selected on the basis of signals, design confidence and functional relationships of the elements and sets within the group. It should be borne in mind that, ultimately, the output of each group must be considered before the verification of elements/sets within that group can begin. As such, the techniques of Section 5.5.3 will also be applicable to groups in this regard. Also, groups higher than first order will usually contain sets and the group design will certainly dictate the handling of these sets. It is not unusual, however, that the requirements of a set design can reflect up the chain to impact group decisions. From this standpoint, once partitioning is complete, the group and set problems can be solved in parallel - with the group problem typically taking the dominant, if not necessarily the most time consuming, role.

5.5.3 The Set Problem

As a consequence of partitioning and any additional constraints established in the solution of the group problem (Section 5.5.2 above), verification design of the sets can begin. From the functional description of the set and the redundancy classification, the method of addressing the output is established, viz.,

- Comparison of Output to Output
- Comparison of Output to Reference
  (output signals and their absolute properties)
- Comparison of Output to Input
  (output signals as they relate to element input and as input/output relates to element operation)

From these three categories and the statistical nature of the signal properties identified as indicative of element operation, the applicability matrix is consulted for candidate coincide development techniques. Using the statement of design confidence, time profiles (where necessary) and the capabilities and limitations of the candidate coincidence development techniques, the technique is chosen which best matches the requirements.

With the coincidence development technique identified a parameter estimation technique must now be selected. This is basically a task of identifying a performance criterio (or criteria in some cases) which best describes the operational integrity of the element/set being verified based on the functional description of the element being verified, the output signal and frequently, the functional description of the immediately succeeding element.

The parameter estimation technique provides a status variable which is indicative the operating integrity of the item being verified (IBV). Using the relationship of the signal properties to status, a mapping function is next designed to translate the values of the status variable into discrete values of conditional status. It should be noted that if the status variabl consists of a compound performance criterion (e.g., integral squared error, volts squared per cycle) the translation into conditional status will involve more than the basic signal property relationships to status. The reader is also reminded that a single simple set can require sever status variables. Consequently, a typical mapping approach will consist of two levels of threshold (or equivalent) decisions. Once a means of obtaining conditional status for each IB is established, the process must return to the higher level group problem for solution of the stat resolution problem. Along these same lines, it is possible that any of the techniques above ca be implemented on a digital processor. This should be borne in mind and if this implementatio is selected, the problem again essentially becomes one for solution at the higher level group with requirements passed along from the set solution.

5.5.4 Design Outputs

The final automated redundancy verification design should provide:

- A means of status reporting
- A status resolution function
- An implementation that is, within all practicability, independent of the principal system
- A high confidence in the status being reported
- Minimum changes to the principal system or the tenant signals

6.0 DEVELOPMENT OF DESIGN CRITERIA AND IDENTIFICATION OF NEW TECHNOLOGY

It is the purpose here to address, in particular, redundant situations which may be "unverifiable". The goal of this investigation is to point out means by which such situations may be avoided, including the elimination of troublesome practices from use, and the employment of new technological means for changing these practices into an acceptable form.

6.1 Verifiability

It is important to realize at the start that, while some redundant situations are, in a strict sense, not verifiable, many other situations may be considered unverifiable from the standpoint that a sufficiently high level of confidence in the verification cannot be established, or from the standpoint that the allowable or available verification equipment is incapable of deriving or fully utilizing the information available in the signal. To illustrate the former situation, consider the example of a diode which is at all times forward biased, Then the observation of its output signal is simply inadequate for the evaluation of its operational integrity, although there may be nothing about its physical situation which makes it unverifiable. An example of the latter situation is the case of "hardwired" element outputs. While such element outputs are not distinguishable in a voltage sense (they are voltage-common), they are distinguishable in a current sense (they are current-additive). However, unless verification equipment is capable of extracting this current information, the situation must be considered to be unverifiable. Also, the sensitivity or accuracy of verification equipment may determine the verifiability of a situation. One could easily imagine an occurrence of redundancy wherein the output of a redundant set varied as the number of properly functioning elements within the set, but where this variation was so small that laboratory-grade equipment would be required to sense it. It would be possible then that this case would be classed as unverifiable on the grounds that proper verification equipment was not available.

It is seen that a statement of verifiability must be taken in the context of what is required of the verification process and of the capabilities of the verification equipment.

By considering the group problem, one realizes that the only occurrence which would lead to an unverifiable group situation but whose effect would not be seen in the set problem is the necessity for sequential switching if iterative deduction is to be used. It is reasonable to expect that this method will not be employed unless such switching is or can be provided. The lack of switching capabilities will not be considered a roadblock to verification since methods other than iterative deduction are available. Therefore, only those things which cause unverifiability in simple sets need be considered.

There are, then, basically four ways in which a situation may become classed as unverifiable.

1. The features of the principal system which are important to the verification process may be such that the situation is placed in redundancy class H.

2. The electrical points of interest in the principal system may be inaccessible to the verification equipment.

3. The signal available for verification may be inadequate for establishing the required verification confidence.

4. There may exist basic incompatibilities between principal system and verification equipments.

It may be noted that, by expressing these as the only possible paths to unverifiability, an implicit assumption has been made. This assumption, which has been invoked earlier in the study, is that, given the proper output signal from the redundant items and the capability in verification equipment to analyze the information in this signal, any given level of verification confidence can be established. That is, all the information necessary to establish a given level of verification confidence may be obtained from the proper output signal. This may mean, of course, the necessity of providing the input which corresponds to this proper output.

To discover why the situations of class H are termed unverifiable, one may list all the possible combinations of the four redundancy features which define the redundancy classes and examine those combinations comprising class H. When this is done, it is noted that two occurrences can be responsible for the classification. Firstly, if the set output does not vary detectably with the number of operational elements in the set and the output/effects of each element are not distinguishable, there is simply no way to identify any malfunction, either on a set or on an element basis. Secondly, if the failure detect scheme demands an indication of the status of each element but the outputs/ effects of each element are not distinguishable, requirements of the verification process cannot be met.

While the statements above concern the existence of proper set or element outputs, it is certainly true that their existence is not sufficient and that they must be made available as inputs to the verification equipment. This question may reduce to one of simply providing for the physical connection of verification equipment to principal system equipment or of bringing out the necessary signals for verification to a point that is geographically accessible to verification equipment. Whereas the problem of these outputs existing is one of concept, configuration, and redundancy policy, the problem of accessibility is one of providing the proper principal system equipment features and of packaging.

If the signal available for verification is insufficient to establish the desired verification confidence, no verification equipment can compensate for the inadequacy. The meaning here is that the element or set output does not contain all the information necessary for verification to a given level of confidence. Recall the example of the diode which is not reverse-biased by the signal through it.

On a very practical basis, it may happen that there are incompatibilities between principal system equipment and verification equipment. These incompatibilities may be either physical or electrical in nature. If principal system equipment were not tolerant of electrical loading by verification equipment, an electrical incompatibility would exist. If element outputs were hardwired together in a printed circuit board implementation, current-sense distinguishable outputs would exist. However, if only current probes were available to extract the information, an incompatibility would exist which would render the situation unverifiable.

Because these are the four ways in which an unverifiable situation may arise, it is the avoidance of these situations to which design criteria should be addressed and the alteration of these situations to which the development of new technology should be addressed.

In examining the first of these areas, the placing of a redundancy situation into class H, it is necessary to ask what practical factors result in such a classification. Assuming that the requirements of the failure detect scheme are fixed and may not be compromised, the placement of a given situation into class H is entirely dependent on the manner in which element outputs are combined. However, if the different methods for combination are listed, including hardwiring, majority voting, sense-and-switch arrangement, etc., it is seen that only one method, that of hardwiring element outputs, destroys voltage-sense distinguishability of element outputs, and this method provides current-sense distinguishable element outputs. In fact then, the concern is not for whether distinguishable outputs exist, but whether they are available to and usable by the verification equipment. Obviously, too, the redundancy configurations requiring the greatest attention here are those employing hardwired outputs.

6.2 Design Criteria

It is desired here to establish design criteria which, when imposed on redundant equipments, help insure that those equipments may be verified in an automated fashion. These criteria should be viewed as standards of judgement or decision thresholds to be applied to the characteristics of principal system equipment. No unique set of such criteria may be constructed. This is because of the dependence of what is required of equipment being verified upon what is required of the verification process and also because of the fact that several different combinations of characteristics in principal system equipment may be capable of satisfying the needs of verification. For example, verification requires either distinguishable element outputs or a suitable set output but generally not both. This clearlys shows the influence of requirements placed on the verification process. It is, therefore, necessary to set forth a number of criteria and identify when each should be imposed and when each may be ignored.

In order to avoid the placement of a redundant situation into Class H, one of three criteria must be met. These are:

1. The outputs from redundant items shall be distinguishable, one from the other.

2. The output from a set of redundant items shall vary according to the number of operable items in the set.

3. From each redundant item there shall be provided an output which is in addition to and isolated from the signal throughput path.

Any requirement that the status of individual redundant items be determined immediately means that the first or the third of these criteria must be imposed. In other cases, the satisfaction of any one criterion will be satisfactory. In Number 1, above, "Distinguishable" must be interpreted with regard to the capabilities of verification equipment and may be specifically stated as "voltage-sense distinguishable" if current sensing equipment is not available. In Number 2, above, "shall vary" must also be interpreted in the context of verification equipment capabilities. Both the type and magnitude of the variation must be observable by the coincidence development equipment. Criterion Number 1 needs only be met during the period of actual verification and, where continuous verification is not a necessity, switching could be used to satisfy the requirement during verification. Number 3 represents the inclusion of additional features in the design of principal system equipment expressly for the purpose of enabling verification.

To make sure that the electrical points of interest are physically accessible, the following criteria may be presented.

4. Access to the output of each redundant item shall be provided.

5. Access to the combined output of redundant items shall be provided.

6. Access to such points as are determined to be necessary for the injection of verification signals shall be provided.

In general, it should be required that Number 4 be satisfied when satisfaction of either of Numbers 1 or 3 is required. Number 5 should be required when, of the first three criteria, the satisfaction of only Number 2 is sufficient. The satisfaction of Number 6 should always be required.

In all of criteria 4, 5 and 6 access may be provided either by simply allowing for the attachment of verification equipment or by "bringing out" signals for verification to a point at which interface with verification equipment may be conveniently accomplished.

No design criteria have been established to assure that the signal for verification is adequate to establish the desired level of verification confidence. It would be unreasonable to flatly require this capability of the tenant signal, since a conflict with its primary goal, that of transferring intelligence might arise; and, if an injected signal were used for verification one should assume that such a signal would be designed to fulfill its purpose.

The following criteria may be set forth to avoid the occurrence of incompatibilities between equipment being verified and verification equipment:

7. Principal system equipment shall be tolerant of effects of verification equipment such as electrical loading.

8. Accesses provided in the satisfaction of criteria 4, 5, or 6 shall be in a form acceptable to verification equipment.

It is deemed unwise to set quantitative limits on the effect to be tolerated as mentioned in Number 7. If, for example, limits were set on loading effects according to the worst case to be expected from verification equipment, a requirement which would be overly stringent in a majority of cases would be established. If tolerance to the minimum loading to be expected from verification equipment were used as a limit, the result could be that verification equipment presenting a greater load than the minimum would be unusable.

It is necessary, too, to require that information made available to verification equipment be provided in a form usable by that equipment. For example, element outputs might be brought out of a unit by fiber optics and presented in the form of amplitude modulated light. Though all the information be present, if the verification equipment could not accept it in this form, verification would not be possible. If verification requires access to current information, the provision of access to voltage information would not be satisfactory.

Numbers 7 and 8 should both be applied to every set of equipment.

The discussions above have shown that some knowledge of equipment to be verified and requirements on the verification process must be available to allow the intelligent imposition of these criteria. Included are:

1. Whether the status of individual elements is required.

2. Whether the level of confidence attainable by using the tenant signal is sufficient.

3. Whether continuous verification is required.

4. What types and magnitudes of signal variation the verification equipment is sensitive to.

5. Acceptable forms of input to the verification equipment.

6. Confidence level required of the verification process.

The design criteria generated have been concerned with three primary areas of application.

Area A - the avoidance of placing a situation into redundancy class H; consists of criteria 1, 2, and 3.

Area B - providing to verification equipment access to the necessary electrical locations; consists of criteria 4, 5, and 6.

Area C - avoiding incompatibilities between equipment being verified and verification equipment; consists of design criteria 7 and 8.

In the most general case it is necessary that any one criteria from Area A must be satisfied, that one of criteria 4 and 5 must be satisfied, and that all of criteria 6, 7, and 8 must be satisfied. The comments accompanying the introduction of these criteria, above, will aid in identifying when requirements should be different from those of the general case.

The criteria presented here appear in a form consistent with NHB 8040.2 in Appendix D.

6.3 New Technology

There have been identified four ways in which a redundant situation may come to be considered unverifiable, and there have been presented design criteria aimed at preventing the classification of these situations as unverifiable. It is the purpose here to investigate by the application of what new technologies the occurrence of unverifiable situations may be avoided.

Realizing that these new technological developments must be used as aids in complying with the design criteria, the major areas of concern are the provision of distinguishable element outputs and the provision of access to the electrical points of interest. Again, attention is focused on situations which employ hardwired element outputs. Also, when the problem of adapting existing equipment to verification is considered, technologies which allow the derivation of signal information for verification without major alteration to the equipment being verified becomes important.

Addressing the situation of hardwired outputs, there are two ways to alleviate the problem. One may either contrive another method of combining outputs which provides voltage-sense distinguishability or devise means for deriving information from current flowing in the outputs.

Semiconductor technology is the likely area for development of a new technique for combining the outputs of redundant elements. The object would be to construct a device which retains, at its inputs, separate and distinguishable (in a voltage sense) signals, yet employs no switching or voting to develop its output and meets the success criteria that if one element of the set is operable, set operation will be proper. This device might, in fact, function as a combination of parallel isolation devices whose outputs are voltage-common. As a minimum, such devices should be developed to handle two and three inputs. Naturally, it should be true that failures in the device do not cause total loss of set output.

The derivation of current information is perhaps a more attractive solution to the problem and, in fact, the extension of some existing technologies offer promise. There are at least five types of devices which are candidates for this function. They are current transformers, light-emitting diodes, grain-of-wheat lamps, ferrite core devices, and Hall-effect devices.

Current transformers are currently used as sensing devices for clip-on ammeters and voltmeters and are often referred to as current probes. They operate by sensing voltages induced by the electromagnetic field of a current-carrying conductor. The characteristics of a presently-used current probe are listed below to represent typical values.

Sensitivity	1 mV/mA ±1% at 1 kHz
Frequency Response	±2%, 100 Hz to 3 MHz; ±5%, 60 Hz to 4 MHz; -3 dB < 25 Hz and >20 MHz
Input Impedance	< 50 mΩ in series with 0.05 μH

The major disadvantage of these devices include their susceptibility to stray electromagnetic energy, and their restriction to use with certain forms of conductors. For example, they cannot be used when stripline or coaxial cable are the transmission medium. Also, the achievement of high sensitivity may impose a requirement for a power supply for the probe itself. They may, however, be easily retrofitted in some cases.

Light-emitting diodes are of great interest for current-sensing purposes. Models are presently available which offer essentially linear output-intensity/throughput-current characteristics over an appreciable current range.

Typical ranges of values for Gallium Arsenide emitters are listed below.

Output Wavelength	9000Å
Output Power	200 μW - 1.5 mW
Total Device Dissipation	150 mW
Maximum Continuous Forward Current	150 mA - 1.5A
Forward Dynamic Resistance	0.2Ω - 1.5Ω
Maximum Reverse Voltage	3V
Forward Voltage Drop	1 - 2.5V

The use of these devices offers a great deal of isolation between the equipment being verified and the verification equipment (up to 10" Ohms). These devices are necessarily placed in line with the signal being verified. While this means that provision for verification must be made before the fact, these devices may be made very reliable and, since the probability is high that when they fail it will be in such a way that the through signal current will not be interrupted, their being placed in line will not seriously affect principal system reliability. Gallium Arsenide and Gallium Arsenide Phosphide diodes are presently available for application up to the 30-50 MHz range. Because these are diodes, in many redundancy verification applications it would be necessary to employ two emissive diodes paralleled with opposite polarities. In this way, both positive and negative portions of the signal will be transmitted as light.

Great flexibility is afforded in the transmission of derived information since it may be transmitted either by fiber optics in the form of light or immediately detected by a photoconductive device to establish an electrical signal for transmission. It would be profitable to develop unitized modules containing two photocoupled pairs (emitters and detectors) to derive current-proportional information from hardwired element outputs. Such devices could be made to be inexpensive, rugged, and impervious to interference from surrounding equipment.

The major shortcomings of these light-emitting diodes are their sensitivity to temperature variations and their forward voltage drop. The relative intensity of their emissions may vary by a factor of 6 between -50°C and 120°C and the form of this variation is dependent on forward current in the device. The forward voltage drop, which can usually be minimized to 1.3V, could easily be intolerable in some implementations.

The third candidate device is the grain-of-wheat lamp. This is simply an exceptionally small tungsten filament lamp which may be placed in line to sense current. Because the device has a relatively long decay time, it must be viewed as an integrator and should be used as an indicator of rms current. However, there is practically no upper limit on frequency response of these lamps. It is true that these devices fail to an open condition and by their failing would destroy the output of the redundant element they were monitoring. However, by operating at low current levels, their expected life can be thousands of hours and, whenever this reliability is great compared to that of the element being monitored, overall reliability will not be affected. As with light-emitting diodes the derived information may either be transmitted in the form of light or detected and transmitted electrically.

Ferrite core indicators offer another possible means for sensing current but are limited to the sensing of dc currents. These indicators consist of primary and secondary windings on a toroidal ferrite core. The dc current to be sensed is passed through the center of the toroid and an ac signal is supplied to the primary windings. Monitoring the amplitude and phase of the voltage at the secondary windings reveals the magnitude and direction of the dc current of interest. Devices such as this have proved their capability to sense currents from 5 to 300mA. The major disadvantages of these devices, aside from their limitation to dc sensing, are the requirement for an ac signal source and restrictions on the conductor configurations to which they may be applied.

Hall-effect devices may be used to sense current in either of two ways. The device may be placed in line with the current to be detected and an external magnetic field applied. The voltage developed across the device transverse to the current flow is then proportional to that current. Alternatively, the device may be placed in the air gap of a magnetic collar which surrounds the conductor carrying the signal for verification. An input signal is supplied to the device and an output signal is derived which contains information from the signal for verification. In fact, this is an alternate form of current probe. The former of these two implementations requires the supplying of a magnetic field, the latter an external power source. The use of the device in line would probably not result in sensitive detection. The magnetic collar implementation should provide sensitive detection, but would be restricted in the conductor configurations with which it could be used.

Of the methods discussed above, current transformers, ferrite core indicators, and current probe implementations using Hall-effect devices all offer sensing without electrical connection to the circuit under investigation. Such ability could be of immeasurable worth in the verification of existing equipment wherein the opportunity for electrical connection to the circuit does not exist. Therefore, these areas should be expanded and tailored for employment in the verification of redundancy. Any additional techniques having this capability should also be investigated and developed.

Also identified as an area for development is the use of multiplexing techniques for gaining access to electrical points important to the verification process. That is, using already existing conductors for the transport of coincidence and status variables. Power supply conductors should be included as a possibility.

In the area of redundancy verification equipment, it has been realized from the case study that there exists a need for sampling spectrum analyzers with extended capabilities. Present analyzers are limited in the upper end of their frequency range by their maximum sampling rate. Also, time required for verification is increased by the processing time inherent in these machines. The processing time is dependent not only on sampling rate but also on the time required for the generation of an autocorrelation function and the Fourier analysis of this function.

Because of the power of the spectral analysis technique and the often-desired advantages of sampling, the availability of more capable sampling spectrum analyzers is an attractive prospect.

6.4 Technology Development Plan

Four major areas for technological development have been identified. These are:

1. Techniques for sensing current and for sensing without electrical connection.

2. Devices for combining element outputs in a voltage-common manner while retaining voltage-sense distinguishability at some point in the circuit.

3. Techniques for multiplexing verification information onto existing conductors.

4. Construction of sampling spectral analyzers with extended capabilities.

These four areas are essentially independent and future efforts in these areas may be highly divorced from each other. A technology development plan, then, should consist of four major branches which may proceed in parallel. Each of these branches will be discussed individually below.

6.4.1 Current Sensors and "No-Touch" Sensing

Development in this area should include investigation into the possibility of overcoming the limitations of presently available devices and the establishment of a family of such devices to fill the existing gap. Elements of such a development are given in flow chart form in Figure 6.4.1-1 and are identified and explained immediately below.

Task 1. Investigate the practicality of reducing temperature sensitivity in photocoupled pairs, producing integrated bipolar combinations, and reducing forward voltage drop in photoemissive diodes.

Task 2. Investigate the practicality of extending ferrite core devices for use in sensing ac and for use with difficult conductor configurations such as stripline and coaxial cables.

Task 3. Investigate the practicality of improving the efficiency of Hall-effect devices, of altering undesirable characteristics, and of adapting their use as current probes to difficult conductor configurations.

Task 4. Investigate the practicality of improving the efficiency of current transformers and adapting them for use with difficult conductor configurations.

Task 5. Establish suitable families for the devices according to frequency and current ranges. That is, partition the ranges of frequency and current to be accommodated into segments which can be covered by a single member from a family of devices.

Task 6. Evaluate the effect of devices on principal system reliability. Here the consideration of whether or not the device is used in line with the tenant signal must come into play.

Task 7. Generate estimates of development time for the devices with altered characteristics.

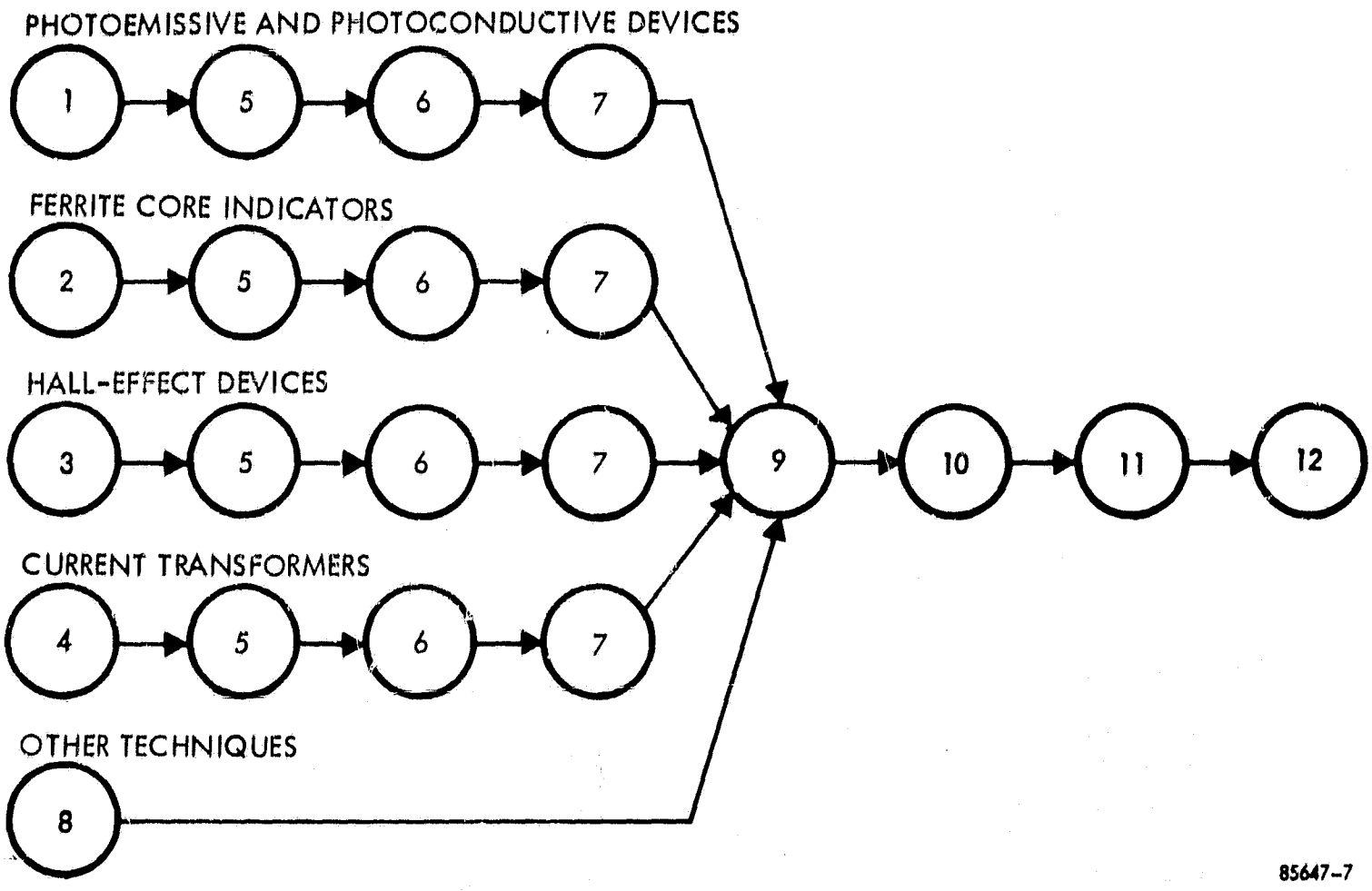


Figure 6.4.1-1. Development Plan - Current and "No Touch" Sensing Devices

Task 8. Investigate the existence of other techniques for sensing which meet requirements. If such techniques are identified, bring the state of knowledge concerning them to a level equal with that concerning the devices identified herein as candidates.

Task 9. From all the information gathered in earlier tasks, compare the various techniques and devices to develop a maximally efficient approach to providing the capabilities desired. The resulting approach may include the actual development of several different types of devices.

Task 10. Produce prototypes of the devices.

Task 11. Test and develop to production-ready status the prototype models.

Task 12. Disseminate information on new devices and techniques.

It is estimated that to accomplish Tasks 1 through 8, above, will require 4-6 months of intensive effort. The time required for Tasks 9 through 12 is estimated at 8-10 months, though time required to develop prototypes could cause gross deviation from this estimate.

Of the four major branches for technological development, this first is the most important and promises the greatest return on investment.

6.4.2 Devices for Combining Element Outputs

The second branch of the development plan, that for devices to be used to combine element outputs, ranks second in importance and consists of five series steps detailed below.

Task 1. Develop a concept for a device to fulfill needs in this area as described previously.

Task 2. Compare such a device against alternate methods of achieving the voltage-common combination of isolated element outputs.

Task 3. Contingent on a favorable decision in 2, above, establish characteristics for the members of a family of combining devices.

Task 4. Design, produce, and test prototype devices.

Task 5. Disseminate information on the new devices.

The estimated time to accomplish these five tasks is 8-10 months.

6.4.3 Multiplexing Techniques

The third branch of the development plan, the establishment of techniques for multiplexing verification information onto existing conductors ranks third in importance and is comprised of six series tasks. These are:

Task 1. Identify types of signal paths available for the multiplexing, discover the features of these paths which are important to the multiplexing process, and identify roadblocks to the multiplexed information.

Task 2. Study, enumerate and invent techniques for bypassing the identified signal roadblocks.

Task 3. Evaluate the techniques of 2, above. Establish statements of limitations.

Task 4. Identify technologies required for implementation of techniques.

Task 5. Develop identified technologies.

Task 6. Disseminate information.

It is estimated that the completion of the first four of these tasks would require 4-6 months. Because of the dependency of Task 5 on preceding tasks, it is impossible to estimate further.

6.4.4 Sampling Spectrum Analyzers

The fourth branch of the plan is the development of sampling spectrum analyzers having extended capabilities. No detailed plan has been developed here. There are two reasons for this: it is certain that segments of private industry are in full pursuit of this goal; and it is felt that pursuit of the other three branches of the plan will be more rewarding than the expedition of developments in this area which would result from the dedication of additional funds.

7.0 A CASE STUDY

A case study was performed of the design of Redundancy Verification for a hypothetical communication system. The technical description of the hypothetical system used for the case study is given in Appendix B. The experience of the design team and the resulting redundacy verification design is given in Appendix C.

The purpose of conducting the case study has been threefold:

a. To show proof of redundancy verification methodology;

b. To sound out the methodology for weak areas and possible oversights, and

c. To provide an illustrative example of the redundancy verification design process.

To realize these ends, the case study closely followed the design process and implementation considerations of Redundancy Verification in Section 5.0.

7.1 The Hypothetical System

Rather than use an existing system on which to perform the case study, a hypothetical system was developed for several reasons. Firstly, it was felt that the system should be of limited scope so that a reasonably complete design could be performed in the allotted time. Secondly, a hypothetical system gives greater freedom in choosing redundancy schemes and operating conditions so that more classes of redundancy verification techniques could be exercised. Thirdly, preconceived notions (and sacred cows) could be avoided by the designers and by those critiqueing the design.

The system developed for the case study is a Hypothetical Communications Down-Link Earth Receiving Subsystem (HCDL-ERS). The Earth Receiving Subsystem is located at one of three stations equally spaced in longitude around the world.

The purpose of the HCDL-ERS is to receive information from a fixed, manned moon base via an S-Band link, convert this information to baseband and feed the baseband signals to the proper distribution buses. The S-Band carriers contain commercial-grade video, a one megabit per second telemetry channel, a voice channel consisting of five frequency multiplexed circuits, and an emergency telemetry channel. The case study is limited to the receiving system of the earth station. The microwave feed subsystem, the servo electronics and other auxiliary equipment are not considered part of the earth receiving subsystem for purposes of this case study. The HCDL-ERS system parameters and operating profile were chosen to be reasonable and practical. The receiving subsystem of the Unified S-Band Apollo communications system was used as a guide to assure practicality. However, it is worth reiterating that the system described in Appendix B should not be judged per se; it is a vehicle for performing the redundancy verification case study. The personnel who developed the HCDL-ERS were not members of the Redundancy Verification design team. They did, however, provide additional system details as the design team recognized the need for them.

7.2 Redundancy Verification Design

The Redundancy Verification design team was composed of three experienced system design engineers. One had been a member of the study team who developed the Redundancy Verification techniques. The others became familiar with Redundancy Verification techniques by reading the published reports. The following instructions were given at the redundancy verification design kickoff meeting. The case study must evolve through the developed process, using the developed methodology. It is imperative that the verification redundancy terminology be used consistently and throughout the case study. The design is not to simply be a passive effort to fit the subsystem as detailed. So long as the subsystem functions are performed in the proper time reference, a verification design can be expected to require additions and modifications to a system--especially in the areas of redundancy tie points, redundancy configurations and signal insertion/extraction. The scope of the design is to be such that reliability and cost tradeoffs can be performed and some confidence statements can be developed. Design decisions must be justified.

After a brief orientation period during which the design team tended to encumber themselves with end of the design details, they were directed to begin at the beginning of the Redundancy Verification Design Process. The design then proceeded extremely smoothly. They found that the Design Process was very effective. From time to time the team requested additional details concerning system signal characteristics when the information furnished originally proved inadequate. After a few days, the partitioning was completed, the signals were classified, and the coincidence development techniques were chosen. The bulk of the design team effort was then spent in determining the best hardware configuration to perform the redundancy verification. An informal design review was held which was attended also by the principal investigator of the Redundancy Verification Technique Study and by the persons who developed the HCDL-ERS. The redundancy verification design team did recommend changes in the HCDL-ERS. Usually these included a change in the method of implementing the redundancy. They were not permitted, nor did they feel it was necessary, to change all of the redundancy to simple set form. In every instance the design team had come up with a feasible method of implementing the redundancy verification. Some suggestions were made for alternative implementation schemes in a few cases. Of these one or two were adopted.

Generally it may be concluded the experience of the case study has been most gratifying. The three goals were met. The Design Process proved most adequate. Feasible hardware implementations were obtained. (The availability of through variable (flow) sensors would have permitted hard wired outputs which would have simplified the implementation in some cases.) The design team, inexperienced in redundancy verification design, was able to work smoothly together.

8.0 CONCLUSIONS AND RECOMMENDATIONS

In the course of Phase I through III of this study, the examinations of redundancy and the verification thereof have revealed a number of important facts.

8.1 Conclusions

Redundancy may be characterized, for the purpose of verification, by four features. Based on these four features, eight redundancy classes about which general and categorical statements may be made, can be established. The placing of an occurrence of redundancy into one of these classes is by no means a sufficient description to allow the choice of a verification method. Information concerning the characteristics and properties of the output signal is also required. Where the use of the tenant signal for verification is not satisfactory, that is, where the desired level of confidence in the operational integrity of the redundant equipment cannot be thus established, the use of symbiotic, idle, or simulative signals must be considered. By definition, simulative signals negate the possibility of continuous verification.

The problem of redundancy verification has been shown to be most profitably viewed as a segment of the overall status identification problem.

It has been seen that, for verification purposes, redundancy situations may be placed in one of two categories. Namely, a given collection of redundant items should be considered to be either a group or a set, the approaches applying to the two problems being quite different.

The verification process consists of five distinct functions: coincidence development, parameter estimation, mapping to conditional status, status resolution, and status reporting. Two of these functions, parameter estimation and status resolution, may, in special instances, be greatly simplified or even eliminated. The conditions under which this may occur have been determined.

The five constituent functions of redundancy verification have been individually examined.

Exhaustive and mutually exclusive categories can and have been established for methods of implementing the coincidence development function. This function interfaces with the equipment being verified and it is significant that there is no class of coincidence development techniques the use of which negates the possibility of continuous verification. Bases of comparison and selection among various coincidence development have been identified to include the number of failure types detectable, the ability to identify failure type, the degree of specialization to the equipment being verified, sharability, complexity, amenability to digital implementation, sources of errors, restrictions on minimum sampling rate, assistance in status resolution, and sensitivity to unsymmetrical redundancy. A design process for the selection of a coincidence development technique has been defined and the required inputs to the design have been determined.

The function of parameter estimation has been seen to be influential and complicated. It is capable of restricting design confidence to a level below the maximum offered by a given coincidence development technique and a given signal for verification.

Mapping to conditional status is a comparatively uncomplicated process to implement, though design decisions on the interpretation of status variable values may be involved.

The status resolution function is usually a member of the group problem but may sometimes be eliminated as an entity through a proper choice of coincidence development techniques. For large groups of equipment, the need for status resolution may require the employment of a central processor.

An overall design process for redundancy verification has been detailed. A case study has been carried out in order to exercise and test the presented methodology. The study affirmed the presented methodolgy and design process.

It has been determined that restrictions on the number of status levels achievable are determined by two factors; quantization in the verification process and the number of dimensions allowed the status variable

The reasons for needing continuous verification have been identified. They are the criticality of failures, the importance of unidentified false information, and the need to repair immediately upon failure. An investigation of the need for continuous verification has provided tools for determining the suitability of substituting periodic verification. The tenant signal should always be considered first as a signal for verification so that the possibility for continuous verification may be retained.

The things which make an occurrence of redundancy unverifiable (in some context) are the following:

a. The possession of characteristics which force the redundancy situation into class H. This occurs when a neither distinguishable element outputs nor a set output which varies detectably with the number ot operational elements and exist or (b) when the failure detect scheme requires an indication of the status of each element but distinguishable element outputs do not exist.

b. The lack of availability of the required electrical locations.

c. The absence of a signal suitable for verification purposes.

d. Interface problems between principal system equipment and verification equipment.

The term "verifiable" must be interpreted in the context of required verification confidence and difficulty of implementing the verification. A given redundant configuration may well be verifiable only if a very low level of confidence is required or only through the use of very complicated, sophisticated, or even exotic verification equipment.

Likewise, "distinguishable element outputs" must be interpreted in light of the capabilities of allowed and available verification equipment. Hardwired element outputs, while not distinguishable in a voltage sense, may be considered so in a current sense so long as current sensors are available to make use of this distinguishability.

Design criteria for principal system equipments have been generated. These are standards of judgment for evaluating the adaptability of these equipments to automated verification. The particular criteria to be applied in a given situation must be a function of what is to be required of the verification process, such as the identification of failed elements or the "exercising" of certain elements.

The areas of current sensing and sensing without physical connection to redundant circuitry are the most important technological areas as regards the establishment of increased adaptability to automated verification. The development of isolation devices having particular characteristics and of new techniques for the combining of outputs from redundant items would also prove profitable.

8.2 Recommendations

As a result of the investigations of Phase I, II, and III of this study, the following recommendations are made.

Inputs to the redundancy verification design which concern required levels of verification confidence, the required number of levels of verification confidence, and time profiles should be provided in the early design stages of principal system equipments. These factors should be allowed to influence system and tenant signal design.

The equipment designer should be required to justify a need for continuous verification, particularly when associated with a high level of verification confidence. This is recommended as a cost-effective measure in light of the equipment savings which are often commensurate with the relaxation of a requirement for continuous verification. A similar requirement to justify a high level of confidence would also be a cost-effective measure.

The function of parameter estimation should be investigated to the extent that coincidence development has been. A general organization and explanation of the techniques, or classes thereof, should be provided to the designer of verification equipments.

The influences of redundancy verification requirements on a redundancy design have been pointed out. These influences have given rise to the desirability of considering the relative advantages and disadvantages of redundancy designs in their own right, i.e., in the absence of any requirement for verification. The result should be comments, criticism, and

evaluations which take into account both the inherent qualities of the configuration or policy and the influence of the required verification.

Means of sensing current and of sensing signals without electrical connection to the source circuit are the primary areas to be pursued and developed to the end of achieving increased adaptability of common redundant configurations to automated verification.

APPENDIX A

DISCUSSIONS OF COINCIDENCE DEVELOPMENT TECHNIQUES

TABLE OF CONTENTS

Paragraph	Title	Page
A1.0	Introduction	A-3
A2.0	Compare Two Techniques	A-3
A3.0	Voting Techniques	A-7
A4.0	Cross Power Spectrum Techniques	A-12
A5.0	Value Check; Sequential Techniques	A-15
A6.0	Value Check; Nonsequential Techniques	A-19
A7.0	Coding Techniques	A-23
A8.0	Signal Form Analysis Techniques	A-25
A9.0	Spectral Analysis Techniques	A-29
A10.0	Inverse Transform Techniques	A-33
A11.0	Correlation Techniques	A-37
A12.0	Acknowledgment Techniques	A-40
A13.0	User Complaint Techniques	A-42
A14.0	Combined Signal Form Analysis/Compare Two Techniques	A-44

A1.0 INTRODUCTION

These discussions are intended to aid the designer in the selection of a coincidence development technique by pointing up the relative advantages, disadvantages, limitations and pitfalls attributable to each. A number of statements appear herein which should be mentally prefixed by the reader, "where applicable". That is to say, statements concerning sampling rates should be taken to apply if sampling is employed, those concerning computer implementations when computers are employed. One should not consider that statements concerning sampling rate infer a recommendation that sampling be used, nor that statements about computers infer that computer implementations are recommended.

Throughout these discussions a careful distinction between the terms "discrete" and "digital" is made. "Discrete" means that only discrete values, as opposed to a continuum of values, may be assumed by the function. "Digital" implies the encoding of a value to form a digital word.

A2.0 COMPARE TWO TECHNIQUES

The Compare Two class of coincidence development techniques is one of the simpler approaches available and has the distinction, along with voting methods, of requiring at least first-order redundancy.

Techniques of this class are generally capable of detecting a large number of failure types, the only requirement being that the failure result in a sufficient change in output from that which would be present from a properly operating unit. The addition of excessive noise by the Item Being Verified (IBV) would be detectable by this method. Differentiation among failure modes is not possible when Compare Two is employed. That is, a determination can be made that a failure has occurred, but the way in which an element has failed will remain in question.

It can be noted from the matrix of Figure 5.2.2.2-5 that this class of techniques requires that element output be distinguishable and, in fact, that application to set output is not possible.

The application of Compare Two techniques may be on an analog basis by using a simple differential amplifier or on a discrete basis with logical comparison done by computer or by specially designed, but probably uncomplicated, logic gates. The use of sampling implied by digital implementation of these techniques would not be sensitive to sampling rate. Since there would be no concern over signal information lost in the sampling process, sampling could be performed on a slow or even random basis as long as care were taken to assure the synchronization of sampling on the two element outputs under consideration. A further design option would be realized in determining a method for comparing sample values; the values could either be compared directly by differential circuitry, or could be encoded (perhaps to a binary form) and compared on that basis.

For the case of comparison on an analog basis, verification equipment could be made very reliable, at least by comparison to implementations of more complex coincidence development techniques. If a sampling approach were chosen, the reliability of the verification equipment would be dependent upon the sampling equipment and the equipment performing the comparison of the samples. If the latter were, for example, a computer, the fact that it was being used for the comparison of two samples would not enhance its reliability beyond that for the case where the same computer was used for spectral analysis. The fact that lower sampling rates are a possibility in Compare Two techniques might, however, allow the use of simpler, more reliable sampling equipment than that required by more comprehensive coincidence development techniques.

In some cases, to take advantage of the simplicity of Compare Two techniques will mean a sacrifice of accuracy. Whereas some methods allow comparison of an output (or a representation of that output or a portion thereof) against a well-defined standard, a comparison against another output forces the designer to allow for the possibility that both outputs will, at some time, vary within tolerable limits and in opposite directions. This could be crudely viewed as building twice as much "sloppiness" into the equipment.

The output of a Compare Two system will always be simple in form and display requirements for any individual Compare Two implementation will be minimal. The coincidence variable developed from one of these implementations may be continuous if analog implementation is chosen, through the use of sampling implies the generation of a coincidence variable which is discrete in time, only the use of encoding restricts the coincidence variable to be discrete in range.

With regard to equipment location, for the analog implementation a good general statement would be that the basic comparison equipment, for example, a simple differential amplifier, should be located in proximity to the IBV. For sample-and-compare implementation, as for the analog case, the coincidence variable should be developed before any transmission is attempted. If samples are encoded before comparison, transmission of the encoded samples will generally be possible without loss of precision in the verification process. This allows the coincidence variable to be developed elsewhere.

A particular advantage might be attributed to the Compare Two techniques when time multiplexed signals are considered. Since the only assumption is that two outputs should be alike, an evaluation of the truth of any statement of "likeness" will not require the use of timing information. For example, if two elements are expected to output the bits comprising digital words in a synchronous fashion, it is of little consequence which bits in which words are compared. Indeed, a larger, more important statement can be made: if Compare Two techniques are used, the transition from conditional status to status requires only the knowledge that the input is admissible - the status of the input is not required.

A restriction on these techniques is that, where the use of unsymmetrical redundancy means the use of redundant equipments with different capabilities, a comparison of their outputs may not furnish useful information. To realize its full potential, this class of techniques should

be applied to "identical" outputs, where here "identical" is taken to mean alike within the practical restraints of equipment tolerances, noise environment, etc.

The time-sharing of Compare Two equipment is certainly possible and may be envisioned in several different forms. For analog implementation, it would only be required that the output of the verification equipment be inhibited during the required switching among items to be verified - this provided that all outputs to be investigated by a given set of verification equipment be the same. In general, equipment doing the actual comparison would be sharable either among elements of the same set or among different sets; equipment preparing signals for comparison, such sampling networks would not.

Since no accumulation of a number of samples is necessary for comparison (it could be done on a sample-by-sample basis if desired), verification can be done quite rapidly. Any speed limitations imposed by operations prior to actual comparison would be insignificant.

Some degree of disadvantage must be attributed to these techniques in certain cases where off-line elements are to be verified, since it would be required that two off-line elements be available and powered up. If only one off-line element existed in a configuration, it would be necessary to involve the on-line element in verification; in other cases, perhaps where power conservation is desirable, Compare Two techniques will be less preferable than techniques which require only one powered-up element.

By comparison with other coincidence development techniques, such as Inverse Transform and Spectral Analysis, a minimum of design consideration with regard to the type of elements and class of signals under scrutiny is demanded by Compare Two techniques.

Sources of Type I errors in Compare Two systems will be lack of synchronization between two acceptable outputs, imbalance in verification equipment, and system noise. Also, when comparison is made analog or sample-by-sample basis, the verification equipment will have no way of discriminating between element failures and legitimate errors on one of the outputs. For example, if one of two elements outputs a bit error which doesn't exist in the other element, an indication of disagreement will result. Techniques which operate by collecting information for evaluation (spectral analysis would be one) would be more forgiving. Compensation for this shortcoming could be accomplished through parameter estimation.

Viewing the signal comparisons here as the measurement of one element output against a "noisy reference signal" (the other element output) it appears that the likelihood of a Type I error due to noise will be somewhat greater than would result from a comparison against a noiseless reference. However, the aforementioned fact that any Compare Two design would allow tolerance for variations in both element outputs, independently and in the absence of noise, would probably be that no net increase in Type I errors would result.

Type II errors should result only from catastrophic failures in the verification equipment and in the case of identical failures in the elements being verified. However, it should be noted that if elements contain bilevel logic, the likelihood of identical failures may be greater since it is common for such logic to fail by locking up in one state or the other.

Compare Two - Relative Advantages

- Allows continuous verification
- Simple and, in some implementations, inexpensive
- Capable of detecting numerous types of failures
- Analog or digital implementations available
- Sampling rate, if used, not critical
- Computer implementation possible
- Does not require timing information
- Requires only an admissible input

Compare Two - Relative Disadvantages

- Not applicable to set output
- Unable to distinguish among failure types
- Unable to identify failed element
- May lack accuracy
- May experience limitations with regard to unsymmetrical redundancy
- Requires two powered-up elements
- Not advantageous in low S/N situations

A3.0 VOTING TECHNIQUES

It should be pointed out here again, that the voting techniques to be discussed are Voting techniques applied for the purpose of redundancy verification and do not necessarily have anything to do with the manner in which redundancy is achieved. Majority voting for the purposes of error elimination or the achievement of redundancy is not of interest here.

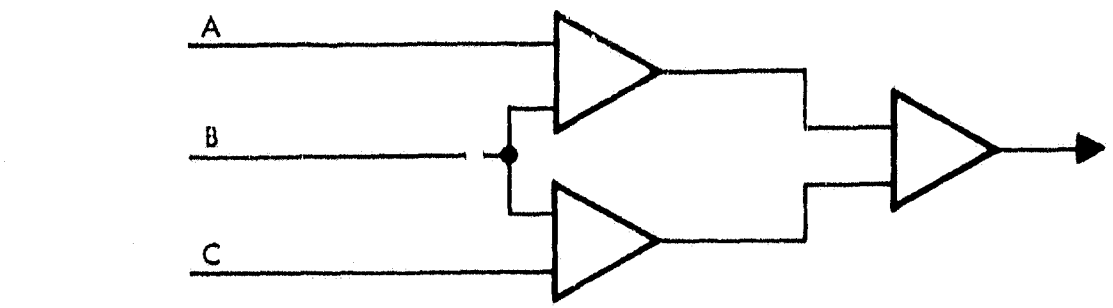
When used for redundancy verification, it is characteristic of Voting techniques that they are unable to distinguish among failure types. That is, when the results of a polling procedure indicates a disagreement among element outputs, it is generally not possible to determine whether the cause of the disagreement is noise, loss of signal, signal distortion, etc.

The number and kinds of failures detectable by Voting are highly dependent on the implementation of Voting chosen. For the purposes of discussion, consider the three baseline implementations shown in Figure A3 where the three input lines may be considered to be element outputs. Implementation A allows analog voting. In practice, some estimation process, such as mean squaring and/or integration would be performed on differential amplifier outputs. It would likely be a complicated matter to decide on the details of developing a coincidence variable in any analog Voting implementation; for example, if mean squaring were done on the outputs of the first two differential amplifiers, what level of disagreement at the third differential amplifier should be acceptable. While many failure types may be detected by a first comparison of outputs, the multiple application of estimation techniques and comparison may mask some failure types and complicate the mapping to status.

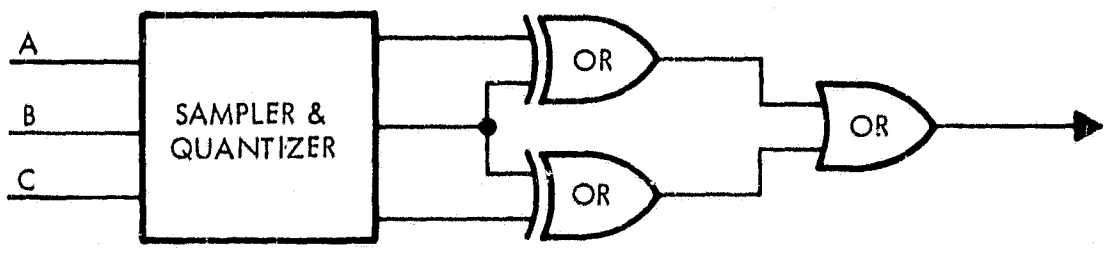
Implementation B uses Exclusive OR logic gates for voting. To assure proper logic operation, samples have been quantized before applied to the gates. The choice of quantization levels and sampling rates will, in large part, determine the accuracy of verification and the number of failure types detectable.

Implementation C compares outputs on a digital basis. Again, quantization and sampling rate enter the picture as limiting factors on verification accuracy and on the types of failures detectable. It would be expected, however, that voting on a digital basis could be made both more accurate and more comprehensive than voting on a quantized but nondigitized basis (Implementation B). In general, implementations of the form shown in C will be the preferred of the three. Too, for implementation on a digital basis, the equipment could be made to indicate the significance of the bit (most significant, least significant, etc.) on which a disagreement was detected thereby allowing mapping to a more comprehensive statement of status.

The first of the two implementations above are incapable of identifying the status of individual elements. That is, they can indicate disagreements, but cannot choose which of the outputs disagrees with the other two. In implementation C a statement of which is the disagreeing element is possible. It is not intended to imply that this capability is attributable only to comparison on a digital basis. In general, voting on any basis is, in its simplest form, incapable of identifying element status but, with simple extension of the technique, such capability may be realized.

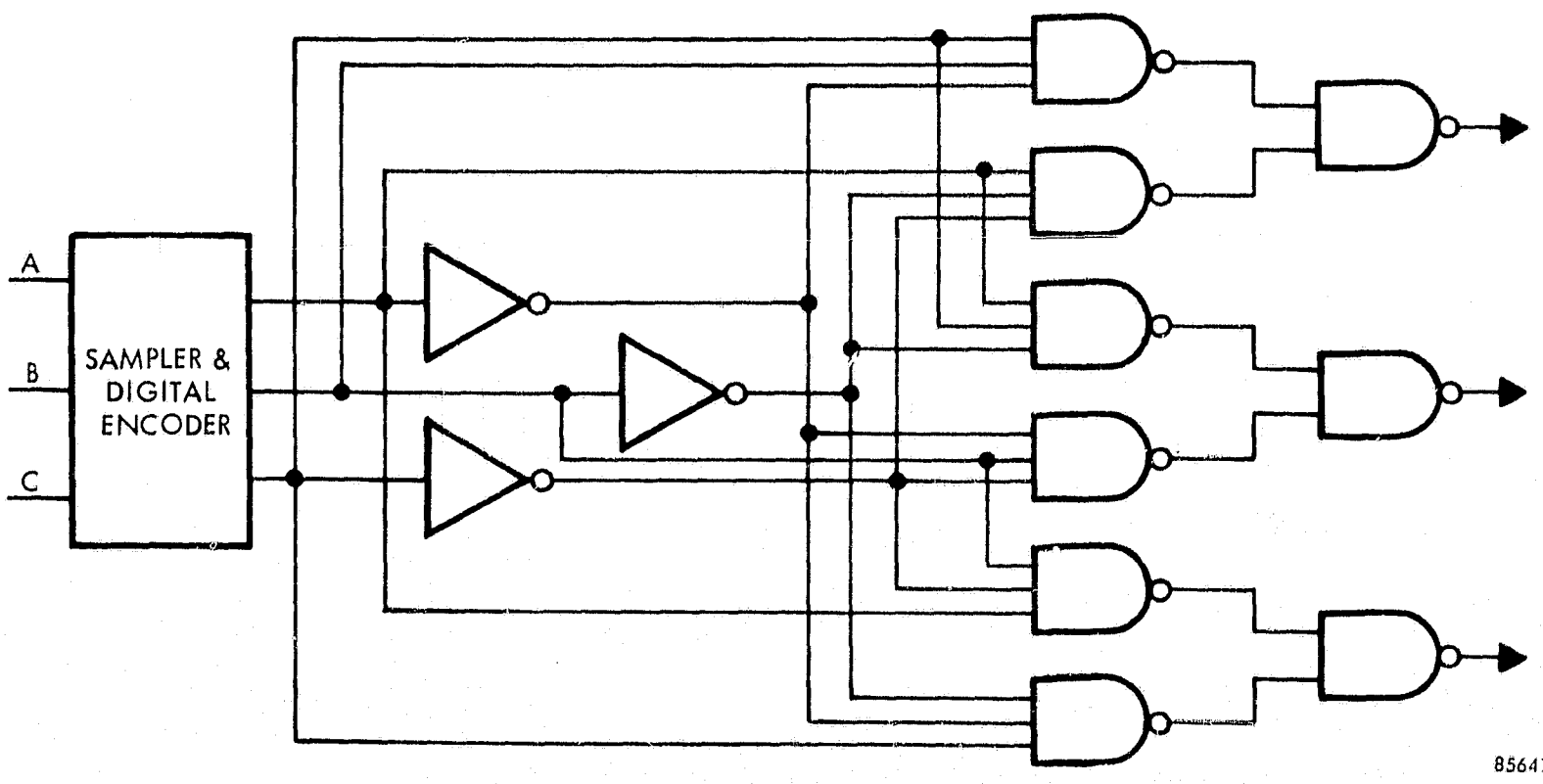


IMPLEMENTATION A



IMPLEMENTATION B

IMPLEMENTATION B



IMPLEMENTATION C

Figure A3 . Voting Techniques - Some Sample Implementations

Perhaps a strong advantage of Voting techniques is that input status will usually not be required for a transition from conditional status to status. If indications are that two of three outputs agree or that all outputs agree, one will likely require only a knowledge of input admissibility before he is willing to pronounce an element status.

The three implementations shown have implicitly assumed that inputs ABC may require sampling, quantization, or digitization. Certainly, it may be the case that the signals to be polled are already in such a form that they may be directly applied to the logic; for example, if A, B and C were bilevel bit streams.

If the approach chosen were Voting on a digital basis, Voting procedures could be handled by computer, either special purpose or a large general purpose machine.

While sampling rates would affect the confidence and accuracy of Voting, there is no minimum placed on sampling rate as is the case with spectral analysis. It is conceivable that, for a clean digital bit stream, one would be satisfied to vote on one bit out of every ten, one-of-fifty, or one-of-one-hundred.

Voting methods are applicable only to distinguishable element outputs.

Timing information need not be supplied to Voting equipment. The only important factor is that element outputs are allowed to vote in a synchronous fashion.

Because of the simplicity and inexpensiveness attributable to voting equipment, it would not likely be attractive to time-share Voting equipment among sets or elements. An exception would be when computer implementation was used and then sharing should be a simple matter.

Type I errors may occur due to system noise or failures in verification equipment; also, lack of accuracy due to quantization may result in Type I errors though this can be avoided by careful design. Type II errors will be very unlikely in verification by Voting. However, one should consider the possibility of two elements failing in the same way. If this happens in a triple redundant configuration, both Type I and Type II errors may occur; two failed elements could show good while one good element would show bad. Similar failures in all three elements would result in an indication that full redundancy was present. The likelihood of such occurrences is not so remote if the elements contain digital logic. It is very common for such equipment to fail by "locking up" in one of its legitimate states. Also, total loss of signals from elements might result in an indication of unanimity.

The simple and straightforward nature of Voting leads one to expect that mapping to status and display of status will usually be uncomplicated. Equipment required to display status, then, could probably be as simple as two or three lights.

To avoid errors in verification, equipment voting on element outputs should be located in proximity to the IBV's. If samples of element output are digitized before voting, these digitized samples could be transmitted for voting elsewhere with no loss of accuracy.

Unsymmetrical redundancy will affect the applicability of Voting techniques only insofar as the element outputs differ. If elements perform their functions in different manners but have identical outputs, it is of no consequence. The degree of dissimilarity which can be accommodated by the Voting equipment without sacrificing verification confidence will be entirely dependent on the nature of the dissimilarity and the particular situation.

It is obvious that, if elements require prime power, all elements to be involved in the polling procedure must be powered up. This could be of concern if power consumption were critical or if an off-line equipment situation exists.

Voting techniques would probably not be a good choice for verification in low S/N ratio situations, since the effect of noise could cause apparent disagreements when, in actuality, all elements were operating properly.

As with Compare Two, the fact that element outputs are being compared against each other, rather than against a stored reference, probably represents some sacrifice in accuracy since it must be allowed that outputs may go to opposite extremes within their range of tolerance with no indication of disagreement.

Voting Techniques - Relative Advantages

- Simple, reliable, and inexpensive implementations available
- Can be made to identify element status
- Requires only admissible input for status determination
- Implementation by simple computational machines possible
- No restriction of minimum sampling rate
- Simple development of status variable, mapping to status, and display of status

Voting Techniques - Relative Disadvantages

- Unable to distinguish among failure types
- Less accurate than comparison against a stored reference
- May be affected by unsymmetrical redundancy
- Requires all polling elements to be powered
- Not advantageous in low S/N ratio situations
- For, say, a three element case, the techniques are unable to give a conclusive status indication when two failures occur
- If an element must be added to a set to achieve the technique, the final design can be noncompetative from a cost and utility standpoint.

A4.0 CROSS POWER SPECTRUM TECHNIQUES

The Cross Power Spectrum technique of coincidence development consists of taking the cross-spectrum of output pairs of the redundant elements in a simple set. This results in a qualitative measure of the amplitude and phase similarities of each frequency present in the outputs. The measure can be normalized by computing the coherence function from the cross-spectrum. Naturally, the technique is limited to analog signals.

The interpretation of the cross-spectrum is rather limited in scope without a priori knowledge of both the spectral content of the input signal and the element transfer function. Even this knowledge may not explain some high values of coherence at frequencies which were not expected to be coherent. A high cross-spectral measurement at some frequency may be attributed to a strong gain of the two elements at that frequency, or to a large input at that frequency, or to strong contaminating noise common to both elements. Thus, the only feasible way of interpreting the cross-spectrum or coherence measure is by simply ascertaining that the coherence is high for any pair of outputs, over the frequency range of interest. The lower limit for "high" coherence will depend on the elements under consideration. Noise on the input to the elements will not degrade the coherence, since it should appear in the same form on the outputs of the elements. However, the noise added internally by each element will be incoherent with all components, and will thus degrade the overall coherence. Other factors which will affect the degree of coherence are the tolerances of the components in the elements and any external noise sources which affect one element more than the others.

Another possible means of interpreting the cross-spectrum would be to compare the cross-spectrum of the two outputs with the auto-spectrum of one output. For identical signals, these spectra should be the same. The results of this comparison would form the coincidence variable.

The Cross Power Spectrum technique is essentially a "Compare Two" in the frequency domain. As such, it requires first degree redundancy to determine that a failure has occurred and at least second degree redundancy to identify the status of the individual elements (a Voting technique). It has the advantage over the Compare Two techniques of being a more thorough comparison, but it also requires more hardware and time to generate the comparison.

Any admissable input may be used, including the tenant signal, or even a random noise input. Thus the S/N ratio of the input signal has no deleterious effect on the usefulness of the method. The Cross-Spectrum technique does not require dedication of principal system elements. A frequency limit is imposed by the type of sampler used, since the maximum frequency which can be resolved by the cross-spectral process (the Nyquist frequency) is one-half the sampling frequency. Any frequencies in the output above the Nyquist frequency should be removed with a low-pass filter to avoid aliasing error. Sampling rates of up to 10 MHz should be possible with current equipment.

The Cross-Spectrum technique is capable of indicating the degree of failure within an element. Out-of-tolerance failures result in reduced coherence between outputs, whereas

loss-of-signal failures result in zero coherence. Since a general purpose computer performs all analysis of the sampled data, many possibilities exist for the definition of the coincidence variable. This variable could be simply the value of the coherence function, or it could be a complex function of coherence and frequency.

The technique's usefulness is diminished in cases of unsymmetrical redundancy comparisons, because the spectral content of the element outputs is likely to differ. The method may still be useful when the coherence suffers only small decreases.

The only equipment which must be located in closs proximity to the IBV's is the sampling and digitizing equipment. Once digitized, the sample data may be recorded or transmitted to the computer for analysis. No other requirements exist for location of equipment.

The data is sampled simultaneously from pairs of outputs, so time-sharing of the sampling equipment is certainly possible. This sampling in pairs makes it necessary to power up two elements simultaneously for redundancy verification, but then need not remain on after sampling. Only two sampling and digitizing devices are necessary, and these can be manually or programmably switched to different elements.

The reliability of sampling equipment is generally very high, so the computer reliability limits the reliability of the verification equipment.

Type I errors will be primarily due to failures in the sampling equipment. The most common failure is for one or more bits out of the analog-to-digital converter to be locked on one state. This type error would be difficult to distinguish from prime system failures, because either one would degrade the coherence. Since the sampling equipment has high reliability, however, the likelihood of Type I errors is small.

Type II errors should never occur, because the sampling heads operate independently of each other. If one element failed, its sampler will not be connected in any way to the output of the other element, so the coherence should be zero.

In general, the Cross-Spectrum technique can be applied to any functions within a pair of elements for which the same spectral content is anticipated. It may also be used for indirect sensors, provided the outputs are expected to be the same.

The advantages and disadvantages of the Cross-Spectral technique are summarized below:

Cross Power Spectrum - Relative Advantages

- The input need only be admissible
- S/N ratio of input does not affect usefulness of method
- Any admissible signal, including tenant signal, may be used
- May be made able to identify failure type
- Allows great freedom in formation of coincidence variable
- Time-sharing of sampling equipment is possible
- Provides a comprehensive indication of element operation

Cross Power Spectrum - Relative Disadvantages

- Limited to analog signals
- Requires first degree redundancy to detect an error; second degree redundancy to identify element status
- Technique is not as useful for unsymmetrical redundancies
- Necessary to power up two elements simultaneously
- Time and expense are greater than for simpler techniques

A5.0 VALUE CHECK; SEQUENTIAL TECHNIQUES

Sequential Value Checking techniques have a great deal in common with Nonsequential Value Checking techniques. Many of the statements made here will also appear in the discussion of the nonsequential techniques. The major distinction between the two is that here information concerning status is contained in signal values and in their order of occurrence. In Nonsequential, order-of-occurrence is of no interest.

Sequential Value Checking is one of the monitor methods and, as such, carries the requirement of a priori signal knowledge. Indeed, a deterministic signal is required since verification equipment is expected to "know" what values are acceptable and in what order they should occur. This requirement is obvious from the matrix of Figure 5.2.2.2-5.

The fact that time-sequential values are to be observed implies a process that is discrete in time. Where discreteness in time is not a characteristic of the signal under observation, it can be established by quantization, sampling, or digital encoding. Comparison of signal values with stored values may be accomplished on a continuous or a discrete basis. The use of unquantized signal samples for comparison would be a continuous realization; digitized signal samples represent a discrete value comparison. An analog signal such as a sine wave would generally not be compared without sampling since an entire waveform rather than discrete values would have to be stored; a bilevel bit stream out of a piece of digital equipment would already be discrete in both time and value.

Sequential Value Checking equipment will, in general, require timing information or synchronization capabilities since it must know when the sequence of values to be checked is in progress. Often, the achievement of synchronization through the use of digital logic will be relatively simple.

When element outputs are time multiplexed signals, Sequential Value Checking will be a definitie candidate. The serial bit stream will already contain synchronization information so that the establishment of timing should be a simple matter.

Like Nonsequential Value Checks, these techniques require a knowledge of input status to allow the conversion of conditional status into status. As has been pointed out, this requirement along with that of a deterministic signal will in some cases result in the necessity of dedicating principal system equipment to verification procedures.

Value check methods will be inherently more accurate than those techniques which compare output signals against each other since here one constituent of the comparison is a reference which can presumably be made very precise.

As with the nonsequential case, no minimum is placed on sampling rate since there is no concern over output signal information loss. If sampling is to be employed, sampling rate will be determined by the rate-of-occurrence of the values to be observed and the level of confidence to be demanded of the verification.

Equipment for comparing sequential signal values can be made simple and reliable. The ease with which timing is established will vary greatly with the situation. In some cases, timing will be available from principal system equipment; in another case, verification equipment may be asked to synchronize to a quantized form of the signal to be observed. Obviously the requirements of the second case may lead to the use of sophisticated equipment.

Sequential Value Checks can be given the ability to detect a large number of failure types. Their sensitivity to excessive noise can be adjusted through the parameter estimation scheme employed. Since information is available from both the values and the order of their occurrence, the potential exists for these techniques to be more comprehensive than nonsequential checking, but only an investigation of failure modes of the principal system equipment will reveal whether the identification of failure types is possible by sequentially checking values. That is to say, if all failure modes effect each value in the sequence in the same way, no discrimination among types of failures will be possible. The order-of-occurrence information, then, will be entirely involved in the establishment of verification confidence.

Sequential Value Check will have the ability to yield information on individual elements of the set, not only on the status of the set.

Computer implementation, either by special or general purpose machine, is a definite candidate approach to value checking.

The shareability of Sequential Value Checking equipment among element outputs could be extensive. The degree to which equipment would be sharable among sets would likely be limited due to the different timing requirements which would generally exist between different sets and, less importantly, the requirement for storing more sequences of values. If the sequential checking were implemented by logic gates and/or shift register, the design of these would be with consideration for the equipment to be verified and the signal to be observed. Their adaptability to other principal system equipments and signals would likely be small. If implementation were by computer, the machine could act simply as several sets of verification equipment, selecting the proper functions for the equipment and signal under scrutiny.

The general rule for flexibility in the location of equipment will be observed for these techniques; if signal samples are encoded for comparison, transmission of these encoded samples can likely be accomplished with little sacrifice in verification confidence. If nonencoded samples or analog values are chosen for comparison against reference values, this comparison should be performed before any transmission is attempted.

The use of unsymmetrical redundancy will usually not affect the applicability of Sequential Value Checking, though it may complicate or negate the sharing of verification equipment among element outputs.

Since value checks may be performed on one element at a time, if elements require prime power this power need be applied to only one element at a time for value checking. This is in contrast to what is true for Compare Two and Voting Techniques.

The requirement of timing information, generally imposed by sequential value checking, should be viewed as an additional source of Type I errors since bad timing can cause a disagreement between signal values and stored values even though the signal is entirely proper. Of course, bad timing can also cause Type II errors, though it will usually be highly unlikely. Also, attempts to share verification equipment among sets opens the possibility of checking against the wrong set of stored values. Sequential Value Checking techniques are not tolerant of legitimate system errors. If a value does not check "good," the equipment has no way of determining whether the cause is a failure or an error. The effects of such legitimate errors, as well as those of noise, may be minimized through parameter estimation procedures.

Value Checks; Sequential - Relative Advantages

- Simple implementations available
- More accurate than Compare Two and Voting techniques
- No severe restriction on minimum sampling rate
- Computer implementation possible
- Able to identify status of individual elements

Value Checks; Sequential - Relative Disadvantages

- Requires deterministic signal
- Requires timing information
- Usually not applicable to set output
- Requires knowledge of input status for determination of equipment status
- May require dedication of principal system equipment to checking
- Limited in ability to distinguish among failure types
- Timing requirements introduce additional source of errors

A6.0 VALUE CHECK; NONSEQUENTIAL TECHNIQUES

Being one of the monitoring methods, the employment of Nonsequential Value Check techniques entails the comparison of a signal parameter value against a stored reference value. Obviously, then, the requirement that expected values be available is imposed. In fact, the general requirement is that the signal under investigation be deterministic. This is reflected by the matrix of Figure 5.2.2.2-5.

Implementations of these techniques may be of a continuous or discrete nature, both in time and value. For example, the direct comparison of a DC voltage against a fixed threshold is continuous in time and in value. The sampling (at the frame rate) of a bit stream in order to check the presence of a frame marker bit would be discrete in time and could be either continuous or discrete in value depending on whether the sampled value were quantized (discrete) or not (continuous) for comparison against the reference value.

Value Check techniques, like other monitor methods, are, in themselves, capable of giving only an indication of conditional status. To make a statement of set status requires knowledge of the status of the input. This requirement, along with that of having an input of deterministic nature could severely limit the use of these techniques when it is undesirable to dedicate principal system equipment to verification.

Because signal output is compared against a stored reference which is presumably very stable and noise free, the degree of accuracy achievable with value check techniques generally will be greater that with those techniques which compare element outputs.

A relative disadvantage must be accorded to these techniques when it is desired to check values which are not constant in time, for then it is required that verification equipment be given timing information or the ability to derive such information. While timing information may be required, no restriction on minimum sampling rate is imposed as it is by Spectral Analysis. That is, there is no interest here in compiling a sample set which completely describes the waveform. So, to the extent that the designer is satisfied with the level of confidence achieved, a signal value may be sampled for verification purposes at the rate of its occurrences or at any subharmonic thereof.

The reliability achievable in Nonsequential Value Checking equipment will vary widely with the choice of implementation. Wherever synchronization capabilities are required, reliability of verification equipment will suffer. In the simplest cases, such as that of comparing a DC voltage against a threshold, simple and reliable equipment may be used. More complicated and less reliable equipment would be required to check frame marker bits, for example.

Value Check techniques, while not nearly so comprehensive as Spectral Analysis and some other techniques, are capable of detecting numerous failure types. But here again, the characteristics and capabilities of the verification equipment is a strong function of the degree to which its design considers the signal being checked and the nature of that signal. A peak voltage detector, for example, would be relatively insensitive to signal distortion and the

addition of excessive noise; in the comparison of the DC voltage against a threshold, both of these failure types could be detectable. However, the general and significant statement may be made that Nonsequential Value Check techniques are not capable of distinguishing between or among types of failures. They are at the most able to point out that something is of ill order.

It is characteristic of this class of techniques that they identify the status of the individual elements - not only the status of the set.

Computer implementation of Nonsequential Value Checking is a feasible approach. Encoded samples of signal values could be provided to a computer for comparison against a stored reference value. For such a simple operation, however, a small special purpose computer with values stored in read-only memories might be a more cost-effective choice than a general purpose machine.

Value checking equipment would be readily sharable among element outputs. If the value to be checked occurred only periodically in the element outputs, the choice facing the designer would be whether to sample all element outputs simultaneously and store the samples for sequential comparison against a stored value or to use no storage and dedicate the equipment performing the value comparison to one element output at a time. The first technique would require sampling; the second might or might not involve sampling.

Because of the simplicity of the concept of checking an actual value against a stored value (and the limits of derivable information thereby placed), reporting and display requirements for a value checking system will be minimal. Likewise, the development of a coincidence variable will be far less complicated than for, say, Correlation and Spectral Analysis techniques.

As with other classes of verification techniques, flexibility in the location of verification equipment will be dictated by the implementation chosen. If signal samples are encoded for comparison, transmission of these encoded samples can likely be accomplished with little sacrifice in verification confidence. For analog or non-encoded samples, comparison against the reference should be performed, and thus the status variable would be developed, before any transmission.

While the use of unsymmetrical redundancy may complicate the design of value checking equipment, the applicability of the technique will seldom if ever be negated by the fact that element outputs differ somewhat or by the fact that elements have different capabilities. The greatest impact of unsymmetrical redundancy on value check techniques would be in the case that is is desired to share verification equipment among element outputs. Here, differences in element output due to lack of symmetry could force the design and construction of additional verification equipment.

Value Check equipment could also be shared among sets. Most amenable to such usage are the computer implementations because of the ease with which several reference values may be stored and the ability to program the equipment to call forward the proper reference. In other implementations, switching arrangement could be set up to select proper references for various set outputs or element outputs within the various sets.

For cases where it might be desirable to check off-line equipment, it would be necessary to power up only one element at a time for checking purposes. This is an advantage which would probably be seldom realized.

For the Value Check implementations for which timing information is required, and additional source of both Type I and Type II errors is provided. If timing information were incorrect but the signal actually good, a Type I error could occur; if both were incorrect, a Type II error could occur, though for most situations the likelihood of this would be low. Where set-shared equipment is involved, errors could result from comparisons against the wrong reference value. System noise, as is usual, is a source of Type I errors; also these techniques may give incorrect status information because of legitimate data errors. The effects of both noise and data errors may be minimized in the parameter estimation function.

If these is interest in storing information for trend evaluation, value checking methods can certainly provide this.

Value Checks; Nonsequential - Relative Advantages

- Simple implementations available
- More accurate than Compare Two and Voting techniques
- No severe restriction on minimum sampling rate
- Computer implementation possible
- Able to identify status of individual elements
- Simple development of status variable and display

Value Checks; Nonsequential - Relative Disadvantages

- Requires deterministic signal
- May require timing information
- Usually not applicable to set output
- Requires knowledge of input status for determination of equipment status
- May require dedication of principal system equipment to checking
- Unable to distinguish among failure types
- Timing requirements introduce additional source of errors

A7.0 CODING TECHNIQUES

Coding techniques are basically methods contrived for the detection of errors, not for the achievement of the verification of redundancy. However, when error-detection coding is present in distinguishable element outputs, the potential for their use in redundancy verification exists. Probably the simplest example is the case of an element which outputs a digital data stream containing parity bits. Depending on the design of the system, some percent of message errors would be acceptable - say 1%. Then it is likely that, if a simple accounting system revealed that 20% of the messages being received contained bad parity, one would be willing to concede that a failure had occurred. Least the obvious be overlooked, this also implies that Coding techniques will detect failures (e.g., locked logic circuits) in equipment.

As considered here, verification by coding will provide information on the status of individual elements.

A statement of which or even how many types of failures are detectable through coding is difficult to make because of the strong dependence on principal system design. However, it may be pointed out that "failures" occurring between the points of encoding and error detection which do not result in message errors are likely of little interest.

Type I and II errors due to the verification equipment itself are both very unlikely with this technique (considering that a very clean signal will probably be provided as element output). Also, some tolerance to legitimate principal system errors is already built in. The principal contributer to Type I and II errors is the code itself. With careful design of the code, the probability of these errors can be made quite small.

Encoding and decoding equipment for these uses (especially for simple parity checking) is relatively simple and reliable. About the equipment necessary to extend error-detecting capabilities to redundancy verification capabilities, the same may be said.

It would be unlikely that unsymmetrical redundancy would influence the applicabilitiy of these techniques.

The sharing of Coding verification equipment would generally be undesirable because of the necessity of extensive error counting on any given element output. However, the cost of designing equipment to be dedicated to individual element outputs should be such that lack of sharability would be no cause for concern.

Because of the necessity to assume that encoding was done correctly, this is another class of techniques which requires knowledge of input status in order to go beyond a statement of conditional status to a statement of status.

Coding Techniques - Relative Advantages

- Able to identify element status
- Simple implementations available
- Low likelihood of errors in statements of status
- Unlikely to be affected by unsymmetrical redundancy

Coding Techniques - Relative Disadvantages

- Applicable only to digital systems
- Generally not compatible with concepts of shared verification equipment

A8.0 SIGNAL FORM ANALYSIS TECHNIQUES

Signal Form Analysis techniques involve the derivation of some indicator of signal form (rms value, mean value, variance, instantaneous frequency are examples) for comparison against a reference value.* By virtue of this comparison to a reference, the requirement of a priori knowledge of the signal under observation is imposed. However, the instances for which signal form characteristics are predictable can be reasonably expected to outnumber by far those for which signal values are predictable. The requirement for the application of these techniques is that a deterministic property be present.** If the property is reflected by a value which is constant in time, no timing information would be needed. Peak detection applied to an FM signal would be an example of Signal Form Analysis with no requirement of timing information.

The development of many signal form indicators such as rms value, mean value and variance require integration time or the collection of a sample set. This does not, however, negate the possibility of continuous verification since the definition thereof allows reasonable delays for processing. If characteristics such as those named above vary as functions of time, observation of such characteristics by integrating or collecting sample sets will complicate the determination of how closely the observed values should agree with the stored reference and would undoubtedly mean a sacrifice in verification accuracy. Hence, it is a good general statement that a characteristic value will be required to be constant and known over many periods of the lowest frequency present. Then any requirement for timing will be only for gross and relatively inaccurate information.

Signal Form Analysis will most often be applied to element outputs. When this is the case, it will be within the capabilities of these techniques to identify the status of individual elements, not only to identify set status.

An obvious point is that, if Signal Form Analysis is to be applied to set output, the signal characteristic to be observed by the verification equipment should be one that varies as a function of the number of operating elements. For application to set output, the ability to identify the status of individual elements will be lost.

The number of failure types detectable through the use of these techniques will be principally determined by the number of failure types which evidence themselves as variations in the signal characteristic under observation - the rms value of a signal out of an oscillator will not generally disclose frequency drift. The comprehensiveness permitted by these techniques, it is apparent, will be determined only by analysis of the particular situation in which their application is contemplated.

---

*These descriptions are called signal characteristics, in contrast to signal values used in Value Check Techniques.

**This statement deserves some comment. Not that statistical properties have been included among the signal form characteristics. This does not conflict with the deterministic requirement of the technique. Population means and variances are deterministic parameters; even if they are statistical representations.

Depending on the signal characteristic to be investigated, implementation may be either on an analog or on a discrete basis. Mean and rms values of analog signals will be easily derived on an analog basis; the variance of a stochastic signal would more likely be determined on the basis of a sample set. Sampling techniques will generally be applicable to the investigation of signal characteristics. It will be usual that those properties which are amenable to analog implementations can be observed on a sampled basis. An exception is the characteristic of instantaneous frequency. Also, the desire to investigate frequency on a sampled basis will set a minimum on sampling rate. As a rule, for the investigation of signal characteristics other than instantaneous frequency, minimum sampling rate will be determined only by the requirements of verification confidence, a design input. Characteristics such as mean, variance, and rms value may be determined by sampling on a "slow" basis (slow by comparison to signal frequencies) or on an aperiodic or random basis.

These techniques involve both the process of extracting an indication of a signal characteristic and the comparison of this indication against a stored reference; and both of these functions might be performed on a digital basis. As an example, a signal could be sampled and these samples digitally encoded. A computer could then determine the mean of the sample set and compare the derived value against a stored reference value.

The reliability of the verification equipment for Signal Form Analysis will vary over a wide range, depending on the signal property chosen for investigation and on the selection of a basis of comparison. Some of the simplest implementations, such as an envelope detector to determine peak amplitude, may be made very simple and reliable. Equipment to sample and compute a mean, though certainly not failure-prone, would fall far below the envelope detector in reliability. By comparison to swept frequency mixing and FFT implementations of Spectral Analysis, the use of these techniques will usually result in good reliability of verification equipment.

In contrast to some other techniques, the inherent time delay of this technique will typically allow erroneous information to be transmitted before an unacceptable status indication is realized. This could be a drawback for large filter constants with critical information. Trading off shorter filter constants with the probability of error will inevitably result.

Equipment required to implement Signal Form Analysis techniques could be shared among the elements of a set without complication. For symmetrical redundancy, both the equipment examining the signal characteristic and that performing the comparison would be sharable. One implication of unsymmetrical redundancy might be the necessity of dedicating the property-examining equipment (such as the peak voltage detector) to a particular element; also, a different reference value might need to be supplied for each element. But comparison equipment along with that performing the functions of parameter estimation and mapping would be sharable among elements.

The design of Signal Form Analysis equipment would usually be specialized to the iBV and the signal and would, hence, likely be unsharable among sets.

For signal observations which require integration or sample collection, the likelihood of errors, both Type I and Type II, attributable to the coincidence development function would be determined by the accuracy built into the equipment versus the accuracy asked of the equipment. That is to say, for a given degree of accuracy, the tighter the tolerances placed on the comparison, the more Type I and the fewer Type II errors would be expected. For other signal observations, such as the checking of instantaneous frequency, system noise would also be a source of Type I errors.

Signal Form Analysis - Relative Advantages

- Allows continuous verification
- Computer implementation possible
- May be applicable to set output
- Requires one powered-up element
- Able to identify status of individual elements

And, depending on the signal property of interest,

- No severe restriction on sampling rate

Signal Form Analysis - Relative Disadvantages

- Requires input status to allow transition from conditional status
- Usually unable to identify as many kinds of failures as techniques observing signal values or spectral characteristics

And, depending on the signal property of interest,

- Restriction on minimum sampling rate

A9.0 SPECTRAL ANALYSIS TECHNIQUES

Spectral Analysis techniques are comprehensive and generally complex and expensive. Their implementations may take the form of swept frequency mixing, filters, chirp filters, autocorrelation equipment, or a computer performing fast Fourier transforms. All these implementations are concerned with the investigation of a single signal. This signal may be a set output if elements failures are reflected as changes in the spectral content of the set output. More often, Spectral Analysis will be applied to an element output.

As with all monitoring techniques, the requirement of a priori knowledge is present. Here, the requirement is placed on the frequency content of the signal under investigation. In many cases, the necessity of an output with known frequency content will mean that an input will have to be provided; this, in turn, would require the dedication of prime system equipment to verification.

The types of failures detectable by Spectral Analysis are almost without exclusion and, certainly, it is difficult to imagine that one would be interested in any failure which would not cause a change in signal spectral content. Loss of signal, excessive noise, and signal distortions are all detectable by some of these implementations, and, significantly, these techniques offer the potential for going beyond the detection of these failures to a statement of the nature of the failure. In the usage imagined as most common for these techniques, the scrutiny of an element output, identification of the faulty element (as opposed to only the indication of some level of redundancy) may be a valuable capability.

Spectral Analysis by filtering might be achievable rather simply in certain instances. Most often, however, a bank of filters or a set of swept filters will be required. Along with this implementation the other forms of Spectral Analysis must be rated as comparatively complicated and requiring much maintenance.

A result of the ability of these techniques to furnish great amounts of information may be a complicated process for the development of a coincidence variable. One could require simultaneously, for example, that third harmonic content be in a certain ratio to the fundamental, that the fundamental be within certain ranges of amplitude and frequency, that even harmonics be missing, etc., so that the display of information desired or the development of a simple statement of primary system "goodness" therefore becomes a sizeable task within itself.

Spectral Analysis may be implemented using sampled data. One possibility is the generation of an autocorrelation function directly from the samples; a second possibility is the encoding of sample values for analysis by Fast Fourier Transform (FFT) methods. In the former implementation, sampling rate would not be critical - could in fact be done on a random basis. In the latter implementation, sampling rate would be critical; the Nyquist sampling criterion would have to be observed and the fixing of a sampling rate would imply an assumption of fundamental frequency.

In at least one form, namely Spectral Analysis by the generation of an autocorrelation function, the verification equipment would tend to reject random components of the output. This should be counted as an advantage when the output to be investigated possesses a low S/N ratio, since the signal could be retrieved from the noisy background. On the other hand, if the addition of excessive noise by the IBV were a failure type of interest, the inability of this implementation to detect this noise would be disadvantageous.

The reliability of verification varies widely depending on the choice of implementation. Where passive filters or chirp filters (tapped dispersive delay lines) could be used, relatively good reliability would be achievable. Swept frequency mixing would be significantly less reliable. For the case of computer analysis of sampled data (FFT and autocorrelation), naturally, the reliability would be the same as for any other verification technique using computer analysis of sampled data. However, the fact that Spectral Analysis might impose the requirement for more complicated sampling equipment than that needed for other techniques (notably Compare Two and Voting) could mean less reliable verification equipment.

There is nothing inherent in any of the implementations of Spectral Analysis which should preclude the time sharing of verification equipment. Where such sharing is contemplated among set outputs, the choice of implementation should consider the fact that swept frequency mixing, chirp filters, swept filters and autocorrelation require the least attention to the particular signal under scrutiny (though general limitation on frequency range must certainly be observed). For fixed filters the restrictions are obvious. The sharing of equipment to perform Fast Fourier Transforms is certainly feasible, though sharing among different signal types would demand that sampling rates be tailored to the particular signals. In other words, while the processing could be shared among sets; sampling and preprocessing equipment would generally have to be dedicated to a set.

All these Spectral Analysis implementations are capable of constant verification, but two practical considerations might make this undesirable:

a. The expense of most Spectral Analysis equipment makes the sharing of verification equipment very attractive.

b. Many real-world signals will have neither constant nor predictable frequency content; the situation then would require that a set input be provided (probably a simulative signal) and this, in turn, would require the dedication of prime system equipment to verification.

The computer-based implementations of Spectral Analysis may exhibit limitations on the speed of verification. FFT, though achievable through algorithms which reduce computational redundancies, is a time-consuming process in itself. Of less direct influence is the fact that, in order to make efficient usage of computer capabilities, a machine would probably be shared and the verification time of any element or set would be determined primarily by the computer's load.

It is true of Spectral Analysis, as it is of the other three monitoring techniques, that the transition from a statement of conditional status to one of status requires knowledge of input status. This must be considered less desirable than the requiring of only an admissible input as is the case with some other techniques.

The primary sources of Type I errors in these techniques are failures in the verification equipment and system noise. Autocorrelation processing virtually eliminates the threat of errors due to noise. But where a requirement for rapid autocorrelation leads to the use of a "batch" sampling method (this is a method whereby a sampling rate much higher than those for complete sequences of delay, multiplication and averaging can be used) the result is an approximation to the autocorrelation function with the accuracy of the approximation being dependent on the sample size. In this case, then, there is a tradeoff between accuracy (and consequently the likelihood of Type I errors) and the time required for verification.

Unless data is encoded and sent to a computer for processing, all equipment necessary for the development of a status variable should be located in proximity to the IBV's in order to avoid noise pollution and signal distortion by transmission.

The display requirements of Spectral Analysis may be great for, when a great deal of information is derived, the only choices are to allow equipment to perform the operations necessary for reduction to a simple statement of status or to display a large amount of information.

These techniques, despite their generally complex nature, afford a good means of verification where a frequency-multiplexed signal is of concern - for example, on a data bus. Also, though the Spectral Analysis of time-multiplexed signals may require the providing of a simulative input, no synchronization information would be required by the verification equipment.

Because output characteristics are compared to a stored reference, only one element at a time (whether on-line or off-line) need be powered up.

Spectral Analysis - Relative Advantages

- Allows continuous verification
- Extremely comprehensive - detects a large number of failure types and is capable of identifying
- Analog or digital implementations available
- Computer implementation possible
- Does not require timing information
- May be applicable to set output
- Advantageous in low S/N ratio situations
- Adaptable to frequency multiplexed signals

Spectral Analysis - Relative Disadvantages

- Most implementations complex and may be expensive
- Minimum sampling rate requirement
- Requires knowledge of input status for transition from conditional status to status
- May require dedication of principal system equipment to verification
- Inherent time delay for results

A10.0 INVERSE TRANSFORM TECHNIQUES

Inverse transforms, per se, are based on the mathematical premise that the product of an equipment transfer function and its inverse is one. Then conceptually, a signal which is passed sequentially through an item having transfer function F(s) and one having transfer function $F(s)^{-1}$ will have been returned to its original form (input ≡ output). The applicability, in theory if not in practice, of these techniques is dependent on the existence of the inverse transform and on the satisfaction of mathematical characteristics implicit in the statement above. Firstly, the system (not the signal) must be stationary in nature. That is, its transfer function may not vary in time. In practice, it will be sufficient if the system is piecewise stationary and either is predictable in its time-variant behavior or is able to provide timely data on its own form. To see this, consider an amplifier whose gain is time-variable. Neglecting other parameters such as phase characteristics, if one knows the amplifier's (piecewise invariant) gain over a given span of time, a suitable amount of attenuation may be set up to provide the inverse operation. Knowledge of gain values may be had either by prediction or by the amplifier providing, as a separate output, gain information.

A second assumption implied by the use of frequency domain transfer functions is that the system is linear; i.e., the principle of superposition applies to the system because it is both additive and homogeneous. If the time restrictions discussed above are met and the system is linear, a unique inverse transform will exist. For some nonlinear systems an inverse will exist. An example would be the nonlinear system described by

$$e_{out} = m\, e_{in} + b$$

where m and b are constants. The inverse operation is described by

$$e_{out} = \frac{e_{out} - b}{m}$$

A nonlinear system for which a unique inverse does not exist is described by

$$e_{out} = k\, e_{in}^{2}$$

since a solution for e_{in} is

$$e_{in} = \pm \sqrt{k\, e_{out}}$$

and an ambiguity in sign exists. Still, if verification equipment could be given a rule for resolving the ambiguity, perhaps through the knowledge that e_{in} was always a positive quantity, inverse transform would be possible.

In short, if a system is linear and stationary a unique inverse transform will exist. If these conditions are not met, only an investigation of the particular system to be verified will prove applicability of these techniques.

As an example, consider a A/D converter. This is certainly a nonlinear operation. The inverse operation might be performed by a D/A converter. In this case the problem in inversing arises from the fact that the reconstructed input signal suffers the effects of quantization errors. The acceptable degree of coincidence between this signal and the input signal which should be demanded, may be a difficult matter to resolve.

A lack of unique inverse operation may be observed in the case of a limiter or clipper. A loss of information occurs in the operation which cannot be compensated for in the inverse operation.

The Inverse Transform Technique can be a very comprehensive one. With the assumption that all principal system failures of interest will be reflected as changes in that system's transfer function, the types of failure detectable becomes limited only by the accuracy of the verification equipment. Generally, then this will be a very comprehensive approach to the problem.

The ability of verification equipment to distinguish among failure types is dependent on the method of comparison employed. If this comparison is by simple subtraction, no capability in this area will be realized. If comparison is by correlation, the potential for identifying failure types is great. (However, if correlation is to be involved, it might be more cost effective to eliminate the Inverse equipment and go to Correlation techniques entirely.)

The Inverse Transform Technique is capable of providing information on the conditional status of individual elements and will usually be applied to element output. When element transfer functions are observable constituents of a set transfer function, a transform may be introduced which is the inverse of that for the set, thus performing verification on set output rather than on element output. In either case, it is true that the verification equipment must be designed specifically to suit the equipment which it is to verify. This infers that a given set of verification equipment will be inflexible and only rarely will be sharable among sets.

Most implementations will require the comparison of input and inverse-transformed output without deletion of information from either. Therefore, if sampling is to be used on either input or output, the Nyquist sampling criteria should be observed. In effect, a lower bound is thereby set on sampling rate. It is unlikely that inverse operations performed on a sample set which cannot fully represent the output signal will lead to useful results.

At least two possibilities for implementation exist. One choice is the construction of dedicated equipment which operates real-time on the output signal. An example of this is the attenuator performing the inverse operation on amplifier output. A second choice is to digitize output signal and, by employing algorithms, perform the inverse operation. This would necessarily be non-real-time and storage of the input until the completion of the inverse operation would be required. Naturally, there would be quantization errors involved here. An

advantage of the second choice would be that the storage of several inversing algorithms would render a computer sharable among sets.

An advantage of Inverse Transform over monitor methods is that only knowledge that the input is admissible will be required to transition from conditional status to status.

Additionally, as inspection of the matrix of Figure 5.2.2.2-5 shows, nothing concerning the form or statistics of the signal used for verification need be known a priori . This may be a tremendous credit to this technique.

The potential for Type I errors will be higher when Inverse Transform is used than is the case when other techniques are employed. This is because unallowed-for inaccuracies in verification equipment and almost all failures in equipment performing the inverse operation will result in a false indication of poor performance. In many instances the equipment performing the inversing will be complex in nature, costly, and comparatively (with respect to other candidate techniques) unreliable.

This technique is capable of performing continuous verification. When the equipment performing the inverse operation is shared, the sharing would have to be on an automatic basis in order that verification qualify as continuous.

Since no knowledge of the signal being observed is required and no knowledge of input status is necessary, there will be no need to dedicate equipment to verification.

The likelihood of Type II errors will be determined almost entirely by the accuracy of the verification equipment.

Sensitivity of the verification equipment to noise added by the IBV will be determined by the accuracy of verification equipment and by the form of estimation. Note that, in this technique, verification equipment increases the noise level of one of the inputs to the comparison.

Requirements for display and for the development of the status variable are quite flexible and are dependent on the degree of comprehensiveness desired of the verification process. It would always be possible to condense status mapping to an expression of two possible states ("go-no-go" or good-bad"). If comparison were by correlation, for instance, a great deal of information would be made available to develop a coincidence variable, to be displayed (perhaps for mental mapping to conditional status), or to be discarded.

Inverse Transform will not be a good choice for verification when element outputs which have been time multiplexed are to be observed since the multiplexing represents a nonlinear operation. In other situations, Inverse Transform equipment will not require timing information.

Inverse Transform - Relative Advantages

- Allows continuous verification
- Capable of detecting numerous types of failures
- Computer implementation possible
- Does not require timing information
- Requires only admissible input
- Can be made able to distinguish among failure types
- Able to identify conditional status of individual elements
- Requires only one powered element at a time
- May be applicable to set output
- No a priori signal knowledge required

Inverse Transform - Relative Disadvantages

- Little control over expense and complexity
- Restrictions on minimum sampling rate
- Design highly dependent on item being verified
- Verification equipment rarely sharable among sets
- High potential for Type I errors
- Verification equipment adds noise to signal under observation
- Not applicable to element outputs which have been time multiplexed

A11.0 CORRELATION TECHNIQUES

Correlation as a technique for automated redundancy verification has been accepted to mean the employment of information gathered by cross correlation of input and output signals. In general, this technique will be applicable only to linear systems. Immediately, then, any elements or sets which involve encoding or decoding (including A/D and D/A conversion) as part of their functional operation are excluded from consideration. Additionally, if the operation performed by the IBV is not stationary in nature, information on its time-variant nature would have to be provided to verification equipment.

A great degree of flexibility with regard to signal characteristics must be attributed to this approach. In general, the applicability of Correlation is not determined by the signal to be observed, but only by the nature of the operations performed by the principal system. It does happen, however, that a unique situation arises for one particular input signal. If the input is pseudorandom in nature, the result of input/output cross correlation is an expression of the impulse response of the system. Since it is known the impulse response contains all observable information about system performance and since this information may be used to predict system response to any given input, such an analysis is indeed a powerful tool. Adding to the utility of this approach is the fact that a pseudorandom input may be injected at a level 10 to 30 dB below the tenant signal to be carried as a symbiotic signal. By cross correlating this symbiotic signal (actually only a portion of the input signal) with the output, system impulse response may be obtained without disturbing information contained in the tenant signal.

The number of failure types detectable and the extent to which failure may be identified by type is dependent, in large part, on whether impulse response is the result of the correlation process. If it is, the limits of failure detection and identification depend only on the designer's willingness to provide capability in the parameter estimation and mapping functions; all the information obtainable will be available. If correlation is performed on an input signal that is other than pseudorandom, the capabilities of this approach (with regard to the two areas under discussion here) would have to be developed through analysis of failure modes and signal characteristics. A simple example might be the correlation of input and output for an audio amplifier. For such a case, loss of signal, decrease in gain, and signal distortion would show up as decreases in the peak value of the correlation function. What effect different types of signal distortion (clipping, loss of high frequencies, frequency dispersion, etc.) might have on the correlation function would have to be determined by analysis. Regardless of what input was used for verification, design of the mapping process would be highly dependent on the equipment being verified and, as is shown here, the mapping process may not be simple.

Correlation techniques provide the capability for identifying not only set status but also the status of individual elements. They are not, however, restricted to the observation of element outputs. The criterion for application to set output would be the requirement that a change in element transfer function be observable as a change in set transfer function. This criterion would usually be met. If correlation were applied to set output and if symmetrical redundancy were being verified, the ability to identify the status of individual elements would be lost.

As regards application to unsymmetrical redundancy, the choice of Correlation as an approach is an acceptable one. In fact, as was alluded to above, the presence of unsymmetrical redundancy might allow the observation of set output while retaining the ability to identify the status of individual elements. This would be true whenever the elements had different transfer functions. The application of Correlation to the element outputs of an unsymmetrical configuration may be expected to result in complications in the process of comparing against an expected correlation function (assuming the elements have different transfer functions) since what is expected will vary from element to element.

It will be desirable to accomplish correlation through the use of sampling techniques since the process requires the storage of signal values. No restriction on minimum sampling rate will exist; as a matter of fact, no requirement of periodicity will be placed on sampling - it may be done randomly. Accuracy will, however, depend on the number of sample points used to describe the correlation function.

The reliability of correlation equipment should rank low, along with the more sophisticated implementations of Spectral Analysis and Inverse Transform, because of its complexity as compared to that of Compare Two and Voting.

The correlation function must be generated by a computer. A special purpose machine which could be time shared would be a more cost effective choice than a general purpose machine.

Random noise added to the signal by the IBV will be undetectable. This would probably be disadvantageous since, wherever the potential for the addition of a large amount of noise exists, it would probably be regarded as a failure type of interest.

Because of the applicability of correlation to all signal types, the transition from a statement of conditional status to one of status will require only that an admissible input be present, not that the status of the input be known.

The potential for Type I errors will be determined mainly by the design. For a given degree of accuracy in the generation of the correlation function, the degree of agreement which is demanded between generated and reference correlation functions will be determined by a tradeoff of verification accuracy and Type II errors against Type I errors. As the tolerance on agreement is tightened, Type II errors will become less likely and Type I errors more likely. The parameter estimation scheme chosen can provide some measure of compensation to this effect. Legitimate system errors will not be a source of Type I errors when Correlation (not including comparison, parameter estimation and mapping equipment) will result in Type I errors.

Correlation - Relative Advantages

- Allows continuous verification
- Capable of detecting numerous types of failures
- Sampling rate not critical
- Does not require timing information
- Requires only an admissible input
- May be applicable to set output
- Can be made to identify failure types
- Adaptable to unsymmetrical redundancy
- Requires one powered element at a time
- Independent of signal class
- May be used with symbiotic pseudorandom input
- May be made to be extremely comprehensive
- Capable of identifying element status

Correlation - Relative Disadvantages

- Relatively complex implementation
- Use of sampling mandatory
- Design of accompanying parameter estimation and mapping equipment specialized to each kind of IBV
- Applicable only to linear systems
- Not able to detect noise added by IBV

A12.0 ACKNOWLEDGMENT TECHNIQUES

Acknowledgment has been accepted as a method for redundancy verification with the stipulation that backup equipment, as opposed to that primarily relied upon for the accomplishment of a function, is so reliable that the identification of status of the primary equipment constitutes redundancy verification (see Figure 2.2).

The name in itself implies action. The concept is that equipment receives a command and, upon completing its assigned task, acknowledges that its duties have been dispatched. For maximum verification confidence, the functions of compliance and acknowledgment should be as closely associated as possible.

Consider a commandable switch which routes its output to either of points A or B (SPDT). Acknowledgment could be accomplished by noting the appearance of signal at A or B and transmitting notification of this fact as a return, or by using a separate contact to indicate switch position, perhaps being open when the switch is in position A and connecting to a 6V reference when the switch is in position B. The second choice would probably be more reliable because the sensing of the tenant signal would not be required.

Lack of accomplishment or lack of compliance would be the only failure types detectable by the technique. In most acknowledgment situations, Type I and Type II errors should occur only as the result of failure in verification equipment.

Under the ground rule accepted above, acknowledgment would be applicable typically to unsymmetrical redundancy.

Acknowledgment - Relative Advantages

- Generally simple and reliable

Acknowledgment - Relative Disadvantages

- Very limited applicability
- Typically applicable only to unsymmetrical redundancy
- Requires distinguishable outputs

A13.0 USER COMPLAINT TECHNIQUES

User Complaint Techniques, like acknowledgment, have been accepted for the sake of completeness because only under the groundrule that backup systems are so reliable that they do not require checking will these truly represent a class of techniques for automated redundancy verification.

The need for a priori knowledge is implied in that the user must have stored information on performance against which to compare actual performance. This, then, is like a human-implemented monitor method. The failure types detectable will obviously be those which manifest themselves as output which the user can identify as erroneous.

Potential for errors, both Type I and Type II, is great because the performance criteria stored in the mind will often be qualitative and the mind is notoriously poor for accurately recalling qualitative matter. Also, the signals to which these techniques apply will be limited to those observable by a human.

Of course, the advantages of human capabilities including the ability of handling unforeseen occurrences will be realized. It is interesting to note that, ultimately, the user will always detect a failure; although the time lag could be significant in some cases. If a system exists wherein the user would not detect the failure, one must seveously question the utility of such a system. There will be some instances where user complaint, although not an automated technique, will be a sound engineering solution.

User Complaint - Relative Advantages

- No additional equipment design
- No verification equipment cost
- Economical

User Complaint - Relative Disadvantages

- Application to limited class of signals
- Typically applicable only to unsymmetrical redundancy
- Requires a priori knowledge in the form of user experience
- Requires distinguishable outputs
- High potential for errors
- Potentially long time delay to failure identification

A14.0 COMBINED SIGNAL FORM ANALYSIS/COMPARE TWO TECHNIQUES

A technique which observes a signal property and compares the derived value to one similarly obtained will enjoy advantages and suffer limitations which are a combination of those attributable to the two constituent techniques.

The fact that signal properties will be observed will probably mean a decrease in the number of failure modes detectable (from what is the case for Compare Two). It will usually mean a decrease in sensitivity to system noise and, in the design of the equipment observing the signal (such as a low pass filter to observe the mean) less attention to the signal to be observed would be required. As an example, if integration were performed, the time over which the integration was performed would not be very critical; the important thing would be whether the same value resulted when the two signals under scrutiny were each subjected to the same period of integration.

The main features contributed by Compare Two would be the inability to identify the status of individual elements and the possible allowance of transition from conditional status to status through the knowledge of admissible input.

APPENDIX B

TECHNICAL DESCRIPTION

HCDL-ERS

(Hypothetical Communications Down-Link-Earth Receiving Subsystem)

Site A

PREFACE

As the name implies, the HCDL-ERS is a hypothetical system. When faced with the problem of developing a representative example to demonstrate the methodology of the study, careful consideration must be given to an example which will draw on all aspects of the methodology and yet not require an inordinate amount of solution time or detail boarding on being inconsequential. Examples from actual systems in use were found to violate at least one of these prospects and it was determined that a hypothetical system was the only solution. The hypothetical system could not simply be a textbook example which ignored real-word constraints; nor could it involve part-level redundancy. The HCDL-ERS was developed under this philosophy. The system is considered topical and its design is not trivial. In some cases, license was taken with what might be considered a "best" approach to bring out a point in the methodology. The design represents an approach and is not intended to be a recommended approach to Lunar-Earth Communication.

B1.0 INTRODUCTION

The purpose of the HCDL-ERS is to receive information from a fixed moon base via an S-band link, convert this information to baseband and feed the baseband signals to the proper distribution busses. The S-band carriers contain commercial-grade T.V., a 1 Mbs TLM channel, a voice channel (consisting of five frequency multiplexed circuits) and an emergency digital channel. The antenna, antenna pointing control and microwave components prior to the cooled paramp are not considered part of the ERS. Due to the criticality of the mission, redundancy will undoubtedly be required for the ERS.

B2.0 MISSION AND OPERATIONS PROFILES

The mission profile of a single station of the HCDL-ERS coincides with the diurnal cycle of the moon. Since a 15-foot hard-mount antenna on the moon with a 2-degree beamwidth will just illuminate the earth, no relay satellites will be used. The use of relay satellites would require the moonbased antenna to either radiate a 12-degree beam (a loss of about 15 dB) or to be provided with a steerable mount. Neither alternative is attractive. Complete coverage of communications will be achieved by three earth stations located approximately 120 degrees apart in longitude and between 40 degrees North and 40 degrees South latitudes. A HCDL-ERS will not be required to track below 15 degrees elevation. Considering the latitudinal variations in the lunar orbit, we can state that the average mission for Site A will be seven hours in duration. Due to lunar phasing, the time between missions will be 17.8 hours. Due to the criticality of the mission, a complete checkout of the ERS will be required 30 minutes prior to the start of each mission. To achieve the desired reliability, continuous redundancy verification at a high degree of confidence is considered essential during the mission so that failed redundant equipments may be repaired immediately upon failure. These considerations are shown in Figure B2.0 for Site A. (The average mission duration is the only difference between the three sites.)

B2.1 Definition of Failure

The ERS will be considered to have failed if any of the specified outputs are beyond specified limits for longer than the following time durations:

a. 15 minutes with knowledge of suspect (or lost) information, and/or

b. 100 msec without knowledge of suspect information.

The goal for the emergency channel shall be five minutes with knowledge of suspect information.

B2.2 Traffic Density

This section describes the traffic density of the four channels in terms of percent utilization. All times are in Zulu. The profiles are given in Figure B2.2. The PCM channel will be transmitted on a separate carrier from the remaining three channels (a total of two carriers - see Section B4.2). From the detailed operations requirements below, both carriers must remain present at all times.

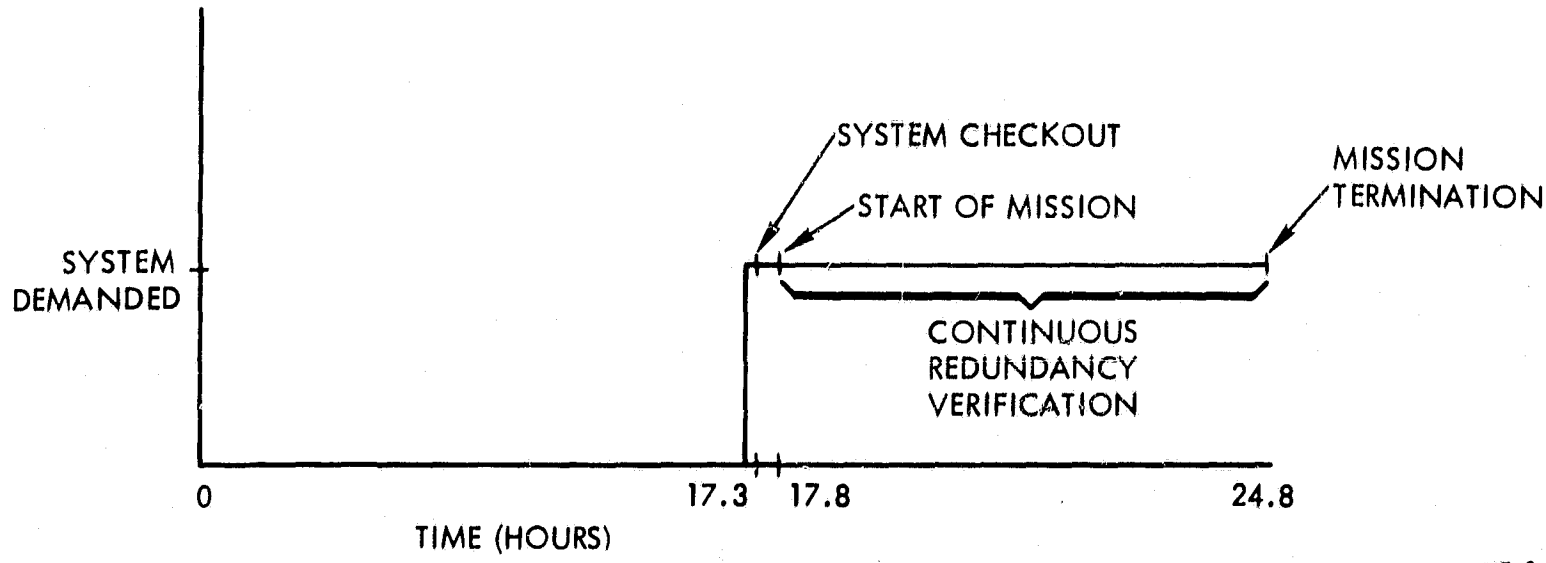


Figure B2.0. ERS Operations Profile - Site A

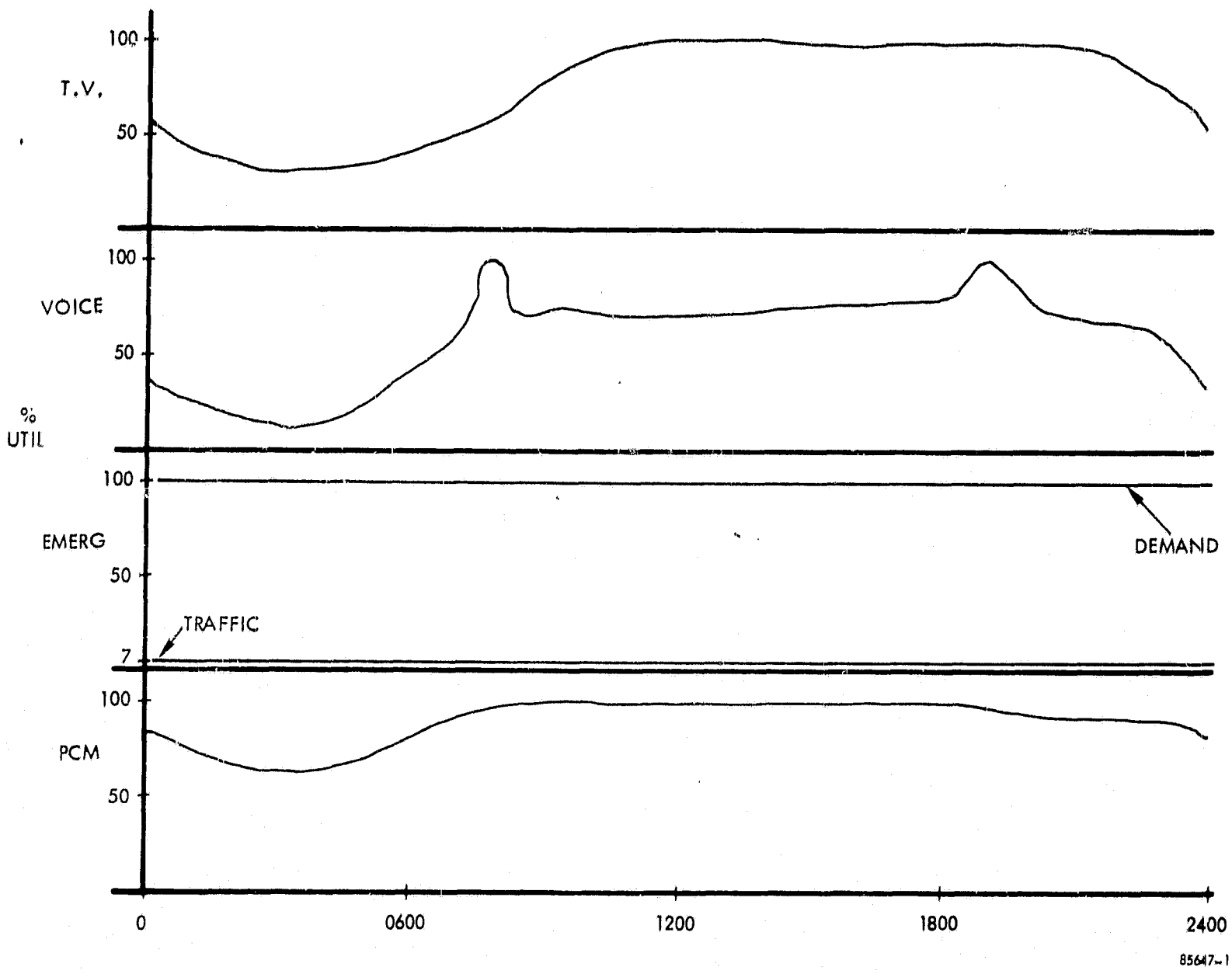


Figure B2.2. Channel Utilization Profiles

B2.2.1 T.V. (Video)

When not in use, it is planned to disable the T.V. drive to the modulator. The audio portion of T.V. transmissions will be through the Voice Channel.

B2.2.2 Voice

The voice subcarrier will be present at all times. One voice circuit will be dedicated to T.V. use.

B2.2.3 Emergency Channel

The emergency channel subcarrier will be present at all times. The channel shall remain open for use at all times. The purpose of the emergency channel is to relay priority messages, provide a reliable link during periods of solar flares and, as the name implies, transmit emergency information.

B2.2.4 PCM

The PCM carrier will remain present at all times. The number of active channels in the bit stream will; however, vary on a diurnal basis as well as with the number of experiments being performed. The utilization profile for this channel reflects the expected number of used channels.

B3.0 IMPLICATIONS OF REDUNDANCY WITH REPAIR

The desire to repair redundant equipments immediately upon failure was expressed in Section 2.0. This policy is especially applicable to equipments carrying the emergency channel. From the definition of failure, it is highly desirable to employ automatic sense and switch policies where the outputs/inputs of redundant equipments cannot be connected to a common conductor. The implication of this policy is that the status of each equipment must be identified. Whether this policy is adhered to or not, a failed equipment must have the capability of being isolated during repair. A second best alternative is to indicate that a fault has occurred and resort to manual identification of the fault -- so long as time constraint (a) under the failure definition is not exceeded.

B4.0 ERS DESIGN DESCRIPTION

This section describes the general physical layout of the ERS as well as the functional flow and signal characteristics.

B4.1 Location of Equipment

The parametric amplifiers and cryogenics will be located above the azimuth axis of the antenna. Maintenance of these items during a mission is disallowed. Failure of the cryogenics is considered an ERS failure.

The line driver amplifier is located in the antenna pedestal. The remainder of the equipment is housed in a facility 100 feet from the antenna. Maintenance during a mission is permitted on these equipments.

B4.2 Downlink Frequency Spectra and Modulation

The Downlink spectra and receiver bandpass are shown in Figure B4.2. A modulation and bandwidth summary is shown in Table B4.2.

The T.V. Video, Voice Channel and Emergency Channel are combined to modulate a 50-watt FM transmitter, with a carrier frequency of 2275 MHz. The TLM channel Bi-phase modulates a 100-miliwatt transmitter with a carrier frequency of 2287 MHz. These two carriers are combined and radiated from a 15-foot dish.

B4.3 Link Budget and Receiver Noise Temperature

The link budgets for the FM and Bi-phase carrier are shown in Figure B4.3 under the case of an 85-foot antenna for the Earth Station*. A receiver noise temperature of 100 degree K is used with the following characteristics resulting.

	S/N (dB)	Noise Power dBm	Signal Power dBm
FM	+26.0	-106.0	-80.0
Bi-phase	+11.6	-118.6	-107.0

B4.4 Telemetry Format

The PCM telemetry is NRZ. The format is shown in Figure B4.4.

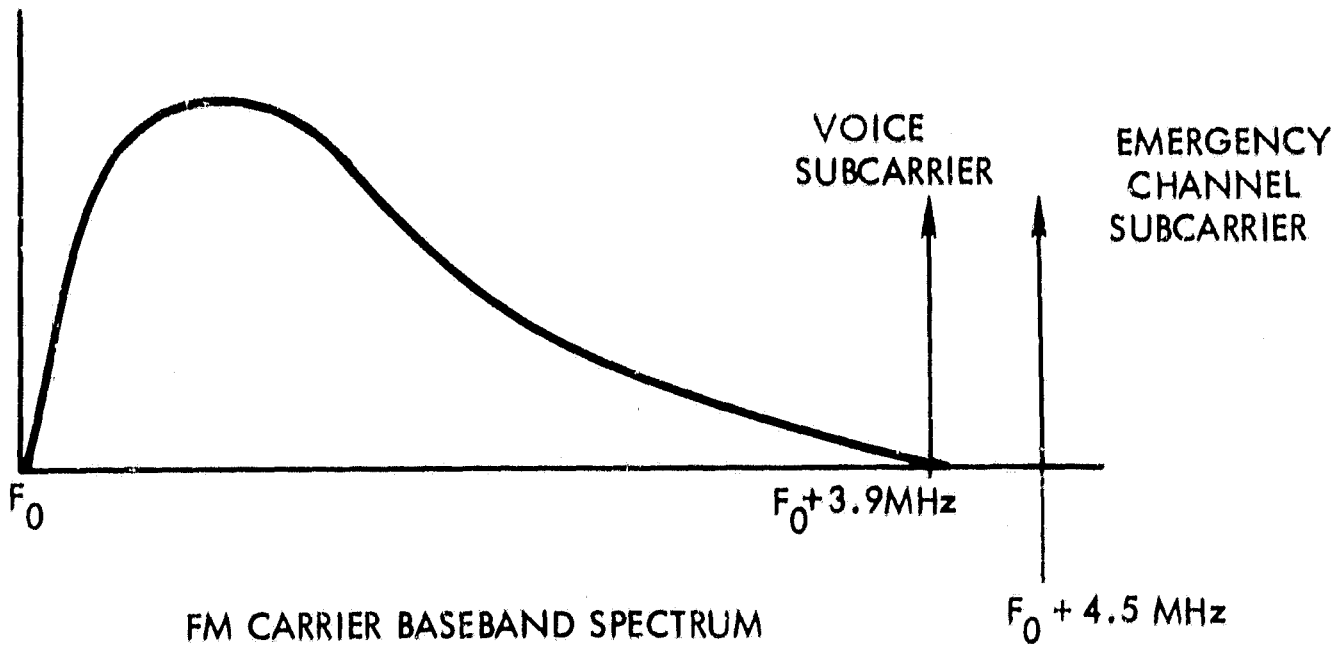
B4.5 Emergency Channel Format

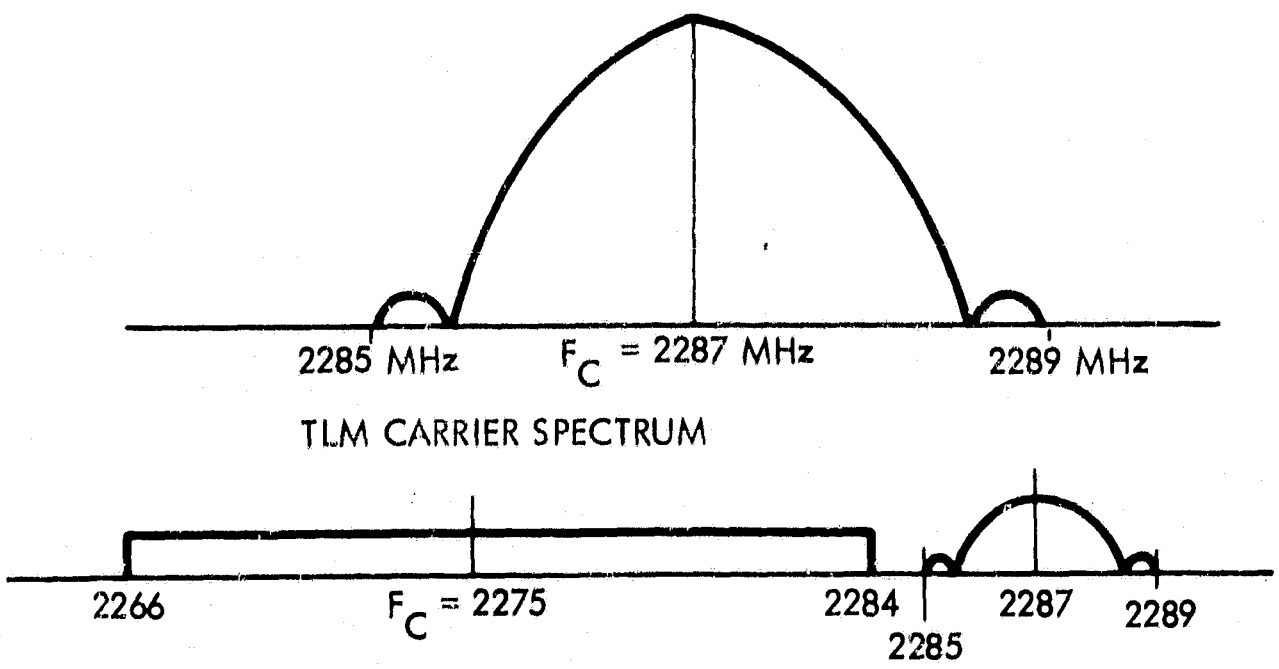
The emergency channel uses an RZ26 bit digital (two level) word for each character. The word contains 18 data bits and 8 redundancy bits. There are 25 special characters reserved for instructing the output device. During the transmission of a message, one of these special characters, the line marker, will appear every 40 characters.

B4.6 ERS Functional Block Diagram

The ERS functional block diagram is shown in Figure B4.6. The general flow of the subsystem is as follows. The received signal enters the low noise paramp and is then fed immediately to the line driver before routing to the equipment facility 100 feet away. Immediately

*The 30-foot antenna case gives a comparison for TLM using a one-watt transmitter.





85647–2

Figure B4.2. Downlink Spectra and Bandpass

Table B4.2. Modulation Summary

Ch. #	Desc.	Baseband	Subcarrier
1	T.V. Video	Freq. band - 0-4 MHz BW = 4 MHz Combined directly with subcarriers in FM Transmitter	N/A
2	TLM	Modulation - PCM, NRZ 1 Mbs	N/A This channel is bi-phase modulated on a 2287 MHz carrier
3	Voice	5 ckts + 1 pilot, AM -SSB, Freq MUX carriers BW = 20 kHz Freq. band - 30 kHz-50kHz Pilot freq = 38 kHz	f_o = 3.90 MHz Freq. band - 3.75M-4.05MHz BW = 300 kHz FM Modulation Combined with video in FM Transmitter
4	Emerg.	Modulation - PCM, RZ 20 Kbs	f_o = 4.50 MHz Freq. band - 4.44-4.56 MHz BW = 60 kHz Bi-Phase Modulation combined with video in FM transmitter

	Telemetry 30' Ant.	Telemetry 85' Ant.	FM 85' Ant.	
Transmitter Power	+30.0	+20.0	+47.0	dBm
Coupling Loss	-3.0	-3.0	-3.0	dB
Antenna Gain (15')	+38.0	+38.0	+38.0	dB
ERP	+65.0	+55.0	+82.0	dBm
Pointing Loss	-1.0	-1.0	-1.0	dB
Space Loss	-212.0	-212.0	-212.0	dB
Atmospheric Atten.	-2.0	-2.0	-2.0	dB
Antenna Gain	+44.0	+53.0	+53.0	dB
Received Power	-106.0	-107.0	-80.0	dBm
System kT_n (100^oK)	-178.6	-178.6	-178.6	dBm/Hz
Bandwidth	+60.0[2]	+60.0[2]	+72.6	dB -Hz
Noise Power	-118.6	-118.6	-106.0	dBm
S/N	+12.6	+11.6	+26.0	dB
S/N required for $P_e = 10^{-5}$	+9.6	+9.6		dB
S/N required for T.V. (39 dB @ video, $\beta = 1$)			+34.0	dB
Margin	+3.0	+2.0	-8.0[1]	dB

[1]This will result in an acceptable but somewhat snowy picture.
[2]Bit rate bandpass.

Figure B4.3. Link Budget

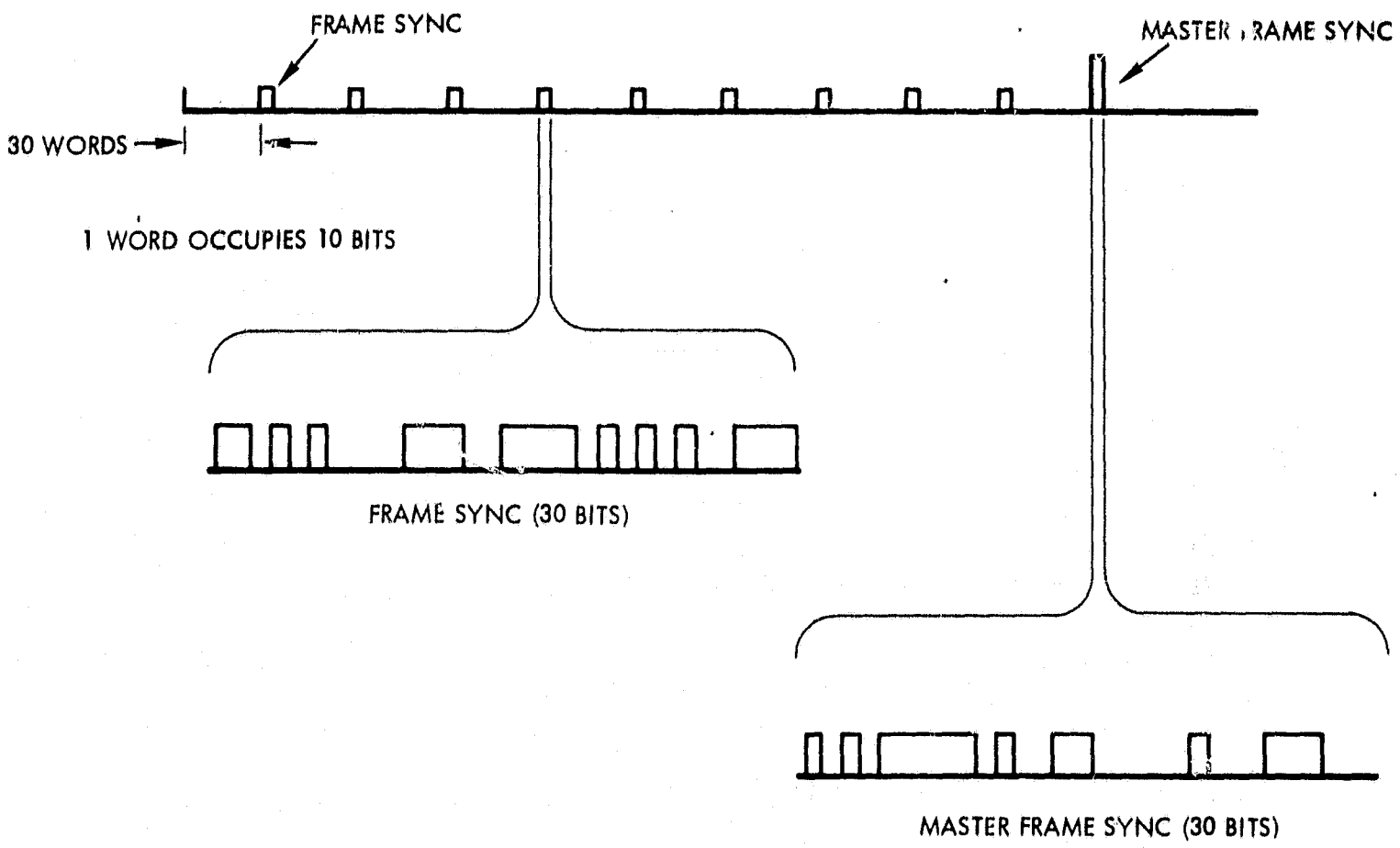


Figure B4.4. TLM Format

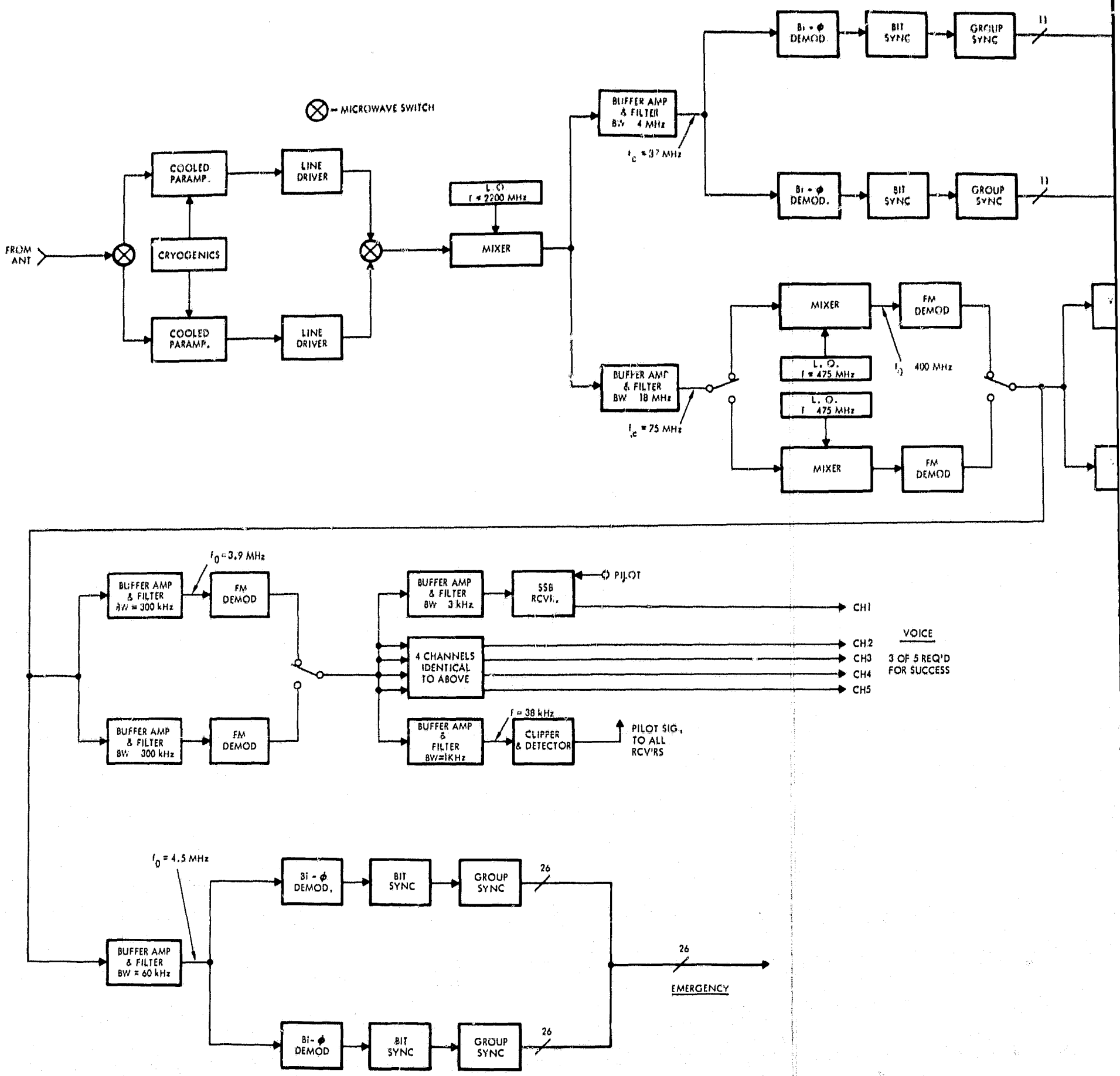
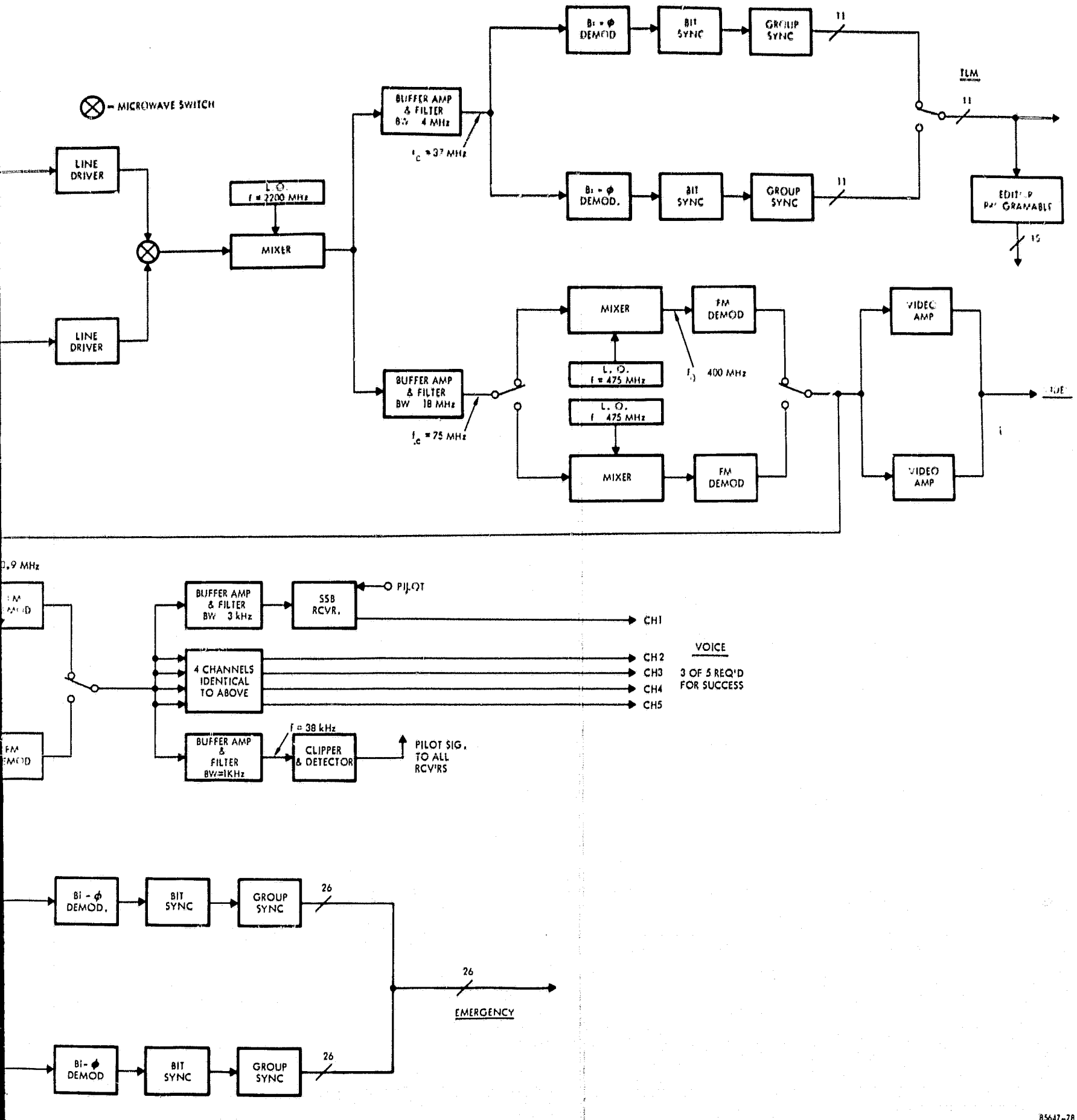


Figure B4.6. ERS Function

FOLDOUT FRAME 7

FOLDOUT FRAME



85647-78

Figure B4.6. ERS Functional Block Diagram

FOLDOUT FRAME 1
FOLDOUT FRAME 2

upon entry to the equipment facility, the signal is down translated such that the center of the total received band is approximately 80 MHz. Selection of this frequency was based on implementation requirements of the two carrier filters and the telemetry bi-phase demodulator. The carrier filters separate the carriers for individual processing by the subsystem*. The telemetry bi-phase signal is demodulated immediately, reshaped through the bit synchronizer and finally arranged into words at the group synchronizer. This output is then routed to the distribution busses and the data editor which strips specific channels for immediate processing at the receiver site.

After the separation operation by the carrier filters, the FM signal is translated upward to f_c = 400 MHz. This translation is performed due to implementation requirements of the FM demodulator. The output of the FM demodulator is the FM signal baseband. Since the T.V. video is modulated directly onto the carrier (i.e., no subcarrier is involved), the video is picked off at this point and fed to a video amplifier for distribution. The video amplifier will perform sufficient filtering of the baseband.

The remainder of the baseband is routed to the subcarrier buffer amplifiers and filters where the voice and emergency subcarriers are stripped off. The emergency channel subcarrier is then fed to a bi-phase demodulator and subsequently operated on similar to the telemetry signal.

The voice channel subcarrier is passed through an FM demodulator which reclaims the original frequency multiplexed audio and the pilot signal. This signal is then fed to the five buffer amplifiers and filters plus a pilot extractor circuit. Having separated the five multiplexed intercarriers, each is fed to a single sideband receiver for detection and routing of the extracted audio signals. The pilot signal is used in the single sideband detection.

With this thumbnail sketch of the ERS functional implementation as introduction, the following sections will address some of the specific blocks.

B4.6.1 TLM Bit and Group Synchronizers

The Bit Synchronizer clocks, formats and reconstructs the serial bit stream received from the Bi-phase Demodulators. The output to the Group Synchronizer is a "clean", serial RZ bit stream at 1 Mbs with +5.0±0.5V as logic true and 0.0 to +0.5V as logic false.

The Group Synchronizer reconstructs the TLM words and adds an even parity bit. The output of the Group Synchronizer is a ten bit word plus a parity bit at 100 kws with the same format as the output of the Bit Synchronizer. The output is routed to the Editor and the distribution bus.

*The TLM Bi-phase demodulator would normally supply sufficient filtering due to the nature of the circuitry, however a filter has been added to reduce noise during lock-up of the demodulator.

B4.6.2 TLM Editor

The TLM Editor selects seventeen operation-peculiar channels from the TLM information stream for immediate processing at the ERS. The Editor is programmable such that it can adapt to changes in TLM Channels assignment and can select from any seventeen of 42 possible channels. Reprogramming is accomplished by paper tape reload. The Editor output to the Processor (not part of the ERS) is a fifteen bit word and operates on a contention basis with the Processor. The output words consist of ten data bits, one parity bit and a four bit tag. The format is the same as that of the output of the Bid Synchronizer. Since the Editor opearates on a contention basis with the Processor, the output rate can be as high as 100 kws.

B4.6.3 Emergency Channel Bit and Group Synchronizers

The Bit and Group Synchronizers in the Emergency Channel are similar in function to those of the TLM Channel except that the Group Synchronizer does not add a parity bit. The output of the Group Synchronizer is routed to the distribution bus at a rate of 770 ws.

B4.6.4 Voice Channel

The Filter, Buffer Amplifier and FM Demodulator are straight forward functions. The frequency spectrum at the output of the FM Demodulator is shown in Figure 4.6.4. The five frequency multiplexed voice circuits and the pilot tone are separated by filtering and the audio is recovered by five single-sideband receivers. The pilot tone is fed to each of the receivers for demodulation. The output of the five receivers is fed to a switchboard (not part of the ERS) where routing and reconfiguration are accomplished. Functionally, each circuit is identical and three of the five must be operational for the Voice Channel to be considered operational.

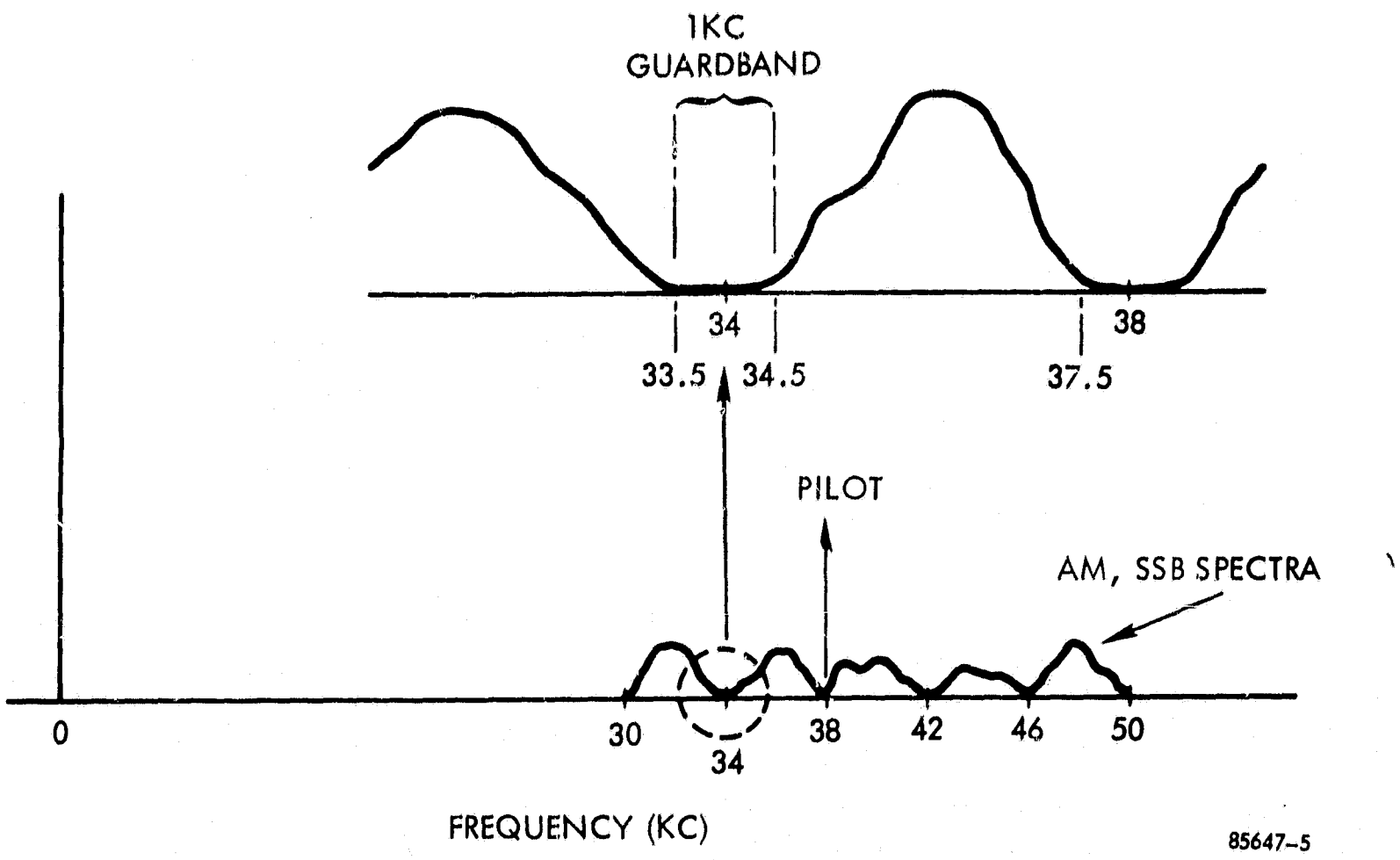


Figure B4.6.4. Frequency Spectrum at Output of Voice Channel Demodulator.

APPENDIX C

CASE STUDY DESIGN DESCRIPTION AND SOLUTION

C1.0 INTRODUCTION

This section will outline the philosophy followed in the case study. The time constraints specified in the technical description of the ERS and the nature of the signals which the system processes are the main factors in the philosophy of approach.

The 100 msec time limit for detecting a failure in the ERS was given primary consideration in designing the verification system. This policy resulted in some rather extreme measures in the design process which otherwise could have been avoided. Most of the signals present in the system under mission conditions contain stochastic, nonstationary elements. This factor eliminates some of the coincidence development techniques.

Finally, we should emphasize that our task was the design of redundancy verification equipment for the ERS. No attempt was made to change the design of the principal system to improve its reliability, since the reliability was considered in the original design. Any changes we made in the principal system were made solely for the purposes of redundancy verification.

C2.0 DESIGN INPUTS

The following paragraphs are a reiteration of pertinent facts about the ERS, as they pertain to the verification design. This section categorizes the technical description into the design input channels called out in the design process.

C2.1 Set I Group Identification

Figure C2.1-1 shows the ERS block diagram partitioned into sets and groups with numbers to identify each group and simple sets (SS).

The choice of this particular partitioning by no means excludes other divisions of the system. For instance, the equipment contained in Group 1 and Group 2 could be combined into one group. We chose to divide the group into that portion which could be maintained (the line drivers) and that portion which is inaccessible to maintenance.

The five voice channels form a difficult problem in identification. Each channel is independent of the others so it would seem reasonable to classify them as five simple sets. On the other hand, the commonality of purpose and the three-of-five success criterion suggests that they all be identified as a single set or a group. To resolve this dilemma, we must carefully examine the function of the voice channels. Their function is to conduct at least three conversations from the moon to earth. The failure of any one channel (or two) does not result in a system failure. Hence, in a functional sense, the five channel's output is a single three-line conversation, not five single-line conversations. We, therefore, identify the five channels as one simple set.

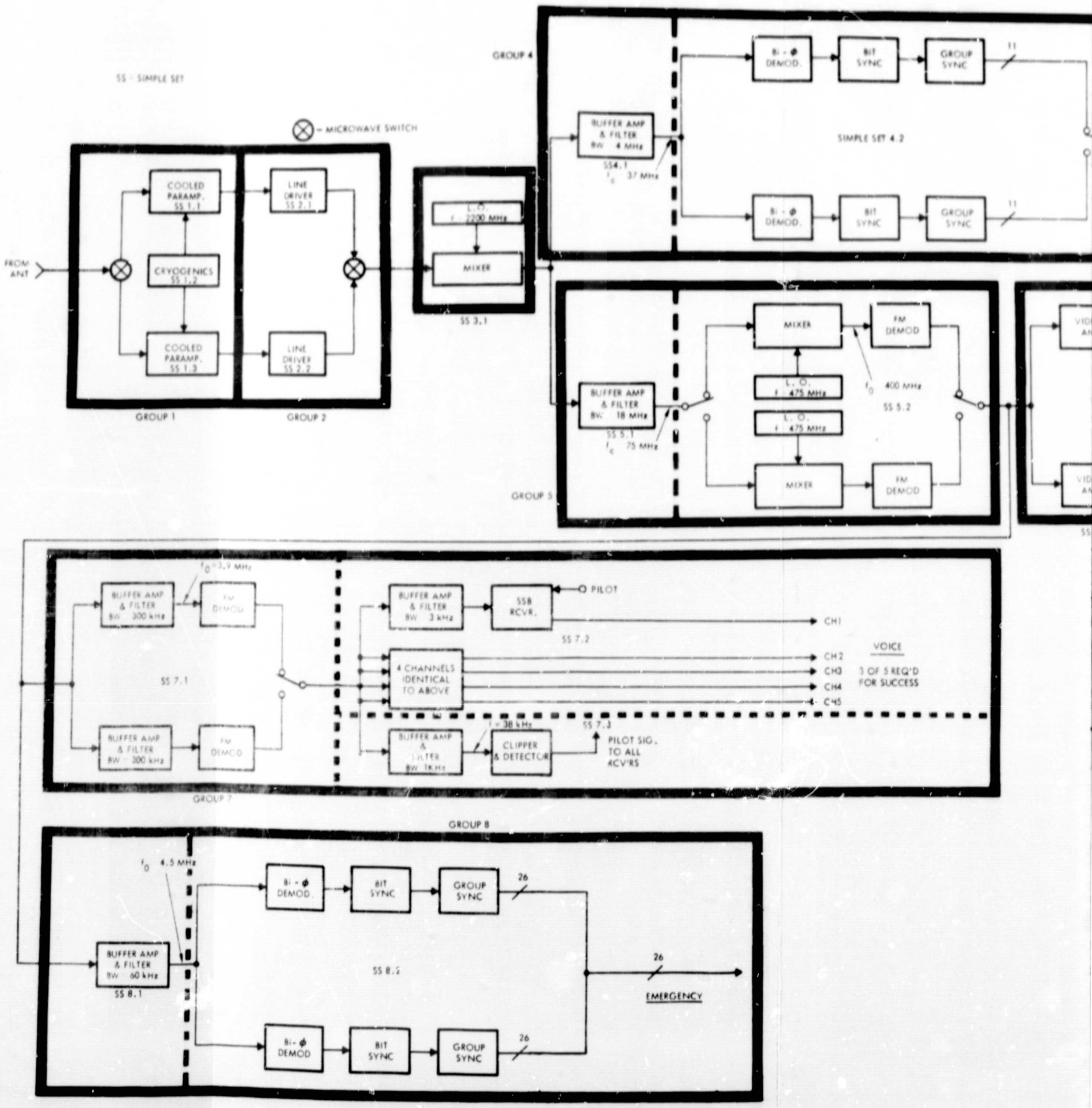
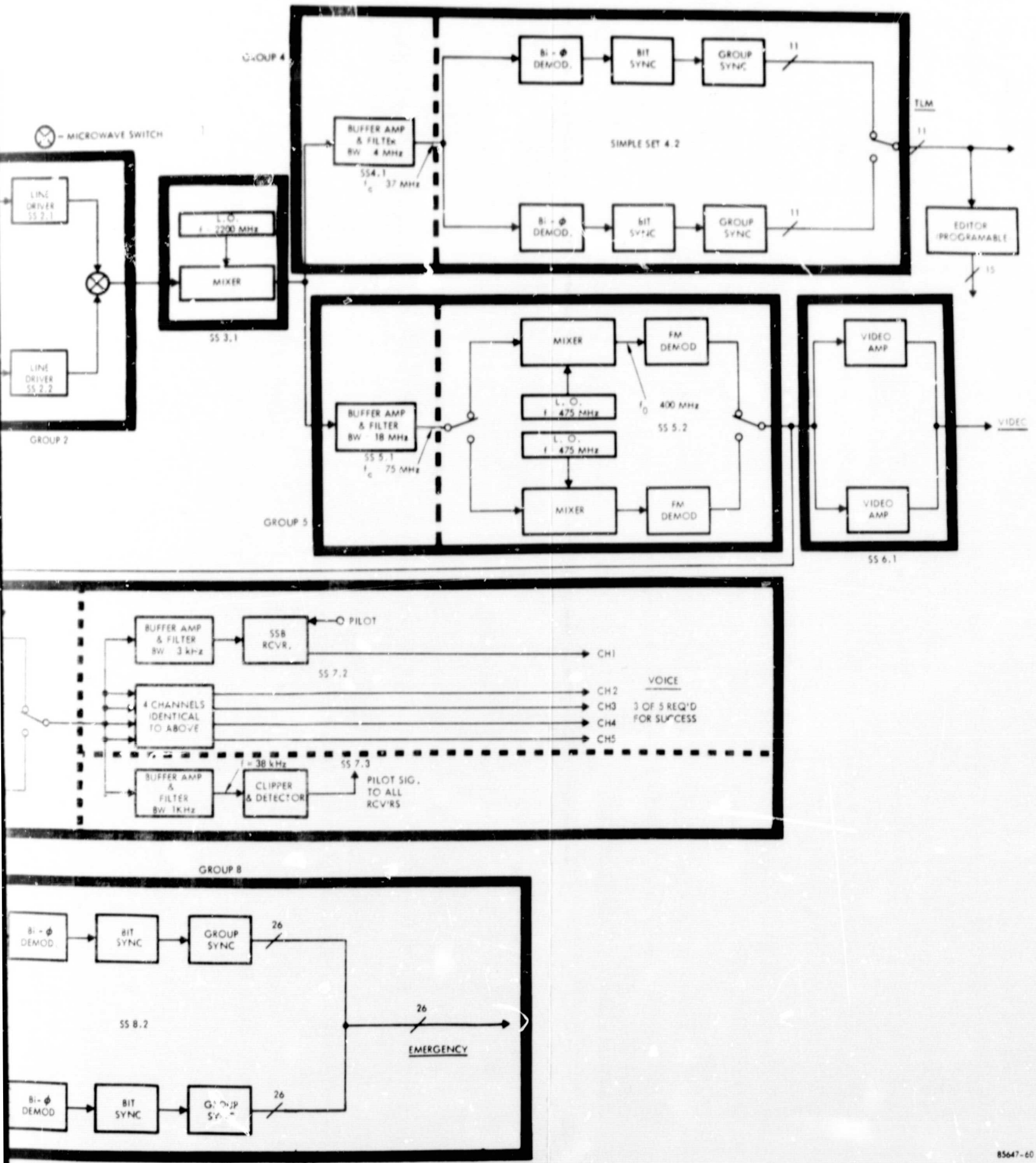


Figure C2.1-1. ERS Functiona
with Partitioning Sh

FOLDOUT FRAME 1

FOLDOUT FRAME



B5647-60

Figure C2.1-1. ERS Functional Block Diagram with Partitioning Shown

FOLDOUT FRAME 1

FOLDOUT FRAME

The remaining set and group classifications are straight forward. The programmable editor was intentionally excluded from the set/group identification process, because its operation is subject to programmed changes. Each configuration must be verified individually.

C2.2 Group Policy

The time constraints for failure detection which are given in the ERS technical description necessitate using the tenant signals for verification wherever possible. Since failures in the verification equipment must be shielded from the principal system, we use isolation amplifiers at all tap points as shown in Figure C2.2-1.

Status reports from each group are routed to a central processor which will evaluate system status, detect a failed element, and automatically switch in the redundant equipment, if available.

C2.3 Time Profiles

Due to the 100 msec fault detection criterion, verification must be accomplished continuously throughout the operating cycle of the ERS.

The required system checkout 30 minutes prior to actual mission provides a high confidence test of all the system functions. This test also permits assessment of internal system parameters which may be useful in setting threshold levels, etc.

The channel utilization profiles in the ERS technical description indicate varied demands on the various functions. (PCM, video, etc.) All functions have intervals of 100% utilization during which idle signals could not be used for verification. In fact, only the voice channels have significant periods of less than 100% utilization for a worst case 8-hour interval. There will thus be a trade-off here between using a two-level technique or a single worst case technique for verifying the voice channels. Another trade-off will be encountered with verifying the emergency channels. A very high confidence level verification can be achieved during the premission test, but the expected channel usage is inadequate for verification purposes. Hence, an idle signal may be needed during periods of nonusage.

C2.4 Signal Characteristics

In order to determine the type of verification technique (and thus the equipment) to use, we must know the class of signal whose properties we wish to measure. Knowing this, and knowing the redundancy class of the simple set/group being verified, we can use the matrix in Figure 6.2.2-5 (p. 59) of the Phase II Report to determine the techniques available.

Figure C2.4-1 is a table of the simple sets in the ERS, with the class of signal on their inputs and outputs.

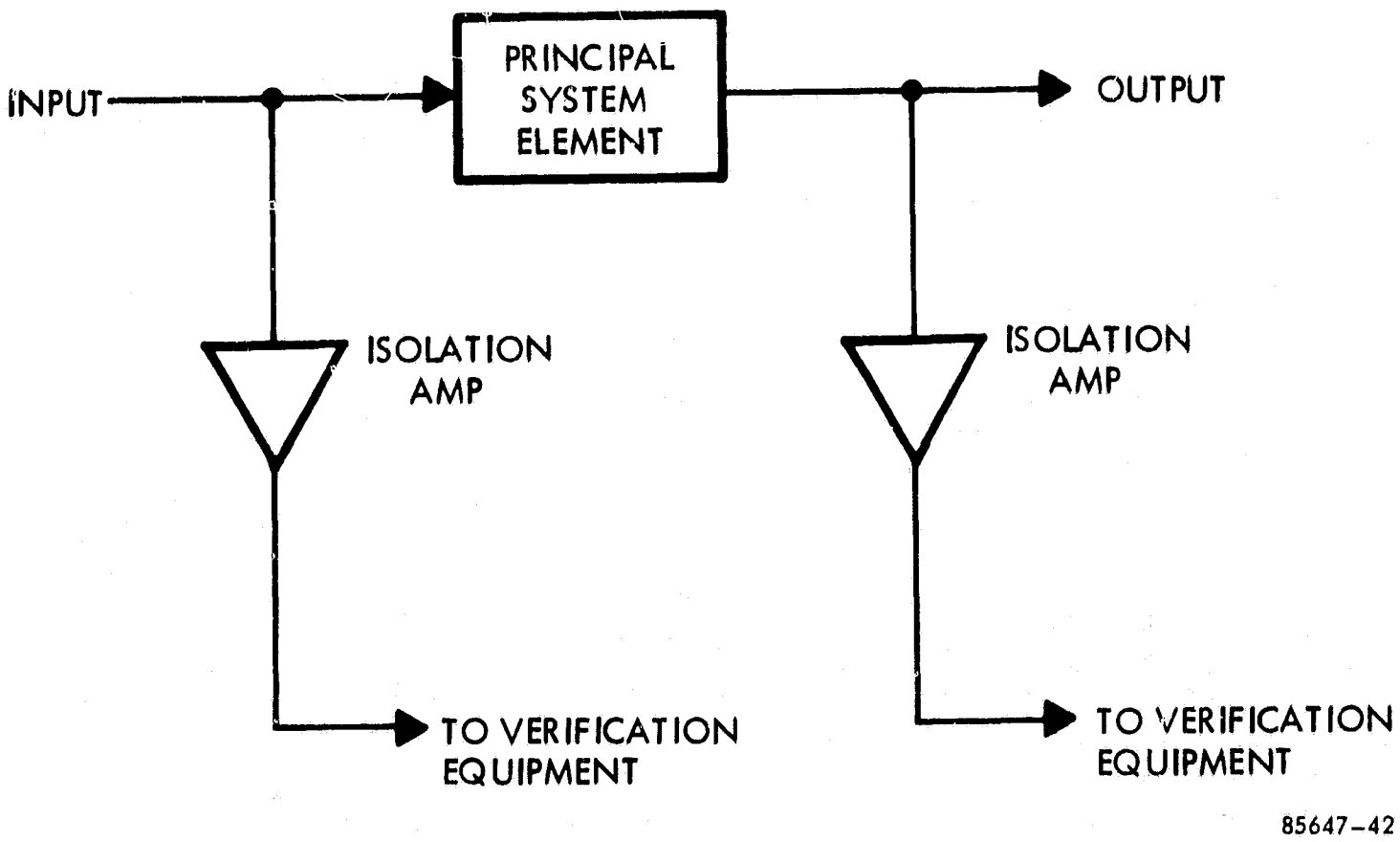


Figure C2.2-1. Typical Isolation Schemes for Tap Points

Simple Set	Input Signal Class	Output Signal Class
1.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
1.2	-	Deterministic
1.3	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
2.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
2.2	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
3.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
4.1	Stochastic, Non-Stationary with/random noise	Stochastic, Stationary
4.2	Stochastic, Stationary	Stochastic, Non-Stationary with/random noise
5.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
5.2	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
6.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
7.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
7.2	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
7.3	Stochastic, Non-Stationary with/random noise	Deterministic
8.1	Stochastic, Non-Stationary with/random noise	Stochastic, Non-Stationary with/random noise
8.2	Stochastic, Non-Stationary with/random noise	Stochastic, Stationary

Figure C2.4-1

C2.5 Properties Indicative of Operation and Their Status Relationship

Most of the signals available for verification are stochastic, non-stationary. This fact, combined with the time allowed for verification, restricts us to a small group of verification techniques. The time constraint eliminates some of the more thorough techniques which could otherwise be used (especially those techniques requiring digital computation). Hence, the properties indicative of operation must be those which lend themselves to verification by the narrow set of techniques available.

Figure C2.5-1 summarizes the properties for each simple set by which we will judge the operation.

C2.6 Design Confidence and Number of Confidence Levels Desired

Due to the nature of the signals in the ERS, the verification techniques of spectral analysis, signal form analysis, and inverse transform will be used extensively. Contributory tolerances of verification equipment must be considered when employing these techniques, since they are analog in nature, Generally, the verification equipment tolerances are inconsequential, except for the case of threshold detectors. For these devices, the probability of decision errors increases as the decision threshold level and the signal level approach a unity ratio. Hence, it is beneficial to noise immunity to maximize this ratio, while maintaining sufficient confidence in the status resolution.

In at least one portion of the ERS, the telemetry channels, there will be two different confidence levels established. During the premission checkout prior to the actual mission, known telemetry data can be used, whereas during the actual mission, most of the received data is unknown. Hence, we can be more confident of the telemetry receiver when every bit is checked. There may be other portions of the ERS which can be more fully verified in the premission checkout than in the actual mission. These will be discussed in the tradeoffs.

C2.7 Redundancy Class

Having determined the types of signals being processed, the properties indicative of operation and the time constraints, we can classify the redundancy features for simple sets with regard to verification. The most prominent constraint is the 100 msec failure detection limit, which necessitates continuous verification. Referring to the Matrix in Figure 6.2.2-6 (p.61) of Phase II, we are left with classes A, B, E, and G. Since we are employing the symptomatic approach to verification, we must be able to distinguish the output of an element (see Section 5.2 of Phase II). This eliminates Class G. Finally, the ERS is not a multiple-mode system. All switching done in the system is solely for selection between redundant channels. Thus the output of a set is inherently dependent upon the output of each element in the set. This property eliminates Class B. Hence, all redundancy in the ERS falls into Classes A or E.

Simple Set	Properties
1.1, 1.3	Gain & BW of parametric amplifiers at carrier frequency
1.2	Temperature of Cyrogenics
2.1, 2.2	Gain & BW of parametric amplifiers at carrier frequency
3.1	Frequency of Local Oscillator carrier frequencies (87 MHz & 75 MHz) at mixer output
4.1	Gain & BW of buffer amplifier & filter
4.2	10^{-5} bit error rate
5.1	Gain & BW of buffer amplifier & filter
5.2	Frequency of Local Oscillators; carrier frequencies at mixer outputs; emergency channel carrier at FM demodulator output
6.1	Gain and BW of video amps
7.1	Gain and BW of buffer amps; frequency spectrum at FM demodulator output
7.2	Gain and BW of buffer amps and filters; frequency spectrum of receiver outputs
7.3	Pilot tone frequency at 38 KHz
8.1	Gain and BW of buffer amp and filter
8.2	10^{-5} bit error rate

Figure C2.5-1

C3.0 HIGHER LEVEL GROUP PROBLEM

Having determined the design inputs, we now formulate the overall system verification plan. The areas to be considered are: 1) the policy for treating off-line elements, 2) the isolation/independence plan, and 3) status resolution, reporting, and the relationship to a central processor.

C3.1 Policy for Treating Off-Line Elements

All off-line elements in the ERS are symmetrically redundant branches of their on-line counterparts. Since the tenant signal is used for verification in most cases, we are naturally inclined to perform the same type of verification on the off-line equipment as we perform on the on-line equipment. This policy has the desirable feature of providing the same confidence level in the off-line equipment as in the on-line equipment.

Input power in a ground system is not a constraint, so all the off-line elements may be verified continuously. This means that all off-line elements will be active and operating, with the outputs available through switching. This mode of operation also minimizes the time delay encountered when a redundant branch must be switched into the principal system. The time delay may be of considerable importance in the PCM telemetry channels. Group synchronization requires a master frame marker, which may mean the loss of up to 10 frames of data after switching is completed.

During the premission checkout, all systems may be considered off-line. Since the tenant signal will not be available, we instead use a simulative signal which duplicates the nature of the tenant signal. This signal, which will be a composite S-band signal with the subcarriers and baseband of the tenant signal, is injected at the front end of the system at the received power level, as called out in the ERS link budget (-106 dBm for a 30' dish, -107 dBm for an 85' dish). Naturally, we may use known information in modulating the various subcarriers which compose this signal, resulting in increased confidence in the principal system. It will be necessary to use the test signal generator during the actual mission for verifying the off-line paramp and line driver, since any splitting of the received signal would cause a 3 dB signal loss in the on-line branch.

C3.2 Isolation/Independence Plan

Most of the verification techniques used will necessarily involve sampling the tenant signal, so it is imperative that the sampling point be as free from verification system effects as possible. To accomplish this, all taps onto the tenant signal must pass through isolation amplifiers, with at least 60 dB isolation between input and output. Thus, a short circuit in the measurement circuits will have little or no effect on the principal system. Of course, a short circuit on the isolation amplifier input could have disastrous consequences, but these devices may be designed so as to virtually eliminate the probability of this event.

The breakdown of the ERS into simple sets, shown in Figure C2.1-1, virtually eliminates the problem of verifying the operation of nonindependent simple sets. The simple sets are in a series relationship, so that a failure in one branch will be isolated to that particular branch. As a further contribution to the independence of the simple sets, we recommend providing each set with its own power supply.

C3.3 Status Resolution, Reporting and the Relationship to a Central Processor

Each of the four different data functions (PCM, Video, Voice, and Emergency) are in a series configuration, with no looping or feedback. Effects of a failure in one element will be passed on to all "downstream" elements in that series. Thus before failure can be attributed to a particular element, the status of the prior element must be assessed. This is the function of the central processor. An indication of element failure will cause the processor to work backwards, checking the outputs of preceding elements, until a good output is found. Then the element next-in-line from the good one will be declared bad, and its status will be displayed on a system block diagram board. The processor will also be responsible for switching to redundant elements, whenever a failure occurs and redundancy is present.

C4.0 THE SET PROBLEM

Considerations in the set problem fall into three (3) categories in the redundancy verification design process:

1. Selection of the coincidence development technique to be used on each set.

2. Formulation of the status vector (parameter estimation).

3. Mapping the status vector into conditional status.

C4.1 Coincidence Development

In selecting a coincidence development technique, we must give primary consideration to the 100 msec fault-detection limit. As described earlier, all the simple sets in the system are in redundancy classes A or E. It seems logical, therefore, that the same coincidence development technique may be used on all of the elements of one type. For example, all of the buffer amplifiers in the ERS might be verified using a bandpass filter and threshold detector. This approach was used in considering each type of element.

The following pages will describe the coincidence development decisions and selection of the technique used for each type of element in the ERS.

1. Parametric Amplifiers - The paramps (and cryogenics) are located on the antenna, and are inaccessible to maintenance. Since any tampering with the inputs of the amplifiers would seriously degrade the quality of the received signal, we can only

observe the outputs of the amplifiers. Even here, the signal level is very low, so all verification equipment must be highly isolated. We decided to ascertain that the power spectrum of the paramp output contained sufficient energy at the two frequencies of interest (2275 and 2287 MHz) for the rest of the receiving system to operate. This is accomplished by an isolation amplifier, two narrow-band filters centered at 2275 and 2287 MHz, respectively, and two threshold detectors. The threshold detectors are monitored continuously.

2. Cryogenics - The cryogenics may easily be verified by continuous value checks of a thermal sensor.

3. Line Drivers - The line drivers may be verified in identical fashion to the paramps by continuously checking the power spectrum of the output at the two carrier frequencies.

4. Local Oscillators - The idealized power spectrum for a local oscillator is an impulse at the frequency of the oscillator. Hence, to verify an oscillator we must verify sufficient power at the desired frequency, and verify that spurious power (at other frequencies) is below an acceptable standard. A narrowband filter centered at the oscillator frequency plus a power level detector will suffice for the first consideration, and a notch filter and threshold detector will satisfy the second.

5. Mixers - Mixers are frequency translation devices whose output frequency is the sum or difference of the frequencies of the input signal and the local oscillator. Hence, they may be verified just like the paramps, by checking the power spectrum of the output with a narrowband filter and threshold detector.

6. High Frequency - Buffer amplifiers (and filters) - These devices are checked in the same manner as the paramps - with a narrowband filter and level detector. "High frequency" means those buffer amps and filters in the system with center frequencies above 1 MHz.

7. High Bit Rate - PCM Demodulators and Syncs - A special problem exists here as a result of the 100 msec fault detection requirement. In order to precisely determine the bit error rate, we must have knowledge of the bits transmitted from the moon. Since the 30-word PCM frame has 3 frame-marker words (with known bit patterns), we have knowledge of 10^{-5} bits/sec at the 1 megabit/sec transmission rate. However, the desired bit error rate is 1 in 10^{-5}, and excessive rates must be detected in 100 msec. This presents an irreconcilable problem for the system in its present state, since it takes a full second to observe 10^{5} known bits. A total failure could be detected within the time limit, but an intermittent failure might not register in 100 msec.

The solution to this problem involves a significant addition to the system - another bi-phase demodulator, bit sync, and group sync, in parallel with the original redundant pair. Now we can employ majority voting between the three channels to detect intermittent errors or failures in any one channel. Since we are now examining every bit, we can count the number of errors in 10^5 bits every 100 msec. The probability of encountering more than 5 errors/10^5 bits without an actual failure is 0.0001; the probability of encountering more than 10 errors/10^5 bits is negligible. Hence, if the error count exceeds 10 bits in any 100 msec interval, the on-line channel can be switched to another branch. The error count per 10^5 bits can be averaged continuously to provide a mean bit error rate.

In addition to the majority voting scheme, we also monitor the frame markers to detect any errors which occur in all three channels simultaneously, such as those caused by EMI. Thus, any type of error in the channels will be detected.

8. Video Amplifiers - The video amps operate up to 3.6 MHz, and at this frequency they can be tested by inverse transform techniques. The input to the amplifier is fed into one input on a differential amplifier, and the output is inverse - transformed (phase & amplitude corrected) and fed into the other input. The output of the differential amp can then be amplified and threshold detected. The threshold detector can be calibrated to any desired degree of fidelity between the compared signals.

9. Emergency PCM Channels - The bit rate of the emergency channels is 20 Kilobits/sec. Due to this reduced rate, the technique employed for the verification of the high-speed channels will not work here. In fact, it is impossible to provide continuous verification of the 1 in 10^5 bit error rate, since we only receive 2000 bits in the 100 msec fault-detection interval. Hence, even if we knew the validity of every bit, it would be 50 seconds, on the average, for one bit error to occur. Two alternatives exist - 1) We can raise the bit-rate of the channel to a sufficient level whereby the channel can be verified continuously every 100 msec; or 2) We can abandon the 100 msec failure detection limit. In the first case, the required channel bit rate would be 10^6 bits/sec (the same as the telemetry channels). This bit rate would make the emergency channel much more susceptible to noise and EMI. The second alternative requires us to place higher confidence in the reliability of the emergency channels. Since the channels can be completely verified in the premission checkout, and since the anticipated demand is only 7%, we are inclined to the second alternative.

10. Voice Channel FM Demodulators - The output spectrum of the demodulators contains the pilot tone at 38 kHz. We observe this output through a narrowband filter centered at 38 kHz and a level detector.

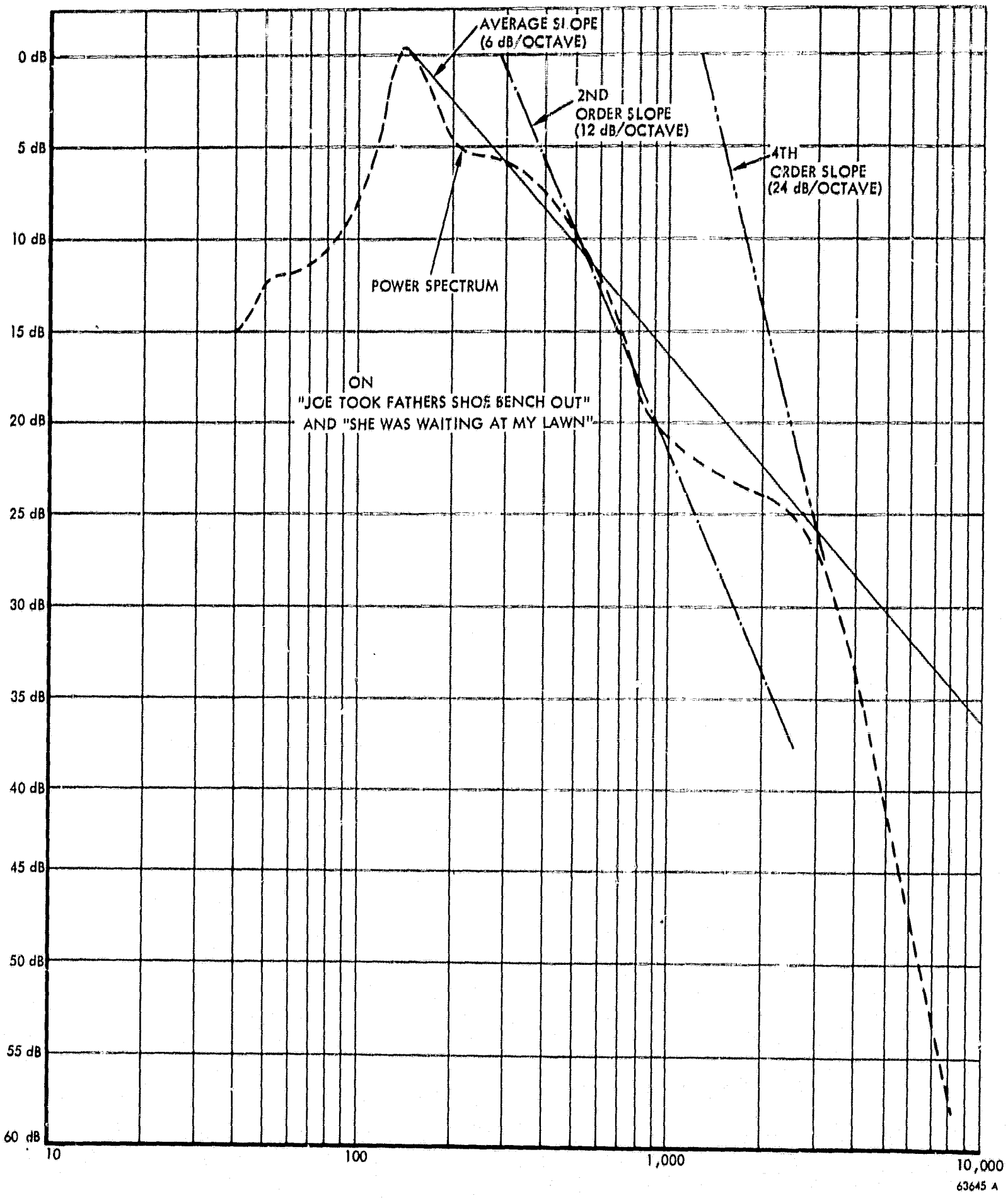


Figure C4.1-1. Typical Power Spectrum for Conversational English

11. Voice Channels - Since the voice channels will have stochastic non-stationary tenant signals, we must inject symbiotic signals to achieve verification. Figure C4.1-1 shows a typical voice spectrum for conversational English. Note that the 2400 Hz range is 25 dB down from the maximum. A symbiotic tone at this frequency will not interfere with the conversation. Hence, we inject 5 symbiotic tones at 32.5, 36.5, 40.5, 44.5, and 48.5 kHz into the input to the buffer amps, and monitor the outputs for these tones. Additionally, we monitor the receiver outputs at the 2.5 kHz frequency to establish continuity through the system.

12. High Frequency FM Demodulators - These demodulate the video, voice, and emergency channel carrier. Since the emergency carrier is always present at 4.5 MHz, the upper end of the band, we observe this carrier output through a narrowband filter centered at 4.5 MHz and a level detector.

Figure C4.1-2 shows the ERS with the verification equipment and system changes added.

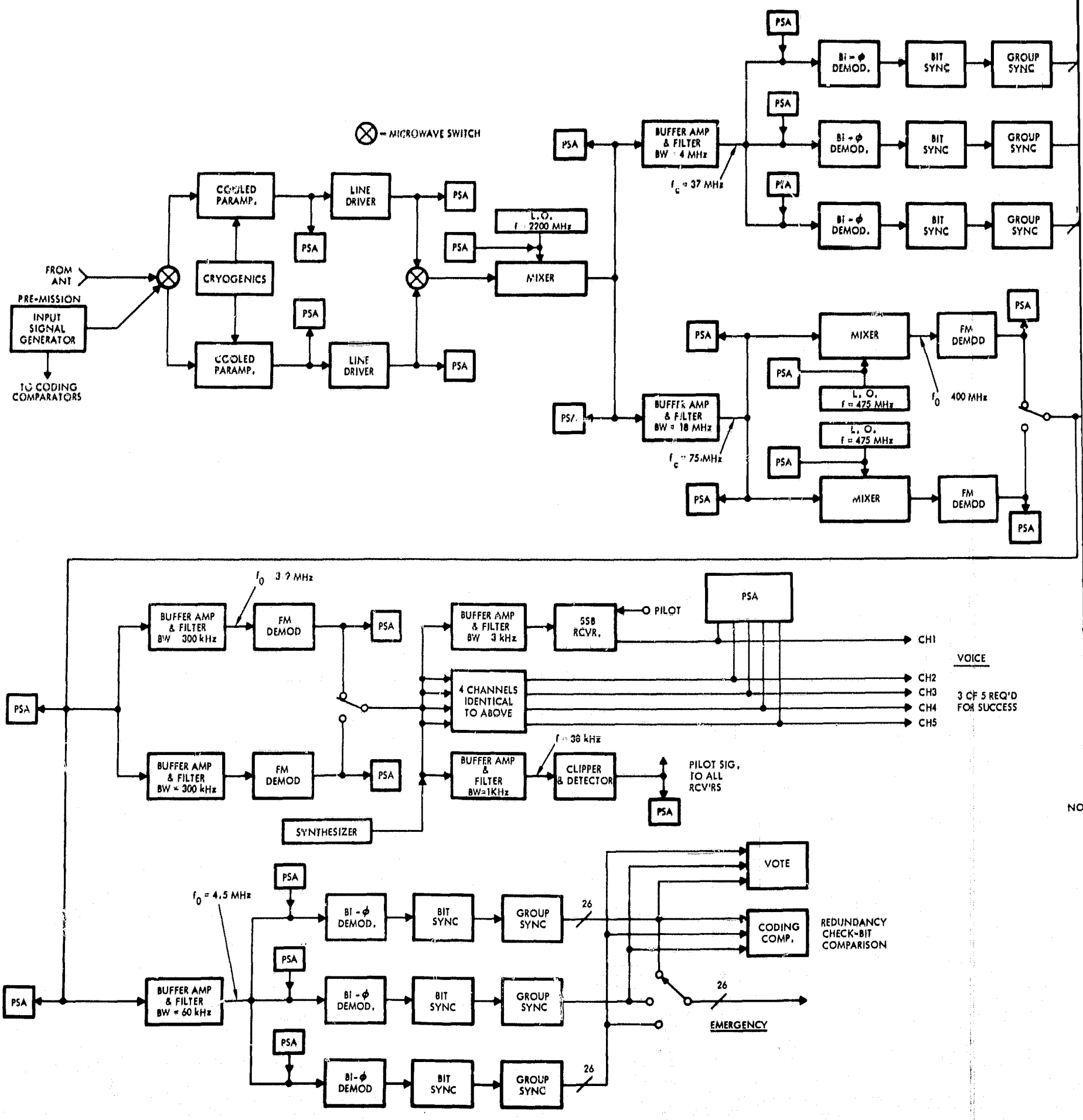
C4.2 Parameter Estimation

All the elements being verified in the ERS, with the exception of the telemetry channels, use some form of threshold detection. In most cases, we determine that a sufficient power level at some desired frequency exists. There are two main reasons for the relatively crude estimate of performance that we obtain. The primary reason is the non-stationary property of most of the signals in the ERS. There is little more that can be done to verify a voice-modulated subcarrier, than to ascertain that the carrier plus modulation are present at a sufficient power level. The other reason that we are restricted to crude estimation devices is the verification time limit of 100 msec , as called out in the technical description. Throughout the course of the case study, we have been reminded that it takes time to exercise control.

The PCM telemetry channels are verified by a more sophisticated parameter, bit error rate. This parameter is an accepted figure of merit for telemetry. As explained previously, we are able to compute this parameter within the time constraint. A running average of the bit error rate over many 100 msec intervals would be a better check on the system.

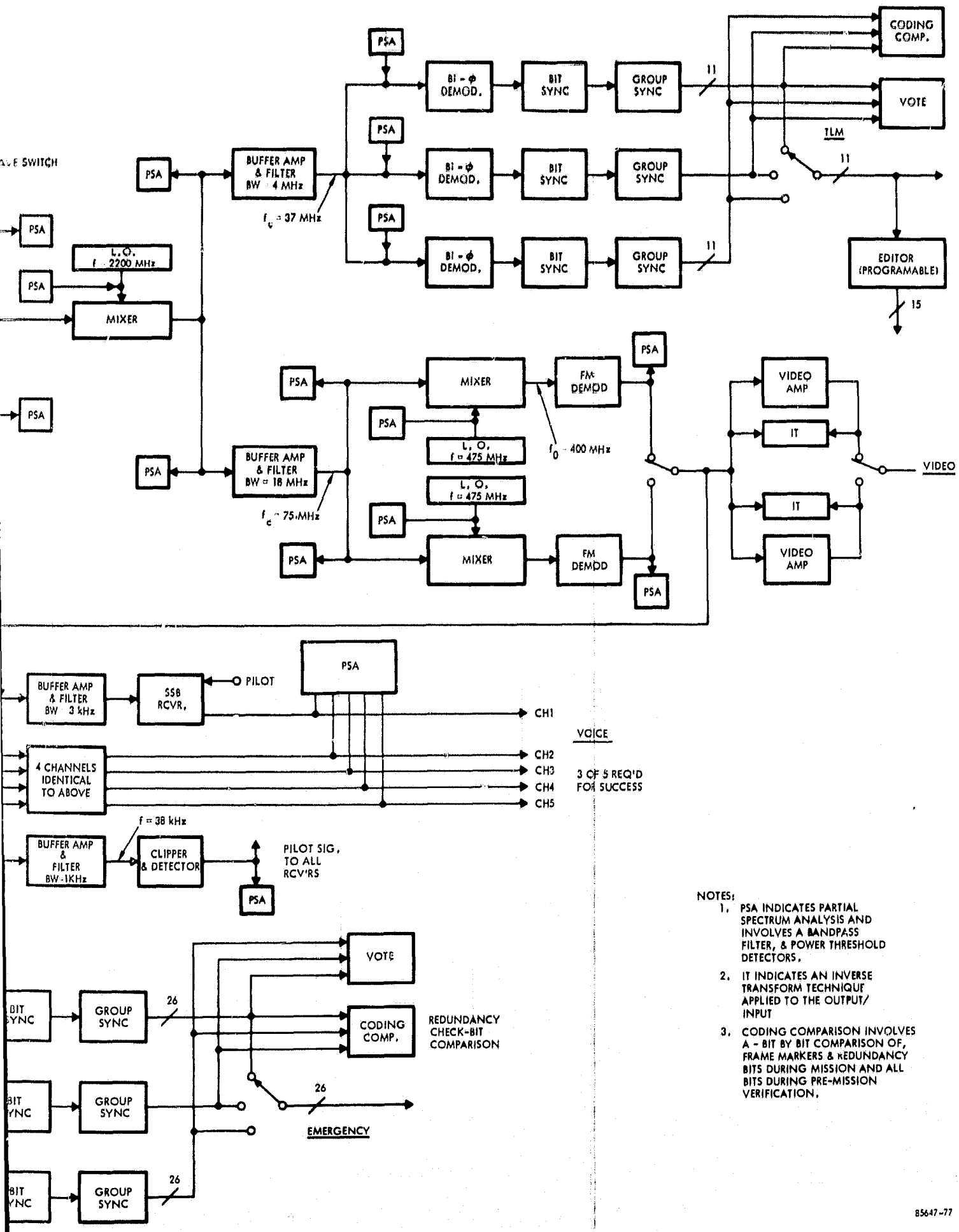
C4.3 Mapping

Conditional status will be a binary variable - either good or bad. For those verification equipments using threshold detectors, a crossing of the threshold level will be interpreted as a change of status. Excessive bit error rates in the PCM channels will constitute bad status. In this instance, we can be more specific by examing the bit error rate; and thus draw conclusions about the type problem that exists. For example, a slightly high bit error rate would probably be due to excessive noise, whereas a general failure would produce a very high error rate.



FOLDOUT FRAME 1

Figure C4
with



NOTES:

1. PSA INDICATES PARTIAL SPECTRUM ANALYSIS AND INVOLVES A BANDPASS FILTER, & POWER THRESHOLD DETECTORS.
2. IT INDICATES AN INVERSE TRANSFORM TECHNIQUE APPLIED TO THE OUTPUT/ INPUT
3. CODING COMPARISON INVOLVES A - BIT BY BIT COMPARISON OF, FRAME MARKERS & REDUNDANCY BITS DURING MISSION AND ALL BITS DURING PRE-MISSION VERIFICATION.

85647-77

Figure C4.1-2. ERS Functional Block Diagram with Verification Equipment in Place

FOLDOUT FRAME 2

APPENDIX D

PERFORMANCE AND DESIGN REQUIREMENTS

SPECIFICATION FOR REDUNDANT EQUIPMENTS

D1.0 SCOPE

This specification puts forth criteria to be imposed on redundant equipments in order to assure that the operational integrity of such equipments may be verified using automated procedures.

D2.0 APPLICABLE DOCUMENTS

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between documents referenced and the content of this specification, this specification shall take precedence.

SPECIFICATIONS

Not applicable.

STANDARDS

Not applicable.

DRAWINGS

Not applicable.

BULLETINS

Not applicable.

OTHER PUBLICATIONS

Final Report - Study of Techniques for the Verification of Redundancy without Disrupting Systems 18 September 1970, Radiation Systems Division Contract No. NAS10-7072

D3.0 REQUIREMENTS

D3.1 Performance

Not applicable.

D3.2 Program Design and Construction Standards

D3.2.1 General Requirements

Equipments shall comply with at least one of the following:

1. The outputs from redundant items shall be distinguishable, one from the other.

2. The output from a set of redundant items shall vary according to the number of operable items in the set. [1]

3. From each redundant item there shall be provided an output which is in addition to and isolated from the signal throughput path.

Additionally, equipments shall comply with one of the following:

4. Access to the output of each redundant item shall be provided.

5. Access to the combined outputs of redundant items shall be provided. [1]

Additionally, equipments shall comply with all of the following:

6. Access to such points as are determined to be necessary for the injection of verification signals shall be provided.

7. Equipment shall be tolerant of the effects of verification equipment such as electrical loading.

8. Accesses provided in compliance with criteria 4,5, or 6 shall be in a form acceptable to verification equipment.

D3.3 Requirements for Program Elements

Not applicable.

D4.0 QUALITY ASSURANCE

Not applicable.

---

[1] Compliance with this requirement will not be sufficient in cases where the status of each redundant item is to be determined.

D5.0 PREPARATION FOR DELIVERY

Not applicable.

D6.0 NOTES

Not applicable.

GLOSSARY

Acknowledgment	-	Coincidence development techniques whereby the receipt and desired effect of a command is indicated through a separate return signal.
Admissible Input	-	An input which is within the range or repertory of an equipment such that its transfer function can validly operate upon it.
Analog Signal	-	Any signal that is not digital. In general, a physical property (or properties) will be analogous to the information (measure) to be communicated.
Automated Redundancy Verification	-	A procedure whereby the presence (or absence) of redundancy can be verified without manual intervention at the redundant set. This is not intended to imply that the verification procedure can not be manually initiated, rather than manual reconfiguration (e.g., moving of cables) and checking (e.g., manual voltage measurements) at each redundant set is not required. Implicit to this requirement is that all elements in a set (both on-line and off-line) must be considered. Depending on the equipment and operational considerations, it may be necessary to identify the status of each element or simply the status of the set (e.g., 4 of 5 elements up).
Coding	-	Coincidence development techniques whereby the coincidence variable is developed by determining the number of information errors or the rate at which they occur. These techniques employ the characteristics of error detecting codes to establish a statement of status.
Compare Two	-	Coincidence development techniques whereby the outputs of two elements are compared on the basis of their values.
Continuous Verification	-	The automated verification of redundancy on a continuous basis (see Automated Redundancy Verification). Note that status identification of just an on-line element in a set is not redundancy verification unless the reliability of the off-line element(s) is great enough that it is reasonable to assume it is functioning (or capable of functioning when called upon). Continuous implies the verification is performed over all time on a real-time basis. This is not intended to exclude time sampling or "acceptable" delays due to filtering, processing or averaging. For digital systems, verification at bit or word rate would be considered continuous verification. In general, if the verification is controlled by the status identification equipment, it will be continuous and if it is initiated by a user on demand it will not be continuous.

Correlation	-	Coincidence development techniques whereby an inference to operational integrity is drawn through correlating the input with the output of the IBV.
Crosspower Spectral Analysis	-	Coincidence development techniques which involve the development of a frequency spectrum which is the combination of the spectra of two output signals.
Digital Signal	-	Any signal that is discrete in both time and signal space. During a finite time, a digital signal can send only a finite (or at most countably infinite) number of messages.
Element	-	The lowest level at which automated verification is established. Each member or entity of a redundant set is an element. Identifiable entities in the lowest level of Group are elements.
Error, Type I	-	The error which occurs when the status identification equipment indicates a failure in the principal system when one has not occurred.
Error, Type II	-	The error which occurs when the status identification equipment does not indicate a failure in the principal system when one has occurred.
Failure, Type I	-	A failure in the status identification equipment which causes Type I errors.
Failure, Type II	-	A failure in the status identification equipment which causes Type II errors.
Group	-	Any collection of elements which do not constitute a simple set. A group can be a redundant set which is not simple, a collection of redundant sets or a defined collection of items comprising interrelated redundancy. In general, status identification of groups involves system-related (as opposed to set-related) schemes.
IBV	-	Acronym for item being verified.
Inverse Transform	-	Coincidence development techniques which perform on the signal under observation, an operation which is the inverse of that performed by the item being verified and compares the result to IBV input.

Monitor Methods	-	Those coincidence development techniques which employ the storage of reference information concerning signal values or signal properties.
Off-Line Element	-	An element which is not communicating with successive functions. Depending on the circumstances, the element may or may not be performing its intended function, tenant signals may or may not be flowing and the element may be inert or stressed. Note that if the element is performing its intended function it will presumably be stressed.
On-Line Element	-	An element through which a tenant signal(s) is (are) flowing; the element is expected to perform its intended function and the output is communicating with successive functions.
Principal System	-	The system which contains elements whose status is to be identified.
Probability of Type I (Type II) Error	-	The conditional probability that the status identification equipment will commit a Type I (Type II) error on a single trial.
Probability of Type I (Type II) Failure	-	The unconditional probability that the status identification equipment will fail in such a way as to produce Type I (Type II) error.
Redundancy	-	The capacity of having more than one way to accomplish the same function where the alternative methods may assume the function within a prescribed time. So long as the alternate method is acceptable (in some sense), there is no implication of equivalent capability. Redundancy has been divided into two areas which fundamentally describe independence. These are interrelated redundancy and redundant sets.
Redundant Set	-	The collection of functional entities (equipment, programs, etc.) which together form the primary and backup (or alternate) capability of performing a particular function. Each entity or member of the set is termed an element of the set. Each element is considered to be dedicated solely to the particular function and to be operating independent of other sets, i.e., not shared with other sets. There is no restriction placed on the physical size or complexity of the set. A single nonredundant element would be a degenerate case of a redundant set. This is redundancy of degree zero.

Redundancy, Interrelated	-	Redundancy which cannot be described as a redundant set. Interrelated redundancy implies that redundancy of some segments of equipment is contingent on the status of other segments.
Signal	-	The alteration of a physical property or properties (voltage, frequency, pressure, etc.), via a prearranged convention, in order to convey information. Whenever information is transferred, conveyed or related from one point to another, a signal is involved. For the purposes of this study, signals have been divided into three functional (as opposed to statistical) groups - tenant signals, injected signals and supporting signals.
Signal Form Analysis	-	Coincidence development techniques which measure signal properties, as opposed to signal values, and compare against reference measures of these properties.
Signal, Idle	-	An injected signal which is used on-line in a real-time basis to substitute for the tenant signal in cases where the tenant signal will be absent for an appreciable length of time. Idle signals are primarily used for a continuous verification policy under the above conditions. An idle signal should exercise elements of the principal system to the extent that the tenant signal exercises these elements and should not be the cause of any ambiguity with tenant signals. Idle signals will be primarily used in principal systems which remain quiescent over the major portion of their mission such as command destruct systems, sentinel alarms, infrequently used communications, etc. The use of an idle signal does not interrupt normal operation of the principal system.
Signal, Injected	-	A signal which has been added into the principal system for the purpose of status identification. This signal can be static or dynamic. Injected signals can be further subdivided into idle signals, symbiotic signals and simulative signals.
Signal Simulative	-	An injected signal which replaces the tenant signal during the interruption of normal principal system operation for the purpose of status identification. The simulative signal must exercise the elements through which it passes and is usually deterministic. Simulative signals are often called stimulus signals.
Signal, Supporting	-	Those signals which are inherent to the status identification equipment but are not injected signals. These signals consist of the command, control and general communication signals within the status identification equipment.

Signal, Symbiotic - An injected signal which is interlaced, multiplexed, mixed or in some fashion comingled with the tenant signal on a noninterfering basis. Symbiotic signals are usually injected on a continuous basis and should exercise the elements through which they pass to the extent that the tenant signal exercises these elements.

Simple Set - A redundant set whose elements all have the same predecessors and followers. For a simple set, conditional status, or the conditional status of each element, can be deduced directly from knowledge of the output and possibly additional state variables which are otherwise unobservable. That is, if the output and any selected state variables are all "satisfactory," one can immediately conclude that the element is conditionally "satisfactory." This is contrasted to the situation where knowledge of the output and selected state variables is not sufficient to deduce the conditional status of an element without further logical operations or manipulations. An additional requirement on a simple set is that it may be treated as an entity from the standpoint of status identification, i.e., the conditional status can be determined without recourse to the status or operation of any other set.

Spectral Analysis - Coincidence development techniques which derive, by any means, partial or complete spectral characteristics of the signal under observation. These characteristics are compared against a reference in order to generate a coincidence variable.

Status - A qualitative, and usually broad, statement regarding the operational integrity of the item under contention, e.g., good, marginal, poor; go, no-go.

Status, Conditional - The status determined from the condition of element/set output signal (s) without prior knowledge of the input signal status or admissibility. The unconditional status of the element/set can only be determined after the status of the input signal is known. For a two level status, the following conclusions would be drawn from indications of unconditional status.

Input acceptable, output acceptable - element acceptable
Input acceptable, output acceptable - element unacceptable
Input unacceptable, output acceptable - reserve judgment
Input unacceptable, output unacceptable - reserve judgment

Status Variable	-	A variable, either continuous or discrete, which is identified as providing a measure of the operability, quality, or goodness of a set, element or function within an element. Status variables can either be developed through the status identification equipment or be identified as a state variable or output directly. The conditional status of equipment (in the principal system) is then inferred from the status variable onto a discrete status range The conditional status will become the equipment status only after the status of the input is identified.
Tenant Signal	-	That signal which is inherent to the principal system -- as opposed to any which are added for the purpose of status identification. Tenant signals are those signals which exist in the principal system before any consideration is given to status identification.
User Complaint	-	Coincidence development techniques whereby the status is directly determined by the observation and judgment of the user.
Value Check; Nonsequential	-	Coincidence development techniques which employ comparison of signal value (s) with reference value (s) without regard to the order in which the values occur.
Value Checks; Sequential	-	Coincidence development techniques which employ comparison of signal value in a sequential manner, deriving information both from the values and their order of occurrence.
Voting	-	Coincidence development techniques whereby inference to operational integrity is drawn from a logical polling of outputs or combinations of outputs.