Design of a Coordinated Plant Control System for a Marine Nuclear Propulsion Plant

by

Guillermo Baltra Aedo

Ingeniero Naval Electricista, Academia Politecnica Naval
(1977)

SUBMITTED TO THE DEPARTMENT OF
NUCLEAR ENGINEERING
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS OF THE
DEGREES OF

NUCLEAR ENGINEER

and

MASTER OF SCIENCE IN NAVAL ARCHITECTURE AND MARINE ENGINEERING

March 1981

Signature of Author ________________________
Department of Nuclear Engineering
March 25, 1981

Certified by ________________________
David D. Lanning, Thesis Supervisor

Certified by ________________________
Paul J. Nicholson, Thesis Co-Supervisor

Certified by ________________________
Douglas A. Carmichael, Thesis Reader

Accepted by ________________________
Allan F. Henry, Chairman, Departmental Graduate Committee

DESIGN OF A COORDINATED PLANT CONTROL SYSTEM FOR A MARINE NUCLEAR PROPULSION PLANT

by

GUILLERMO BALTRA AEDO

Submitted to the Department of Nuclear Engineering
on March 18, 1981 in partial fulfillment of the
requirements for the Degree of Nuclear Engineer
and Master of Science in Naval Architecture
and Marine Engineering

ABSTRACT

A methodology to achieve the preliminary design of a surveillance, data validation and control system (SDCS) for a power plant is developed. This method is applied to the specific case of designing a surveillance, data validation and control system for the N.S. Savannah nuclear propulsion plant. The study has two major sections. The first part develops the procedure for the preliminary design of the SDCS. The second part has the design and analysis of the pressure and volume control system for the N.S. Savannah pressurizer. This second part is included as an example of the procedure to be followed beyond the preliminary design stage.

The preliminary design stage starts with a study of the N.S. Savannah nuclear propulsion plant to obtain the input-output characteristics required for control. With this information, the SDCS is sized and eight alternative architectures are developed.

The selection of the best alternative is made by means of a figure of merit calculated as the Expected Monetary Value for each architecture. The results of this study indicate that a distributed architecture using star interconnection with serial communication is the optimal alternative for the specific case of N.S. Savannah nuclear propulsion plant.

The proposed design of the pressure and volume control system is made on the basis of a Proportional-Integral-Derivative (PID) controller, and motor operated valves. In order to test the transient responses obtained with the control system, a quasi-steady state model for the pressurizer is developed.

The pressurizer and the control system models are simulated in a programmable calculator code. The results of the simulation indicate that no integral action is required for the controller. Also the PID controller is tuned with a strong derivative action. The response of the system under transient conditions is predicted to be within the quarter amplitude decay criterion.

Thesis Supervisor: Dr. David D. Lanning

Title: Professor of Nuclear Engineering

Thesis Co-Supervisor: Dr. Paul J. Nicholson

Title: Visiting Scientist

Thesis Reader: Dr. Douglas A. Carmichael

Title: Professor of Ocean Engineering

To my dear wife Edurne

ACKNOWLEDGMENTS

I would like to express my gratitude to my thesis advisors, Dr. David D. Lanning, Dr. Paul J. Nicholson, and Dr. Douglas A. Carmichael, for their continued support and encouragement during the term of this work. I would also like to thank the support given by the Chilean Navy sponsoring this study. I would like to acknowledge the cooperation provided by the Digital Equipment Corporation and in particular I appreciate the assistance provided by Mr. Carl L. Noelcke, Mr. Timothy Litt, and Mr. Richard A. Gaudette. I would like to thank Mrs. Alice J. Sanderson and Mrs. Priscilla F. Kelly for production of the manuscript and drawings.

BIOGRAPHICAL NOTE

Guillermo Baltra A. was born the 16th of January, 1951 in Santiago, Chile. He completed grammar school studies at the Manuel Barros Borgoño School, and high school studies at Gabriela Mistral School. Both institutions are in Santiago, Chile. From 1966 to 1970, the author attended the Naval Academy where he graduated as a Navy officer with the higher rank in his promotion. From 1974 to 1977 he attended the Naval Polytechnic Academy where he graduated as a Naval Electrical Engineer with the higher rank in his promotion. From 1978 to 1981 he attended Massachusetts Institute of Technology, where his degree program included both Nuclear Engineer and Master of Science in Naval Architecture and Marine Engineering.

The author has previously published his Electrical Engineering thesis entitled "Design and Construction of a Nuclear Reactor Simulator" in 1977. He has worked in several Navy posts, including one as manager of a major electrical project at the Naval Shipyards at Talcahuano, Chile.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

APPENDICES

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

INTRODUCTION

In order to satisfy social needs, and with the assistance of accelerated technological development, complex industrial processes have been developed. Examples include the chemical industry, the metallurgical industry and the electric power generation industry. All of these industries are characterized by a coordinated operation among several devices which are organized to perform a specific task. Another feature of these processes is the high volume of data flowing between the processes and their central control systems. Central control systems are responsible for coordinating all the tasks and guiding the complex toward the optimal point of its capabilities.

Traditionally it has been the human operator who bore most of the control and coordination burden, but the volumes of information together with the short time constants involved in complex industrial processes, have threatened to overwhelm human reaction capabilities. This is especially true in situations with sharp changes in process parameters. Recent trends have been to utilize automatic controls which can handle such situations, thus making the process operation safer and more closely optimal.

The detailed analysis on industrial trends performed by Merrit (Reference Int.1) makes clear that direct digital control (DDC) and distributed digital control are the best automatic control system design alternatives for the near future, to replace the present analog control instruments that are now used in most process control systems. The reasons for replacing the analogic control with digital control are related to the following peculiar characteristics of digital control:

1. Digital control can handle a larger amount of information simultaneously.
2. Digital control has the capability of making logical decision.
3. Digital control has the capability of storing and recalling information.
4. Digital control algorithms can be easily updated by changing the software.
5. Digital control hardware can be used in association with very important tasks of sensor validation, process surveillance, and aiding the operator in critical situations.

These characteristics make digital control ideal for controlling devices to be used in a nuclear power plant in which a high availability plus an optimal fuel utilization, and overall, a high level of safety, are required. What is desired then is to find the appropriate digital architecture which performs these functions in the best possible way.

This thesis seeks mainly to answer the question of finding the digital architecture most appropriate for controlling the plant, performing data validation, plant surveillance, and operator aid. The plant chosen for the analysis (the N.S. Savannah nuclear propulsion plant) is a marine propulsion plant: this plant has a pneumatic-electrical control system (analog control system). Alternatives for replacing the original control system with a digital' control system with data validation and surveillance capabilities are studied, and a method for selecting the best architecture to perform these tasks is demonstrated.

The work has been divided into two major areas:

1. Design and selection of the optimal digital architecture.
2. Design of the automatic control system of one dedicated control loop in the plant. The loop chosen is the pressure and volume control at the pressurizer.

Because the scope of the work is broad, it was decided to develop a general methodology which first leads to the design and then to the selection of the optimal architecture. The design of the pressurizer control loop is intended as an example which can be followed with further work in other distributed control loops.

Although the design will be performed on a specific N.S. Savannah case, the methodology developed is intended to be general and it can be applied to other nuclear power control systems.

The sequence of the work performed in the first part of this study is summarized as follows.

1. Eight feasible architectures are selected among several alternatives, by using a weighting factor method. This step narrows the number of possibilities to a manageable group of alternatives.
2. Each one of the alternative designs is detailed to the component level.
3. A figure of merit for selecting the optimal alternative is developed. This figure of merit is a more elaborate method than

the weighting factors and requires: knowledge of the probability of failure for each alternative, their corresponding costs, and the payoff (negative or positive) that the failure or success of the architectures will involve.

4. In order to calculate the probability of failure for each alternative, the corresponding fault trees are derived. The basic event probabilities will be calculated on the basis of data supplied by component vendors.
5. The figure of merit is calculated and the best architecture is selected by analyzing the sensitivity of the figure of merit to changes in its parameters.

The complete process of designing the eight alternatives and selecting the optimal is explained in detail in Chapter 2. The methodology for the design process and the background for implementing the figure of merit are described in Chapter 1.

The second part of this work concerning with the design of the pressure and volume control system for the primary circuit of the N.S. Savannah nuclear reactor, follows these steps:

1. A statement of the methodology for designing the control system is given. Because the transfer functions of the devices involved in the control process are highly nonlinear, the common linear approaches (Back, Nyquist, root locus) are discarded. Thus, the only practical method available is to perform an analysis in the time domain in order to find the appropriate control system.
2. The time domain approach requires the state equations governing the

whole system (plant and controller). Therefore the state equations are developed. In order to simulate the pressurizer behavior a two-control volume approach has been used.

3. The control system chosen is a common PID controller operating on DC (direct current) actuators. The transfer functions for the controller and actuators are also developed.
4. Using the state equations, a computer code which will simulate the whole system behavior is then written.
5. The final step is to adjust the constants of the controller in the computer code, to demonstrate that the response of the system is acceptable for its future tasks.

The criterion for analyzing the acceptability of the control system will be based on the overshoot (quarter-amplitude decay criterion) and rise time of the response. (No unstable behavior will be accepted.)

The state equations and transfer functions are developed in Chapter 3. Chapter 4 is devoted to the design of the simulating code, and the tuning process of the controller. Chapter 5 is the final section, and contains the conclusions obtained from the work and some recommendations for further work in this field.

REFERENCES

1. Large systems are in control. Richard Merrit. Instrument and control systems. November 1978.

CHAPTER 1

DESIGN METHODOLOGY

1.1 INTRODUCTION

The flow diagram (Figure 1.1.1) shows the stages that have been followed in order to complete the new design for the control system of the N.S. Savannah nuclear propulsion plant. The A and B feedbacks (Fig. 1.1.1) point out the need of comparing the results obtained at the end of each stage with the boundary conditions previously stated. That is, if the system characteristics do not meet the operational requirements, the specific set of characteristics should be modified until the set meets the requirements.

The three last feedbacks are adjustments to the previous design. For example, if at the end of the plant integration and validation stage, the system does not work, the design process has to be fed back to the preliminary design stage where the changes that the designer deems appropriate should be made.

The scope of this work will cover up to the preliminary design stage. The preliminary design stage is considered finished when the optimal digital architecture is selected.

1.2 OPERATIONAL REQUIREMENTS

The operational requirements are implicit in the design objective. The design objective is defined as follows: "To replace the automatic control system of the N.S. Savannah nuclear plant by a modern system which offers better performance and safer operation than the original.

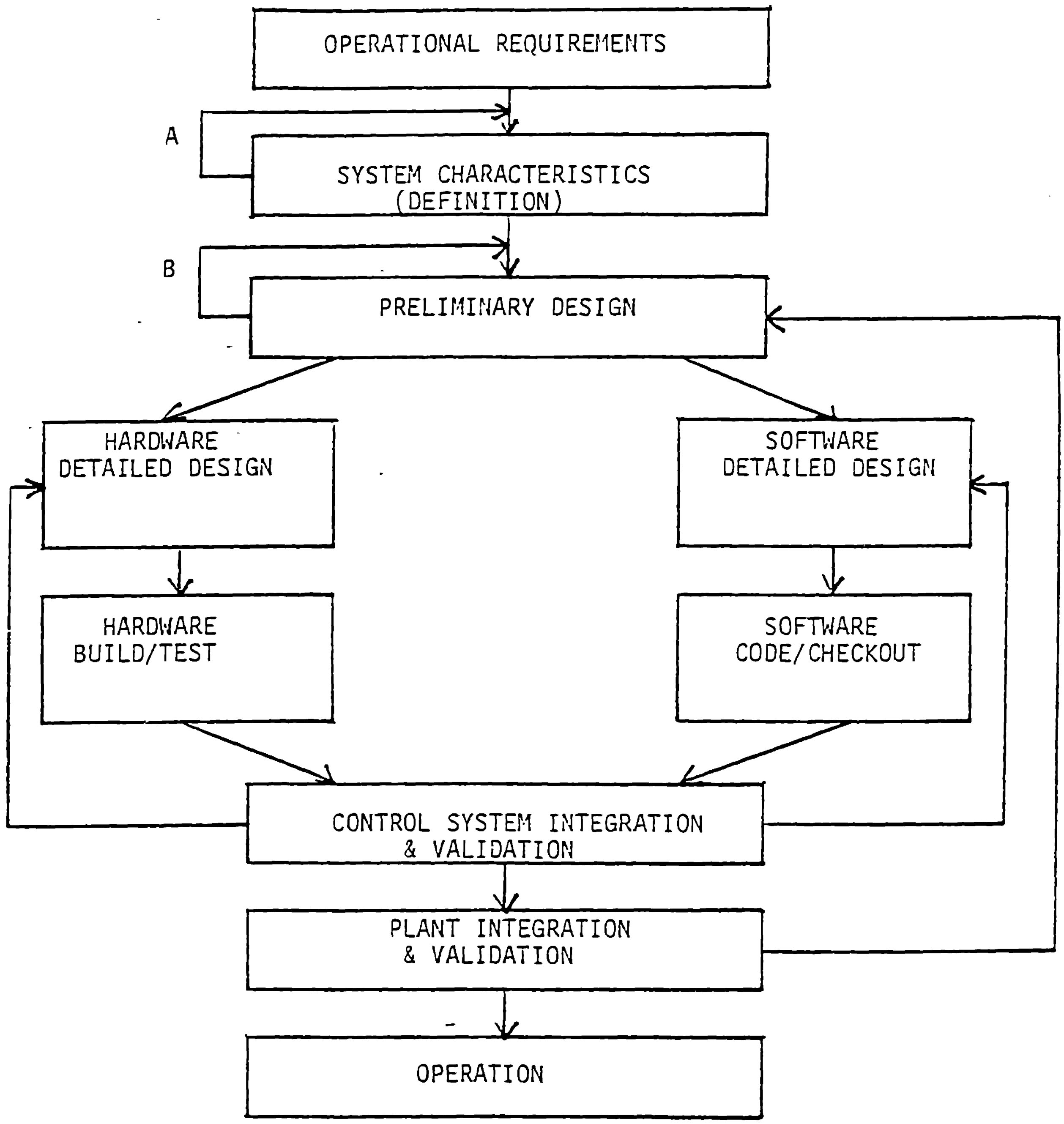


Figure 1.1.1 Design Process Flow Diagram.

The implementation of the new system has to be done with a minimum of changes in the propulsion plant itself, and using the technology available in the market." The performance of the control system can be judged by the behavior of the plant during transients. The improvement in safety during operation can be judged in terms of the features added to the control system which help the operator's performance. (This is a characteristic that the original design did not have.)

1.3 SYSTEM CHARACTERISTICS

The characteristics that the system must have in order to meet the stated objective are the following:

1. To supply, automatically, the necessary power to follow the load demand.
2. To assist the operator continuously on the state of the plant, supplying the necessary information with reliable values. This set of critical parameters displayed to the operator is called the safety state vector (Ref. 1.5).
3. To perform surveillance on-line over the plant, in order to make early detection of malfunctions.
4. To advise the operator, in case of accidents or malfunctions, on probable courses of action to follow.
5. To supply offline data related to the plant, as required by the plant management staff.

Each one of these characteristics requires a separate explanation.

1.3.1 COORDINATED CONTROL OF THE LOAD

Basically, this characteristic is similar to that of the original system. Appendix A has a brief description of the N.S. Savannah nuclear plant that is helpful in the following description. A detailed description of the plant is given in References 1.1 and 1.2.

The ship propulsive plant can be seen as a system of variable load, which must adapt to the different speeds ordered from the bridge. This situation is especially critical when the ship arrives or leaves ports, and when the ship is crossing channels. The variable load has to be matched by the power supply system (the reactor).

Seven loops of dedicated automatic control make up the whole coordinated control system.

- Pressure and volume control in the pressurizer
- Level control in the steam generators
- Steam pressure and flow control in the secondary circuit
- Load following and temperature control in the primary circuit
- Propeller speed control (optional, only when manoeuvring)
- Pressure and temperature control in the buffer seals system
- Temperature and flow control of the primary purification system

1.3.2 SAFETY CONTROL

Safety control is another characteristic retained from the original system. The distinguishing characteristic of the safety control is its absolute independence from the diagnostic and coordinated control system. This type of control will not be examined in this study.

1.3.3 DATA VALIDATION

Validation of the information coming from the sensors is a new operation required by the control system. Fundamentally, data validation means to eliminate the failure uncertainty related with the information given by the instruments. This uncertainty is caused by sensor failures, sensor aging or large random noise added to the readings.

One method used to validate instrument readings is to take 3 signals coming from 3 different sensors (same parameter). The readings are averaged; if one sensor deviates by a specific amount from the average, it is considered to have failed, and the readings coming from that sensor are neglected. The validation process follows with the remaining sensors. The obtained averages are smoothed by means of a fitting algorithm (for example, the least squares method) applied to a group of previous readings, e.g., the ten readings immediately before the current reading. In this way it becomes a smoother signal showing clearly its trend. Finally, the signal is input to a mathematical filter (for example the Kalman filter) with the aim of obtaining a signal which is the best estimation of the variable that can be obtained. Another consequence of using a mathematical filter is that some variables which are not directly measureable can also be estimated.

The information validated in this way can follow four different paths:

1. It can be displayed directly to the operator
2. It can be used as an input to the automatic control algorithms

3. It can be used as an input to the diagnosis algorithms
4. It can be stored offline for further analysis

In the new control system design the data coming from the following subsystems will be validated.

1. Nuclear parameters of the reactor
2. Control rods
3. Primary circuit with its pumps
4. Steam generators
5. Main feed pumps
6. Condensate pumps
7. High and low pressure heaters
8. Main condenser
9. Deaerating tank
10. Main turbines
11. Buffer seals system
12. High pressure steam circuit
13. Primary purification system
14. Electrical generation system.

Only the validated data which are meaningful to the operator will be displayed on a top level display. (Other information can be obtained on demand.) This preselective process is intended to relieve the operator from considering unimportant signals and to show him the significant variables which will help him in making decisions. The preselected set of variables is called the safety vector of the plant (Ref. 1.5).

1.3.4 SURVEILLANCE AND DIAGNOSIS

This is one particularly interesting feature added to the control system. This characteristic is defined as the ability to detect a malfunction and to diagnose its cause.

There are several techniques which aim to achieve these capabilities. To detect malfunctions, the following techniques are available (Refs. 1.6, 1.7, 1.8, 1.9):

- Spectral densities method
- Reactivity balances method
- Coherence function method
- Linear discriminating function
- Multivariable analysis

To diagnose the detected errors the following techniques are available (Refs. 1.10, 1.5):

- Linear regression analysis
- Pattern recognition
- Thermodynamic balances
- Cause-consequence analysis.

In order to estimate the implicit variables (variables which are not directly measureable), the control algorithm will have a model of the process which is controlled. The reactivity balances and thermodynamic balances method also use a model of plant to perform their diagnosis functions. This makes the two latter techniques suitable to be employed together with the filtering technique by shearing the common model of the plant.

1.3.5 OPERATOR ADVICE

Once the malfunction or accident is detected and diagnosed, the system must advise the operator on the proper course of action to cope with the emergency. To do so a predicting algorithm has to be added, which functions foreseeing the behavior of the variables if the situation continues as at the actual moment. There are also several techniques devoted to this advising function. Some of them are (Refs. 1.3, 1.11):

- Fault treee analysis
- Cause consequence charts.

1.3.6 OFFLINE DATA SUPPLY

This feature is intended to be a help to the reactor plant managers. All relevant data will be stored offline to be available for consulting.

1.4 PRELIMINARY DESIGN

The goal of the preliminary design stage is to produce several alternatives satisfying the operational requirements and system characteristics. After that the most suitable alternative will be selected by means of a figure of merit. This figure of merit has to reflect the design policy governing the work.

Once the minimum acceptable requirements of safety and performance are satisfied, the process of selecting the best alternative has to be ruled by a figure of merit which penalizes high cost and low availability. Cost is defined as the total cost of the system calculated at its Net Present Value (NPV). By availability is meant the percentage of operating time compared with its useful life, measured over the life cycle of the control and surveillance system.

The whole problem shows the characteristics of a decision analysis case. The decision maker has several alternatives to decide, each alternative has its own cost. Moreover, the success or the failure of each alternative involves a certain amount of benefits or losses. Finally each alternative has a particular probability of being successful during its time between repairs.

Therefore a figure of merit obtained by applying decision analysis theory is appropriate to this case.

1.4.1 EXPECTED MONETARY VALUE

The Expected Monetary Value (EMV) is a technique used to assess the decision process among several feasible alternatives. Each one of the alternatives satisfies the basic requirements, but they have different costs and different benefits. These benefits are also tied to different probabilities of achieving them.

The EMV of one alternative with several outcomes is obtained by multiplying each possible cash outcome by its probability of occurrence and summing these products over all possible outcomes. The decision analysis theory states that a decision maker will be indifferent between two alternatives with the same EMV and he will prefer the alternative with the higher EMV (Ref. 1.4).

Thus the EMV has the appropriate characteristics to be used as a figure of merit for this study.

The first step to achieve the figure of merit (EMV) is to develop a decision tree which is a graphic display of the alternatives faced by the decision maker. The alternatives that can be controlled by the decision maker are represented by a square, or if they are ruled by chance, and they appear as circles.

Figure 1.4.1 shows a decision tree for a simple but general case. A manager placed at S faces N alternatives e_0, e_1. ... e_N and each one of them has a set of further decisions to be taken by the person, for example, at the point A_0 are a_{01}, a_{01},...a_{0N} alternatives to choose. The same rules for the A_i nodes. The subset of alternatives a_{i1}, a_{ij}, a_{ip} which is a general branch of the decision tree, has a related cost and a related payoff. The payoffs are tied with a finite probability of success of the alternative, in other words, the alternative has a finite probability of obtaining a positive revenue (success) measured in money, and a finite probability of getting a negative revenue also measured in money, or a less desirable revenue than the first one (failure).

The following nomenclature will be used.

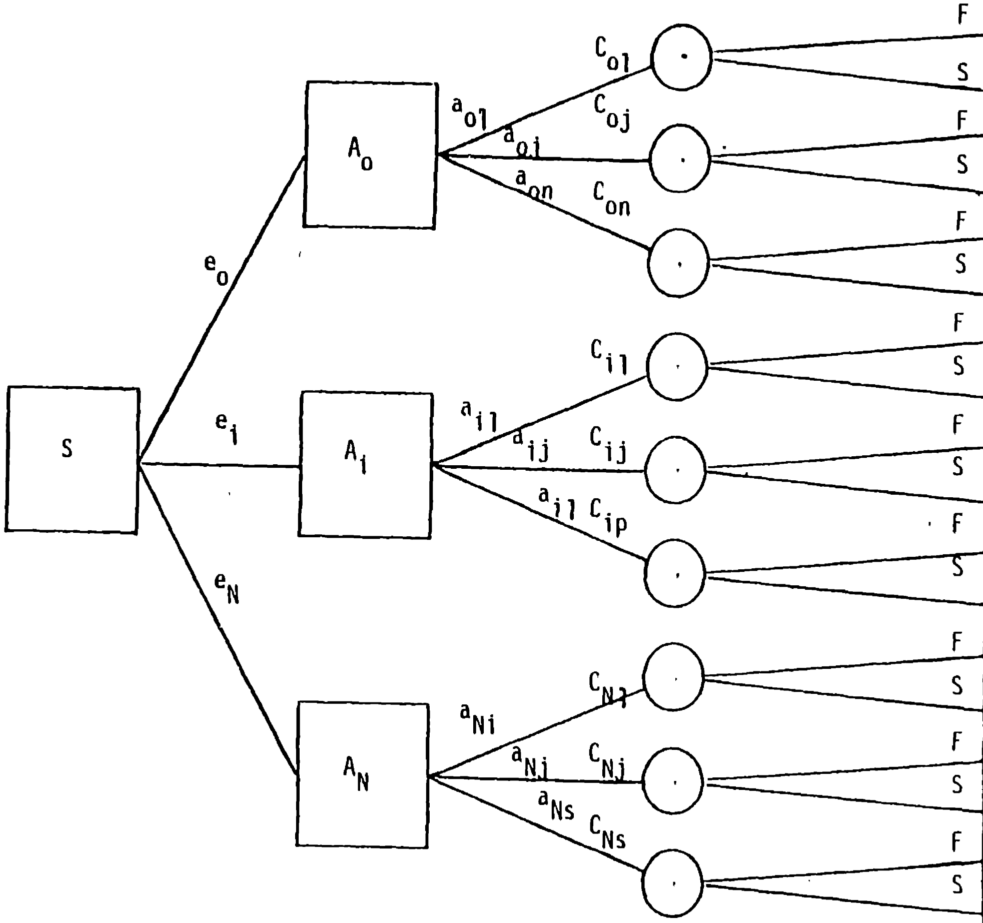
POS(a_{ij}) = Payoff of success in alternative a_{ij}

POF(a_{ij}) = Payoff of failure in alternative a_{ij}

PF(a_{ij}) = Probability of failure in alternative a_{ij}

PS(a_{ij}) = Probability of success in alternative a_{ij}

From the theory of decision analysis the EMV of e_i branch is



Probability	PAYOFF
$PF(a_{o1})$	$POF(a_{o1})$
$PS(a_{o1})$	$POS(a_{o1})$
$PF(a_{oj})$	$POF(a_{oj})$
$PS(a_{oj})$	$POS(a_{oj})$
$PF(a_{on})$	$POF(a_{on})$
$PS(a_{on})$	$POS(a_{on})$
$PF(a_{i1})$	$POF(a_{i1})$
$PS(a_{i1})$	$POS(a_{i1})$
$PF(a_{ij})$	$POF(a_{ij})$
$PS(a_{ij})$	$POS(a_{ij})$
$PF(a_{ip})$	$POF(a_{ip})$
$PS(a_{ip})$	$POS(a_{ip})$
$PF(a_{N1})$	$POF(a_{N1})$
$PS(a_{N1})$	$POS(a_{N1})$
$PF(a_{Nj})$	$POF(a_{Nj})$
$PS(a_{Nj})$	$POS(a_{Nj})$
$PF(a_{Ns})$	$POF(a_{Ns})$
$PS(a_{Ns})$	$POS(a_{Ns})$

Figure 1.4.1 Generalized Decision Tree.

$$EMV_i = \sum_j POS(a_{ij}) \times PS(a_{ij}) + POF(a_{ij}) \times PF(a_{ij}) - C_{ij} \qquad (1.4.1)$$

To make the decision the manager has to choose the higher EMV_i, in other words:

$$\text{selected alternative} = \max\ [EMV_i] \qquad (1.4.2)$$

The main obstacle to following this procedure is the process of obtaining the probability data. Most architectures have no probability data available because they are not even implemented. To solve this problem, the designed architectures are detailed to a level of standard market components, and those devices do have probability data supplied by the vendors. To reach the probability of failure of the whole system, the fault tree analysis theory is required.

The component costs come from direct questioning of suppliers.

The cost of the software and its probability of failure are special issues which require careful study. These considerations are developed later in the work.

Once the EMV analysis is finished, the best architecture is that with the higher EMV; a consistency check with experience and common sense should, of course, also be performed. The next step is to perform a sensitivity study to detect critical points in the design and correct them. Also the sensitivity analysis gives a good insight of the variables' impact; finally most of the conclusions and recommendations come from this sensitivity study.

With all the mentioned steps completed, the preliminary design is achieved.

The next chapter is devoted to the goal of designing the feasible architectures competing as alternatives in the special case of the N.S. Savannah propulsion plant.

REFERENCES

1.1 Nuclear merchant ship rector, final safeguards report. Volume I, Description of the N.S. Savannah. BAW-1164 (Vol. I).

1.2 N.S. Savannah training manual, ship and systems description. Vols. I and II, N.S. Savannah technical staff, Babcock and Wilcox, Tood Shipyards,, Galveston, Texas.

1.3 Use of the cause-consequence charts in practical system analysis. Dan Nielsen. Reliability and fault tree analysis, SIAM, Philadelphia, 1975.

1.4 Decision analysis. Howard Raiffa, Addison-Wesley, July 1970.

1.5 On-line power plant alarm and disturbance analysis system. EPRI NP-613, Project 891. February 1978.

1.6 The use of signal coherence for anomaly detection in nuclear rectors. R.W. Albrecht. Nuclear Technology, Vol. 14, June 1972.

1.7 An on-line reactor surveillance algorithm based on multivariate analysis of noise. K.R. Peity, J.C. Robinson. Power plant dynamics control and testing applications symposium, Knoxville, Tennessee, Sept. 3-5, 1975.

1.8 Experiments on reactivity balance as malfunction detectors for research reactor. Fukutoni, Monta. Journal of nuclear science and technology. Jan. 1970, pp. 54-56.

1.9 On the application of pattern recognition methods to reactor malfunction diagnosis. R.C. Gonzales. Power Plant Dynamics Control and Testing Applications Symposium. Knoxville, Tennessee, Sept. 3-5, 1975.

1.10 Study on diagnosis system of nuclear and reactor power plant.

1.11 J. Wakabayashi, K. Yamaguchi, S. Ina, J. Incondo. The second power plant dynamics control and testing applications symposium. Knoxville, Tennessee, Sept. 3-5, 1975.

1.12 Fault trees for diagnosis of system fault conditions. Howard E. Lambert and George Yadigaroglu. Nuclear Science and Engineering, 62 (20-34), 1977.

CHAPTER 2

PRELIMINARY DESIGN

2.1 INTRODUCTION

This chapter develops the expected money value (EMV) technique already explained in Chapter 1. The specific case under design is the N.S. Savannah nuclear propulsion plant (Ref. 2.9); the information concerning that system is unclassified and is accessible in the open literature.

The aim of this thesis is not to seek an actual replacement of the N.S. Savannah nuclear plant control system. Rather, that plant is used as a basis for a general design procedure, permitting the development of comparisons between current designs and proposed alternatives. Comparative figures are to be developed based on those parameters which are not common for every design alternative. With this constraint the given costs are not the final costs, but are the costs of every distinct parameter which is not common with the other alternatives. Installation, operation, and maintenance costs are assumed to be similar for every alternative. These costs and those for other external factors such as power sources are not included.

The design analysis procedure starts in Section 2.2 with the description of functions required for the surveillance, diagnostic, and control system (SDCS). The next step is given in Section 2.3 where the specific tasks required of each block of the SDCS are explained in detail. The data given in this section form the basis for sizing the possible architectures.

Because the range of possible alternatives to be used in the design is wide, Section 2.4 develops a method to narrow down the spectrum of architectures, ending up with eight feasible alternatives. Section 2.5 explains in detail how these eight different architectures are designed, and what their components are.

Once the hardware modules are specified, the next step is to develop the fault trees appropriate for each alternative; that procedure is given in Section 2.6. In Section 2.7 event probabilities are applied to the fault trees already developed. Costs for each alternative are determined in Section 2.8 and expected money value (EMV) analysis is performed in Section 2.9. Finally, this analysis identifies the architecture with the best figure of merit (EMV), thereby identifying the preferred SDCS preliminary design. This selection is analyzed further in Section 2.10 where sensitivity analyses are performed. The assumptions and uncertainties involved in the design process are tested to determine if they could seriously affect the final decision.

2.2 ORGANIZATION AND DEFINITION OF THE FUNCTIONS

The proposed list of the control system functions is independent of the chosen digital architecture, in other words, all candidate design alternatives must follow a common functional organization. In Reference 2.1 Trchka and Ash propose the following task division for a control system.

a. Control functions

- basic control

- advanced control

b. Communications functions

- tactical communications
- strategic communications.

This task division implies a hierarchical order within it. The following subsections broaden the concept more.

2.2.1 CONTROL FUNCTION

Control functions are related to process variables and the actions needed to keep them at specific levels. These functions are divided into two groups:

- Basic functions or level one functions are those involved in regulating simple variables such as temperature, pressure, etc.
- Advanced functions (also called supervisory or level two functions) are related to variables which require the calculation of special complex algorithms not used in a routine fashion in the control of basic variables.

2.2.1.1 BASIC CONTROL FUNCTIONS

The seven basic control functions required by the N.S. Savannah propulsion plant are (Ref. 2.9):

- water level control at both steam generators
- pressure and volume control at the pressurizer
- temperature control at the primary system tied to a load following capability

- speed control at the propeller shaft (optional)
- temperature and pressure control in the buffer seals system
- temperature and flow control in the primary purification system
- pressure control in the secondary system.

The original system does not have data validation functions, but the new design will be required to have them. Thus the following subsystems may require validation:

- nuclear parameters
- control rods
- primary circuit
- pressurizer
- steam generators
- feed water system
- secondary steam system
- main condenser
- turbines
- buffer seals system
- primary purification system
- electrical generation and distribution.

2.2.1.2 ADVANCED CONTROL FUNCTIONS

The following functions performed by the system are considered to be advanced:

- acquisition and display of safety parameter display (SPDS) (validated plus estimated measurements)
- detection and diagnosis of malfunctions

- forecasting the behavior of the variables and advising the operator
- communication control
- continuous checking of hardware failures

Most of these functions are identified as required for on-line plant disturbance analysis (Ref. 2.11) as well as for direct digital control.

2.2.2 COMMUNICATION FUNCTIONS

The communication functions are divided into two groups: tactical and strategic.

2.2.2.1 TACTICAL COMMUNICATIONS

This kind of communication is a short-term value communication, such as the representation at the display of current values of the process variables. Tactical communications occur on-line in the following links:

- sensor-processor communications
- processor-actuator communications
- processor-processor communications
- operator-processor communications.

2.2.2.2 STRATEGIC COMMUNICATIONS

The strategic information has a long-term value and is used in planning new goals for the plant or planning changes in operations. Strategic communications are typically employed offline since they imply background analysis of data previous recorded and observed on line.

They consist only of:

- processor-operator communications.

2.3 FUNCTIONS SPECIFICATIONS

The control functions listed in Section 2.2 are distinguished in such a way that their performance can be sustained with reasonable independence. Accordingly each can be considered as a unit or block of processing power with its own inputs and outputs. The remainder of this section is devoted to the specification of the inputs and outputs appropriate for each block based on information given in Ref. 2.9. Also the number of channels required for each type of signal is enclosed by parentheses. This information is used later when sizing the architectures. Table B.3 (Appendix B) has a summary of all the parameters shown in this section.

2.3.1 BASIC CONTROL FUNCTONS

2.3.1.1 WATER LEVEL CONTROL OF STEAM GENERATORS

The inputs are

-reference level signal (1)

-actual level signal (2)

-feed water flow signal (2)

-steam flow signal (2).

The outputs are:

-position signal to the feed water valve (2)

-hardware failure signal (1).

2.3.1.2 PRESSURE AND VOLUME CONTROL IN THE PRESSURIZER

When the system is in the automatic mode, the inputs are

-reference level signal (1)

-reference pressure signal (1)

-actual level signal (1)

-actual pressure signal (1)

-overpressure reference signal (1).

The outputs are:

-position signal to spray valves (1)

-position signal to make-up valve (1)

-position signal to let-down valve (1)

-control signal to heaters (5)

-control signal to relief valve (1)

When the system is in the manual mode, the input signals are:

-position signal from make-up valve (1)

-position signal from let-down valve (1)

-position signal from spray valves (1).

The output signals are:

-position signal to make-up valve (1)

-position signal to let-down valve (1)

-position signal to spray valve (1).

In both modes, the inputs are:

-signal for changing spray valve (1)

-signal for transferring auto-manual spray valve (1)

-signal transferring auto-manual spray valve (1)

-signal transferring auto-manual let-down valve

-control signal to close overpressure valve.

The outputs are:

-status mode signal for make-up valve (1)

-status mode signal for sprays (1)

-status mode signal for let-down valve (1)

-cut the heaters down signal due to low water level (1)

-hardware failure alarm signal (1)

2.3.1.3 LOAD FOLLOWING AND PRIMARY TEMPERATURE CONTROL

When the system is in the automatic mode the inputs are:

-steam flow signal from secondary system (1)

-temperature signal from cold leg (1)

-temperature signal from hot leg (1)

-neutron flux level signal (1)

-reference temperature signal (1).

The outputs are:

-position signal to the control rod in service (1)

-position signal from control rods (5)

-position signal from groups of control rods (21)

The output signals are:

-position signals to control rods (21)

-position signal to groups of control rods (5)

In both modes the inputs are:

-command signal to auto-manual (1)

-signal to start fast insertion (1)

-signal to stop fast insertion (1)

The outputs are:

-status mode signal (1)

-signal to start fast insertion (1)

-signal to stop fast insertion (1)

-hardware failure alarm signal (1)

2.3.1.4 STEAM PRESSURE CONTROL OF SECONDARY SYSTEM

The input signals are:

-reference pressure signal (1)

-actual pressure signal (1)

-main condenser back pressure signal (1)

-command signal to fast closing valves (2).

The outputs are:

-control signal to bypass valve to the main condenser (1)

-command signals to fast closing valves (2)

-hardware failure signal (1)

2.3.1.5 SPEED CONTROL OF THE PROPELLER SHAFT

When the system is in the automatic mode, the input is:

-reference speed signal (1).

The outputs are:

-position signal to throttle valve (1)

If the system is in manual mode the inputs are:

-command signal to ahead throttle valve (1)

-command signal to astern throttle valve (1)

-command signal to guardian throttle valve (1)

The outputs are:

-command signal to ahead throttle valve (1)

-command signal to astern throttle valve (1)

-command signal to guardian throttle valve (1)

In both modes the inputs are:

-command signal to quick-closing valves (2)

-command signal auto-manual (1)

-shaft speed signal (1).

The outputs are:

-status mode signal (1)

-valve closing signal due to overspeed (2)

-valve closing signals by operator command (2)

-hardware failure signal (1).

2.3.1.6 TEMPERATURE AND FLOW CONTROL OF THE PRIMARY PURIFICATION SYSTEM

When the system is in the automatic mode, the inputs are:

-total flow signal (1)

-reference total flow signal (1)

-temperature signal (1)

-reference temperature signal (1).

The outputs are:

-position signal to flow control valves (2)

-position signal to cooling flow control valve (1).

If the system is in the manual mode the inputs are:

-position signal to flow control valves (3)

-position signal to cooling flow control valve (1).

In both modes the input signals are:

-command signal auto-manual for flow control (1)

-command signal auto-manual for temperature signal (1)

-open-close signal to 18 circuit valves (18).

The output signals are:

-status mode flow control valves (1)

-status mode cooling flow control valve (1)

-command signals to the 18 valves (18)

-hardware failure signal (1).

2.3.1.7 PRESSURE AND TEMPERATURE CONTROL IN THE BUFFER SEALS SYSTEM

The inputs when the system is in the automatic mode are:

-pressure signal from the reactor (1)

-buffer seal water pressure signal (1)

-reference signal for differential pressure (1)

-reference temperature signal for desurger's tanks (1)

-temperature signals from desurger's tanks (3)

-buffer seal water temperature (1)

-discharge pressure signal from booster pumps (1)

-reference pressure signal for discharge pressure of booster pumps (1)

The output signals are:

-position signal to bypass valve controlling differential pressure (1)

-command signals to booster pumps (3)

-command signals to desurger heaters (3)

-position signal to valve controlling the cooling flow (1)

-command signal to emergency booster (1).

If the system is operating under manual mode, the inputs are:

-position signal to bypass valve (1)

-position signal to valve controlling the cooling flow (1).

The output signals are:

-position signal to bypass valve (1)

-position signal to cooling flow control valve (1)

-command signals to charging pumps (3).

In both modes the inputs are:

-command signal auto-manual for differential pressure control (1)

-command signal auto-manual for temperature control (1).

The outputs are:

-status signal manual-auto mode in controlling differential pressure (1)

-status signal manual-auto mode in controlling water temperature (1)

-hardware failure -signal.

2.3.1.8 VALIDATION OF NUCLEAR PARAMETERS

The inputs to this block are:

-log count rate from start-up channels (3)

-log count rate from intermediate range channels (3)

-neutron flux level from power range channels (3).

The outputs of this block are:

-period signal (1)

-count rate signal (1)

-neutron flux level signal (1)

-hardware failure signal (1).

2.3.1.9 DATA VALIDATION OF PRIMARY SYSTEM

This block does not include the primary pumps. Its inputs are:

-starboard reactor outlet temperature (3)

-port reactor outlet temperature (3)

-discharge temperature port steam generator (3)

-discharge temperature starboard steam generator (3)

-reactor outlet pressure (port) (3)

-primary flow port circuit (3)

-primary flow starboard circuit (3)

-cooling flow to primary pumps (12)

-status signals cooling water valves (12)

-status signals from main isolation valves (12).

The outputs from the block are:

-primary pressure port circuit (1)

-primary temperatures reactors outlets (2)

-primary temperature at the suction of primary pumps (2)

-average temperature for each circuit (2)

-total average temperature (1)

-temperature differential at each circuit (2)

-status signals for main isolation valves (4)

-low temperature alarm signals primary circuits (2)

-high temperature alarm signal at the reactor outlet (1)

-low primary flow alarm signals (2)

-high pressure alarm signal (1)

-low reactor pressure alarm signal (1)

-hardware failure alarm signal (1).

2.3.1.10 DATA VALIDATION OF CONTROL RODS 1-10 AND GROUPS 1-3

The overwhelming amount of data related to this function make it advisable to divide the block into two parts. This block includes the data coming from control rods 1-10 and the group 1-3. The inputs to this block are

-position signals from the control rods (30)

-position signal from the groups (9)

-status signal of the control carrier clutches (30)

-status signal of the control rod motors (30)

-status signal of the control rod groups (9)

-temperature signals from the control rod motors (30)

The output signals are:

-position signal of the control rods (10)

-position signals of the groups (3)

-status signals of the carriers (10)

-status signals of the control rod motors (10)

-high temperature in control rod motors alarm signal (1)

-status signal of the control rod groups (3)

-hardware failure signal (1).

2.3.1.11 DATA VALIDATION OF CONTROL RODS 11-21 AND GROUPS 4-5

The input signals are:

-position signals from control rods (33)

-position signals from the groups (6)

-status signals of the control rod carrier clutches (33)

-status signals from control rod motors (33)

-status signals from control rod groups (6).

The output signals are:

-position signals from control rods (11)

-position signals of control rod groups (2)

-status signals of the control rod carrier clutches (11)

-status signals from control rod motors (11)

-high temperature at control rod motor alarm signals (11)

-status of control rod groups (2)

-hardware failure signal (1).

2.3.1.12 VALIDATION FOR PRESSURIZER DATA

The input parameters are:

-water level (3)

-pressurizer pressure (3)

-pressurizer temperature (3)

-surge line temperature (3)

-status signal of each heater bank (15)

-status signal of each spray valve (6)

-status signal of each relief valve (6).

The outputs are:

-water level signal (1)

-pressure signal (1)

-temperature signal (1)

-surge line temperature signal (1)

-status signal for each heater bank (5)

-status signal for each spray valve (2)

-status signal of each relief valve (2)

-high temperature alarm signal (1)

-high water level alarm signal (1)

-low water level alarm signal (1)

-high pressure alarm signal (1)

-low pressure alarm signal (1)

-hardware failure signal (1).

2.3.1.13 DATA VALIDATION OF BUFFER SEALS SYSTEM

Because of the high number of signals involved, the validation task is split into two blocks. Buffer seal flows are discussed in Section 2.3.1.21.

The inputs are:

-surge tank level signal (3)

-surge tank pressure signal (3)

-surge tank temperature signal (3)

-discharge pressure from booster pumps (3)

-pressure signal from charging pumps discharge (3)

-temperature signals from desurger tanks (18)

-status signals of booster pumps (6)

-status signal of charge pumps (9)

-status signals of desurger tanks' heaters (18)

-status signal of bypass valves (6)

-status signal of cooling flow control valve (3)

-status signal of surge tank drain valve (3).

The output signals are:

-surge tank level signal (1)

-surge tank temperature signal (1)

-surge tank pressure signal (1)

-discharge pressure signal of charge pumps (1)

-temperature signals from desurger tanks (6)

-status signal of booster pumps (2)

-status signal of charge pumps (3)

-status signals of desurger tanks' heater (6)

-status signals of bypass valves (2)

-status signal of cooling flow control valve (1)

-status signal of cooling flow control valve (1)

-high surge tank temperature alarm signal (1)

-high surge tank level alarm signal (1)

-low surge tank level alarm signal (1)

-high surge tank pressure alarm signal (1)

-low discharge pressure of booster pumps alarm signal (1)

-low differential pressure alarm signal (1)

-high cooler's discharge temperature alarm signal (1)

-hardware failure alarm signal (1).

2.3.1.14 DATA VALIDATION OF STEAM GENERATORS

The input signals are:

-water level for each steam generator (6)

-pressure signal for each steam generator (6)

-steam flow signal for each steam generator (6)

-feed water flow for each steam generator (6).

The outputs are:

-water level for each steam generator (2)

-pressure of each steam generator (2)

-steam flow of each steam generator (2)

-feed water flow for each steam generator (2)

-high water level alarm for each steam generator (2)

-low water level alarm for each steam generator (2)

-high pressure alarm for each steam generator (2)

-high steam flow alarm for each steam generator (2)

-hardware failure alarm (1).

2.3.1.15 DATA VALIDATION OF THE FEED WATER SYSTEM

The inputs are:

-main condenser vacuum (3)

-main condenser temperature (3)

-discharge pressure of condensate pumps (3)

-discharge temperature of ejector condenser (3)

-discharge temperature from low-pressure heater drain pump (3)

-steam pressure at deaerating tank (3)

-temperature at discharge of deaerating tank (3)

-main feed pump discharge pressure (3)

-high pressure heater discharge temperature (3)

-status signal of main circulating pump (3)

-status signal of sea water intake valve (3)

-status signal of scoop valve (3)

-status signal of circulation water discharge valve (3)

-status signal of condensate pumps (6)

-status signal of drain pumps (6)

-status signal of the main feed pumps (6)

-status signal of the emergency feed pumps (3)

-status signal of the main feed valves (6)

-status signal of the auxiliary feed valves (6)

-position signal of main feed valves (6)

-position signal of the auxiliary feed valves (6)

-status signal of isolation valves (6)

-oil pressure signal from main feed pump 1 (3)

-oil pressure signal from main feed pump 2 (3).

The output signals are:

-main condenser vacuum (1)

-main condenser temperature (1)

condensate pumps discharge pressure (1)

-main ejector condenser discharge temperature (1)

-drain pump discharge pressure (1)

-deaerating tank level (1)

-deaerating tank discharge temperature (1)

-main feed pump's discharge temperature (1)

-high pressure heater discharge pressure (1)

-high pressure heater discharge temperature (1)

-status signal for main circulating pump (1)

-status signal for water intake valve (1)

-status signal of circulation water discharge valve (1)

-status signal of condensate pumps (2)

-status signal of drain pumps (2)

-status signal of main feed pumps (2)

-status signal of main feed valves (2)

-status signal of auxiliary feed valves (2)

-status signal of isolation valves (2)

-position signal for main feed valves (2)

-position signal for auxiliary feed valves (2)

-low deaerating tank level alarm signal (1)

-low oil pressure main feed pump 1 alarm signal (1)

-low oil pressure main feed pump 2 alarm signal (1)

-hardware failure signal (1).

2.3.1.16 DATA VALIDATION OF TURBINES

The inputs are:

-steam pressure to the seals (3)

-steam pressure to ahead nozzle of high-pressure turbine (3)

-steam pressure to low-pressure turbine (3)

-steam pressure to astern nozzle of low-pressure turbine (3)

-position signal of ahead throttle valve (3)

-position signal of astern throttle valve (3)

-status signal of guardian throttle valve (3)

-status signal of ahead throttle valve (3)

-status signal of astern throttle valve (3)

-speed signal of propeller shaft (3)

-oil pressure signal from high-pressure turbine (3)

-oil pressure signal from low-pressure turbine (3)

-lubricating oil pressure signal from lubricating system (3)

-oil temperature signal at lubricating oil tank (3).

The outputs are:

-steam pressure to turbine seals (1)

-steam pressure to high-pressure turbine nozzles (1)

-steam pressure to low pressure turbine (1)

-steam pressure to high-pressure turbine astern nozzles (1)

-position signal of ahead throttle valve (1)

-position signal of astern throttle valve (1)

-status signal to guardian throttle valve (1)

-status signal of ahead throttle valve (1)

-status signal of astern throttle valve (1)

-propeller shaft speed signal (1)

-status signal for main lubricating pump MLP 1 (1)

-status signal for MLP 2 (1)

-lubrication system oil pressure (1)

-oil pressure to high pressure turbine (HPT) (1)

-oil pressure to low pressure turbine (LPT) (1)

-oil temperature at lubrication system (1)

-oil level at lubrication tank alarm signal (1)

-low oil pressure HPT alarm signal (1)

-low oil pressure LPT alarm signal (1)

-high oil temperature oil system alarm signal (1)

-hardware failure signal (1)

2.3.1.17 VALIDATION OF HIGH PRESSURE STEAM SYSTEM

The inputs are:

-total steam flow signal (3)

-total steam pressure signal (3)

-main condenser back pressure signal (3)

-status signal of quick closing valves (6).

The output signals are:

-total steam flow signal (1)

-total steam pressure signal (1)

-main condenser back pressure signal (1)

-status signal of quick closing valves (2)

-high steam flow alarm signal (1)

-low steam flow alarm signal (1)

-high steam pressure alarm signal (1)

-low steam pressure alarm signal (1)

-high main condenser back pressure alarm signal (1)

-hardware failure signal (1)

2.3.1.18 VALIDATION OF PRIMARY PURIFICATION SYSTEM

The inputs are:

-purification flow signal (3)

-purification pressure signal (3)

-purification temperature signal (3)

-water conductivity at cooler's discharge (3)

-PH signal (3)

-differential pressure at the filters (3)

-conductivity signal at the surge tank inlet (3)

-status signals for 22 valves (66).

The outputs are:

-purification flow (1)

-purification pressure (1)

-purification temperature (1)

-conductivity at discharge of let-down coolers (1)

-PH signal (1)

-differential pressure at the filters (1)

-conducitivity at the surge tank inlet (1)

-status signal for 22 valves (22)

-high purification flow alarm signal (1)

-low purification flow alarm signal (1)

-high purification temperature alarm signal (1)

-high differential pressure at filters alarm signal (1)

-hardware failure signal (1).

2.3.1.19 DATA VALIDATION OF ELECTRICAL GENERATION SYSTEM

The inputs are:

-electric load signals from generators (12)

-voltage signals from generators (12)

-DC voltage signal (3)

-voltage signal for lighting (3)

-emergency power voltage signal (3)

-shore power voltage signal (3)

-shore power load signal (3)

-status signal for 24 breakers (72)

-status signal of AC/DC groups (12)

-status signal of DC/AC groups (12)

-status signal of emergency diesel generator (3)

-voltage signal from main bus (6)

-oil pressure at turbo generator no. 1 (3)

-oil pressure at turbo generator no. 2 (3)

-oil pressure at diesel generator no. 1 (3)

-oil pressure at diesel generator no. 2 (3)

-back pressure signal from turbo generator no. 1 (3)

-back pressure at turbo generator no. 2 (3)

-cooling water temperature at diesel generator no. 1 (3)

-cooling water temperature at diesel generator no. 2 (3)

-starting air pressure for diesel generators (3).

The outputs are:

-electric load for turbo generators nos. 1 and 2 and diesel generators nos. 1. and 2 (4)

-generator voltage (4)

-DC voltage (1)

-lighting voltage (1)

-emergency power voltage (1)

-shore power voltage (1)

-shore power load (1)

-status signal from 24 breakers (24)

-status signal of AC/DC groups (4)

-status signal of DC/AC groups (4)

-status signal of emergency diesel generator (1)

-main bus voltage (2)

-low oil pressure at turbo generators nos. 1 and 2 and diesel generators nos. 1 and 2 alarm signals (4)

-high temperature diesel generators nos. 1 and 2 alarm signal (2)

-high cooling water temperature at diesel generators nos. 1 and 2 alarm signal (2)

-low starting air alarm signal (1)

-hardware failure alarm signal (1)

2.3.1.20 DATA VALIDATION FROM PRIMARY PUMPS

The inputs are:

-primary pumps cooling flow signal (12)

-primary coolings water temperature (12)

-status signal of primary pump (12)

-electric load of primary pumps motors (12).

The outputs are:

-primary pump cavity temperature (4)

-electric load of primary pump's motors (4)

-status signal of primary pumps (4)

-abnormal load primary pump's motors alarm signal (4)

-cooling water flow to primary pumps (4)

-primary pump's cooling water temperatures (4)

-hardware failure signal (1).

2.3.1.21 DATA VALIDATION OF BUFFER SEAL'S FLOW PARAMETERS

The inputs are:

-total input flow signal (3)

-seals flows signals (63)

-total output flow signal (3).

The output signals are:

-total input flow (1)

-seals flows signals (21)

-total output flow signal (1)

-high output flow alarm signal (1)

-hardware failure alarm signal (1).

It should be noted that almost every signal given by the conventional system has been triplicated in the new design. The reason for this redundancy is to provide the validation algorithm with three independent measurements. A real implementation may not contain this level of redundancy, but the digital design has to be sized to allow that possibility.

2.3.2 ADVANCED CONTROL FUNCTIONS

The advanced control functions block requires the data previously validated as input. The outputs from this block are the following variables:

-safety state vector

-communications control signals

-polling signals for detecting hardware malfunctions.

The validated signal traffic is given by the output of the validation blocks (28). The signal traffic involved in the communication process is assumed to be one signal for each block (validation, control, and peripherals) (49). The same assumption is made with the polling signals (49).

The number of variables included in the safety state vector is a matter still under study, but an approximate number is 30 (Ref. 2.2)

2.4 SELECTION OF BASIC ALTERNATIVES

Basically four types of control systems are available:

-analog control

-supervisory control

-direct digital control

-distributed digital control.

These approaches are analyzed in detail in Ref. 2.3. The referenced paper proved that direct digital control and distributed digital control have shown a positive trend in applications, while analog or supervisory control is declining. Moreover, considering the requirements of data validation, plant surveillance, and operator advisory inputs required of the system, a designer has no choice but to discard the first two alternatives.

Narrowing down the spectrum of choices to direct digital control and distributed digital control still leaves several alternatives for further consideration. For example, direct digital control has two possible applications

1) the use of one central computer performing all functions;

2) the use of two processes working in parallel. One computer is in service connected to the plant and receiving and sending signals; the other is in warm stand-by only receiving signals from the plant. If the computer on service fails, a switch changes the plant from the output of the failed device to the output of the back-up computer (Ref. 2.6). Both alternatives are analyzed in greater detail in subsequent sections.

Distributed systems are analyzed in Ref. 2.4, where their main advantages and defects are identified. From Ref. 2.4 five distributed architectures can be used in this process. They are:

-loop architecture

-interconnection architecture

-multiprocessor architecture

-global bus architecture

-star architecture.

Even these five alternatives are too numerous to be compared in detail; a further selection procedure is needed to narrow the choices. To this end, the following definitions are used by Thurber and Masson in Reference 2.4:

-Cost modularity (CM): is the incremental cost of adding a processing element (PE). In some systems this could be free (zero cost); in others it could require that n-1 paths be added to accept the nth PE.

-Placement modularity (PM): is the degree to which the function on location of an element is restricted. In some systems, a path, switch, or PE can be easily added to improve performance. In others, for example, STAR (see Section 2.5.3), the central computer is not amenable to placement modularity. In this case, addition of another computer sharing the processing task would change the architecture to another category.

-Connection flexibility (CF): primarily important in message-switched systems. This is a measure of the alternative cost associated with adding a PE. When a processor is added, whether extra long-distance connection paths or extra local paths have to be added is one measure of the connection flexibility. This issue is similar to the modularity trade-offs associated with path-oriented systems.

-Fault tolerance (FT): is the measure of the effect of a fault in a system. In system configurations, this manifests itself in terms of how the system is reconfigured by architectural changes, performance modifications, or both. Systems with decentralized control are considered most amenable to fault-tolerant design because of their flexibility to share the same function by processors placed at different physical locations.

-Local complexity (LC): deals with a measurement of the amount and complexity of decisions necessary to route information (send a message) within a system.

-Bottleneck (B): deals with resource performance limitations created by saturation or congestion of a system facility such as a data link due to system resource demand.

-Development and application: deals with the degree of theoretical and practical development shown by the architecture. The trend in actual applications is also included in this idea. The concepts defined above will be the basis of choosing two alternatives among the five mentioned. These two will be developed in detail. To decide which alternatives to choose, a weighting factor method is used together with the quantification of each alternative's properties.

2.4.1 THE WEIGHTING FACTORS METHOD

This method is based on quantifying a set of properties for each alternative. After quantification, the desirability of each property is assigned a weighting factor. The desirability is given by the operational requirements asked of the design. This part of of the decision process is under designer control because he has to quantify the weighting factors by considering the importance of each property in relation with operational requirements.

The process starts when the quality of the properties (definitions) themselves are quantified, that is, the analysis of each architecture in relation to the applicability of every property. This process is explained in Ref. 2.4; here the given qualities are translated by the following scale:

extremely good	9.0
very good	8.0
good	7.0
moderate	5.0
bad, poor	3.0
very bad	1.0

The weighting factors have to reflect the importance of each property in light of the operational requirements. For example, fault tolerance is considered to be the most important and receives a weighting factor of 10. On the other hand, bottleneck and local complexity are the least important and they receive a 1.0. The list of weighting factors is:

Fault Tolerance (FT)	10.0
Cost Modularity (CM)	8.0
Connection Flexibility (CF)	8.0

Development and Application (DA)	8.0
Placement Modularity (PM)	5.0
Local Complexity (LC)	1.0
Bottleneck (B)	1.0

The figure of merit is reached by multiplying each property by the weighting factor and making the summation of these products for every alternative. The final results are shown in Table 2.1.

TABLE 2.1

WEIGHTING FACTOR METHOD

(Ref. 2.4)		Properties						Figure of
Architectures	CM	DM	CF	FT	LC	B	DA	of Merit
Loop	9	9	1	3	9	1	7	221
Interconnection	1	9	1	8	9	8	7	214
Multiprocessor	5	9	1	5	1	1	8	209
Global bus	8	8	1	8	8	3	9	275
Star	8	8	1	3	5	3	9	222
Weighting factor	8	5	8	10	1	1	8	

From Table 2.1, the two best architectures are Global bus and Star. Therefore, these, together with the central computer ones, will be used in the next stage of the design process.

2.4.2 DESCRIPTION OF THE SELECTED ARCHITECTURES

2.4.2.1 CENTRAL COMPUTER

The central computer architecture concentrates all the processing intelligence and the communications control in one processor. The processor receives all the data, processes them, and sends the information to the connected elements. Devices connected with the central computer include man-machine interfaces (MMI), plant actuators, or data storing devices. Every signal produced by the plant sensors is wired individually to the interfaces placed in the central computer. The computer/plant interface is usually a I/O hardware device designed to translate real time signals coming from the plant into digital language intelligible to the computer. The process is also performed in the opposite way. Figure 2.4.1 shows a scheme of this architecture.

A typical option in this kind of architecture is to add another computer with its own MMI and I/O interfaces, working in parallel no stand-by. This feature is one way of improving the fault tolerance of the architecture. Figure 2.4.2 presents a scheme of such architecture.

2.4.2.2 GLOBAL BUS ARCHITECTURE

This global bus configuration is show in Figure 2.4.3. As seen on the figure, the processing intelligence is now distributed along several microprocessors located close to the loop they are controlling or watching. A central computer is also needed to coordinate the actions of the distributed microprocessors and to perform general tasks not performed by the dedicated microprocessors. A distinctive feature of this distributed process is the common communication bus used by all the processors. Any processor can communicate with another by means of the

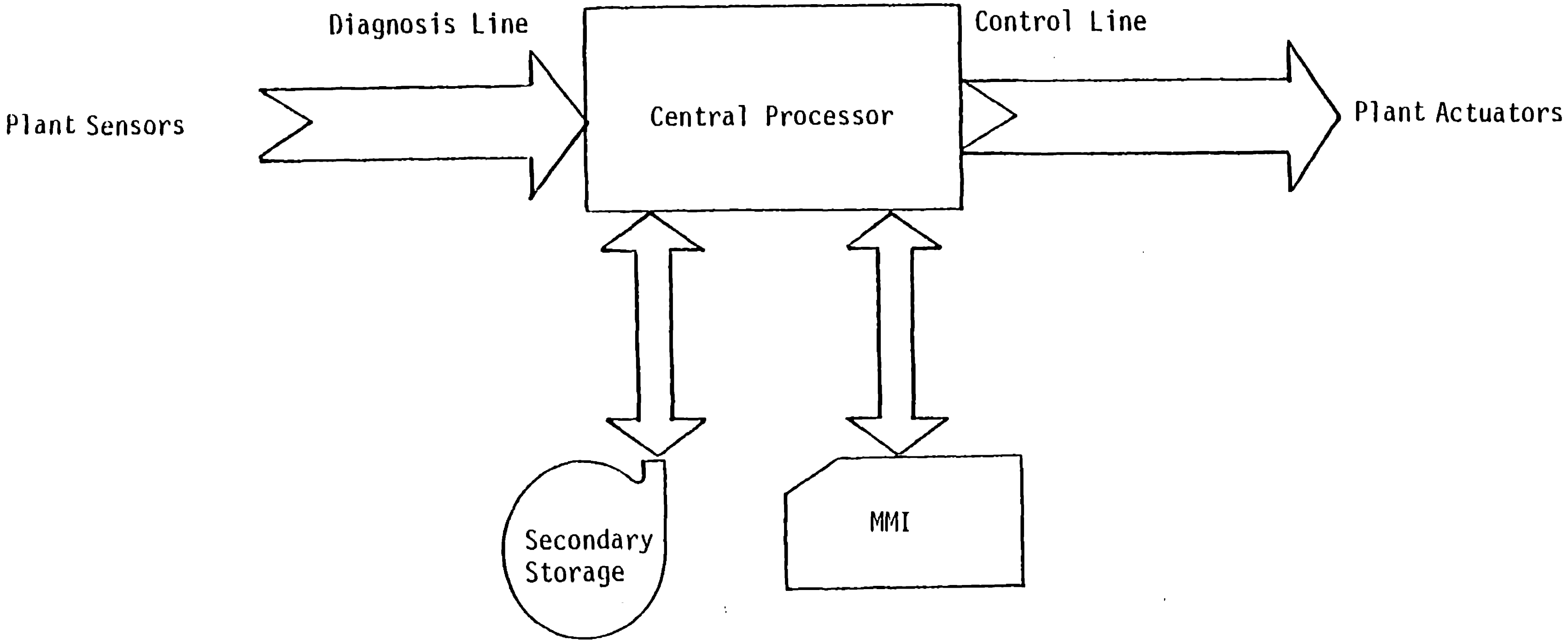


Figure 2.4.1 Central processor architecture, block diagram.

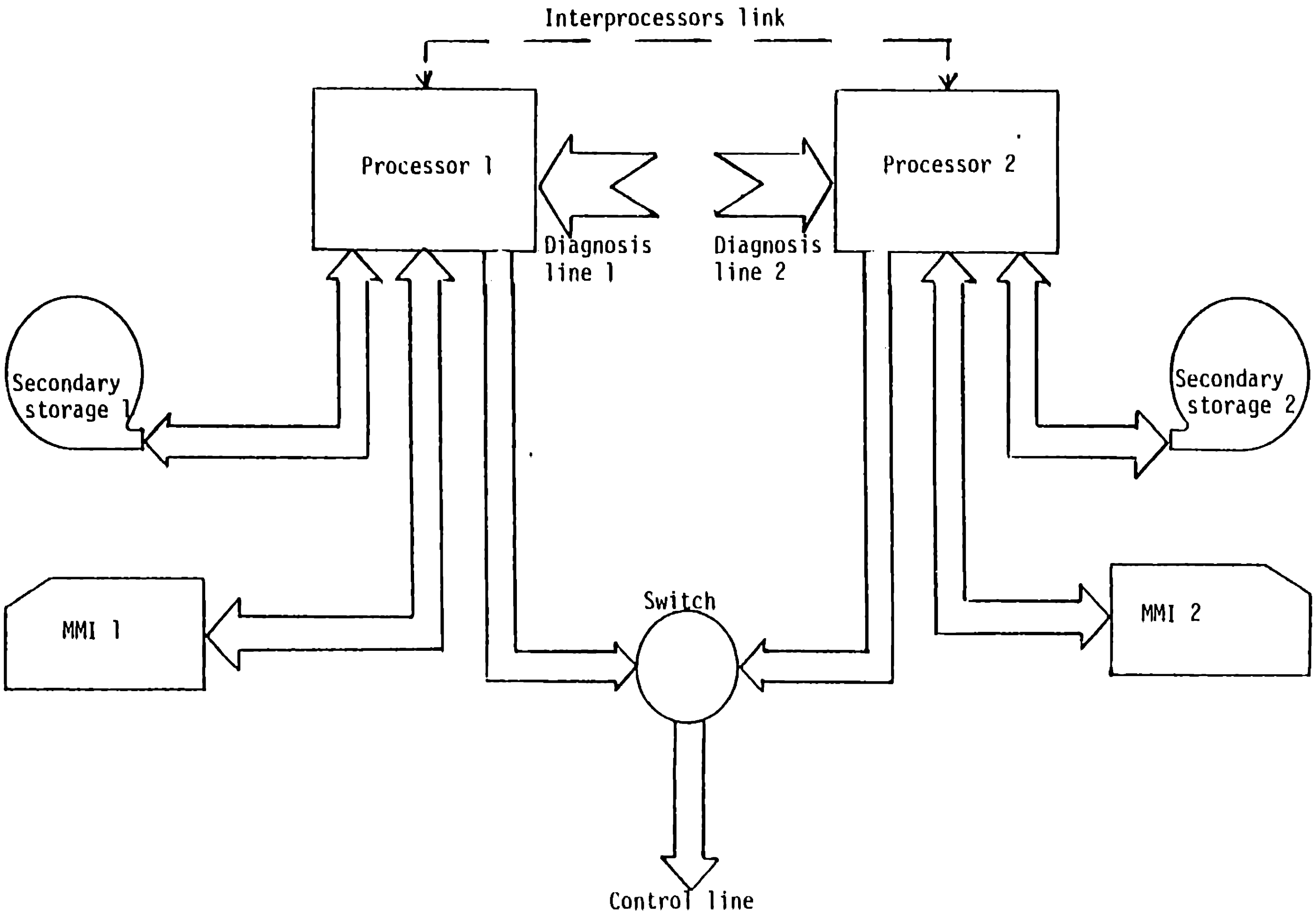


Figure 2.4.2 Dual central computer architecture, block diagram.

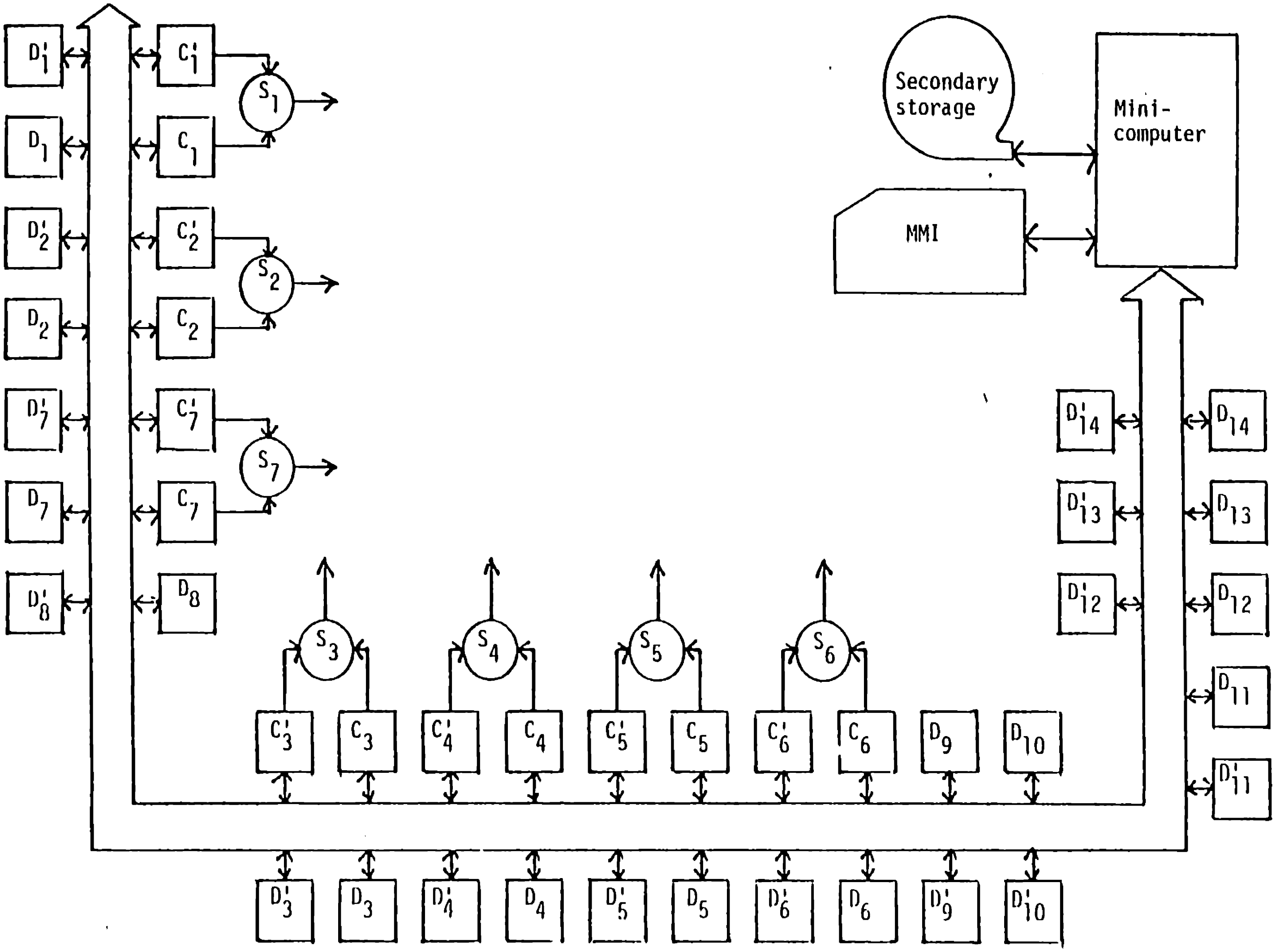


Figure 2.4.3 Global data bus architecture, block diagram.

common bus. The global bus architecture uses a direct transfer strategy; thus there is no switch device acting as a bridge routing the data through it. The communication path is shared, and access to the bus is regulated by the central computer. The communications through the bus are typically made in a serial protocol. The bus can be duplicated to improve the fault tolerance or to achieve higher data traffic.

On the microprocessor side, they are duplicated to improved fault tolerance, control microprocessors have a switch to change the control load from the microprocessor on service to the hot stand-by unit, if the former fails. The latter feature is taken from the dual central computer architecture.

The global bus architecture also has a dual option, shown in Figure 2.4.4. This architecture is the result of adding a complete central computer plus a new bus to the single global bus. Switching from one computer to another is implemented by software.

2.4.2.3 STAR ARCHITECTURE

Star architecture also has the processing power distributed along the plant. This architecture uses an indirect transfer strategy (data crosses through an intelligent processor). The information is routed by the central computer and the communication path is dedicated for each microprocessor (Figure 2.4.5). A distinct feature of this architecture. is that validation microprocessors communicate directly with control microprocessors and with the central computer. The communications protocol can be serial or parallel depending on the required volume and

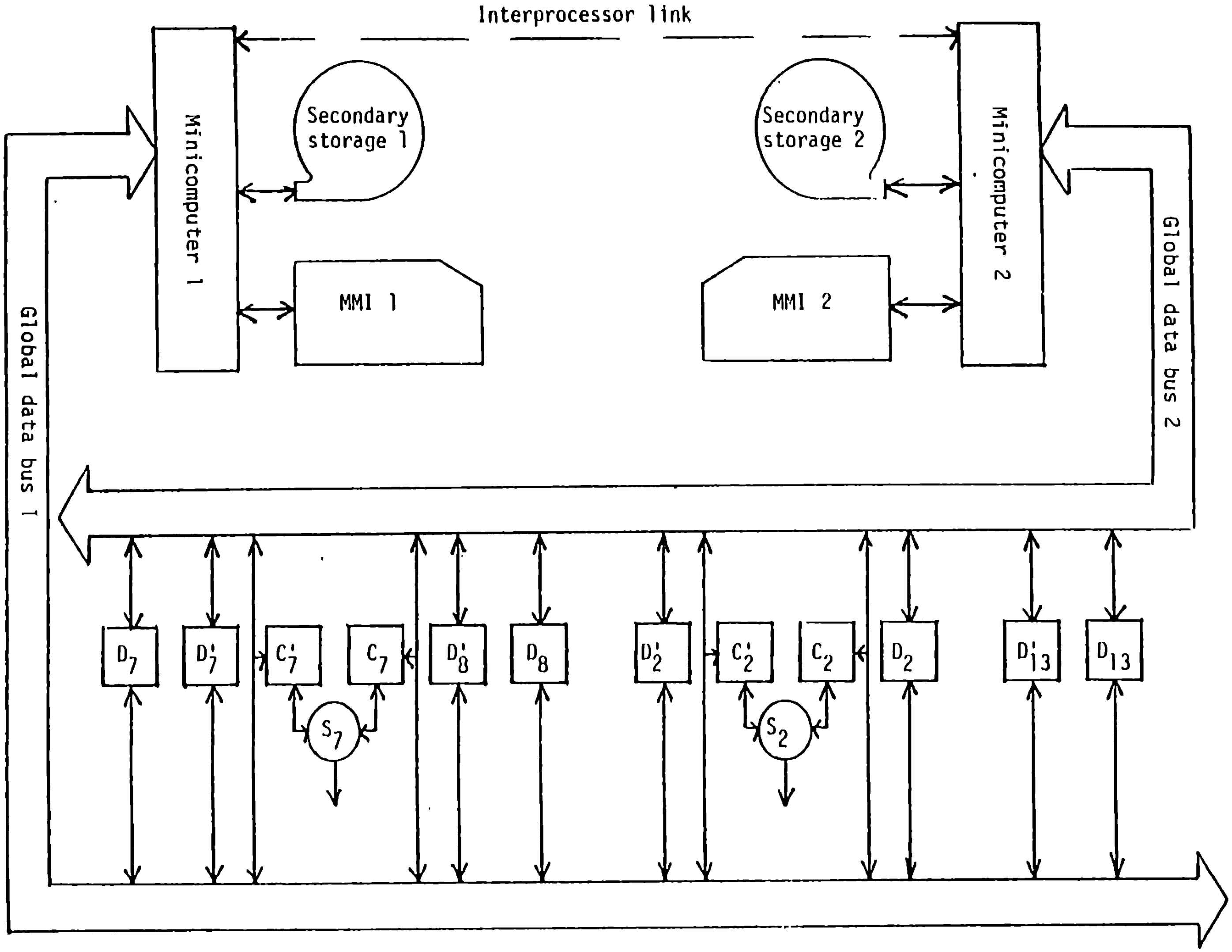


Figure 2.4.4 Dual global data bus architecture, partial block diagram.

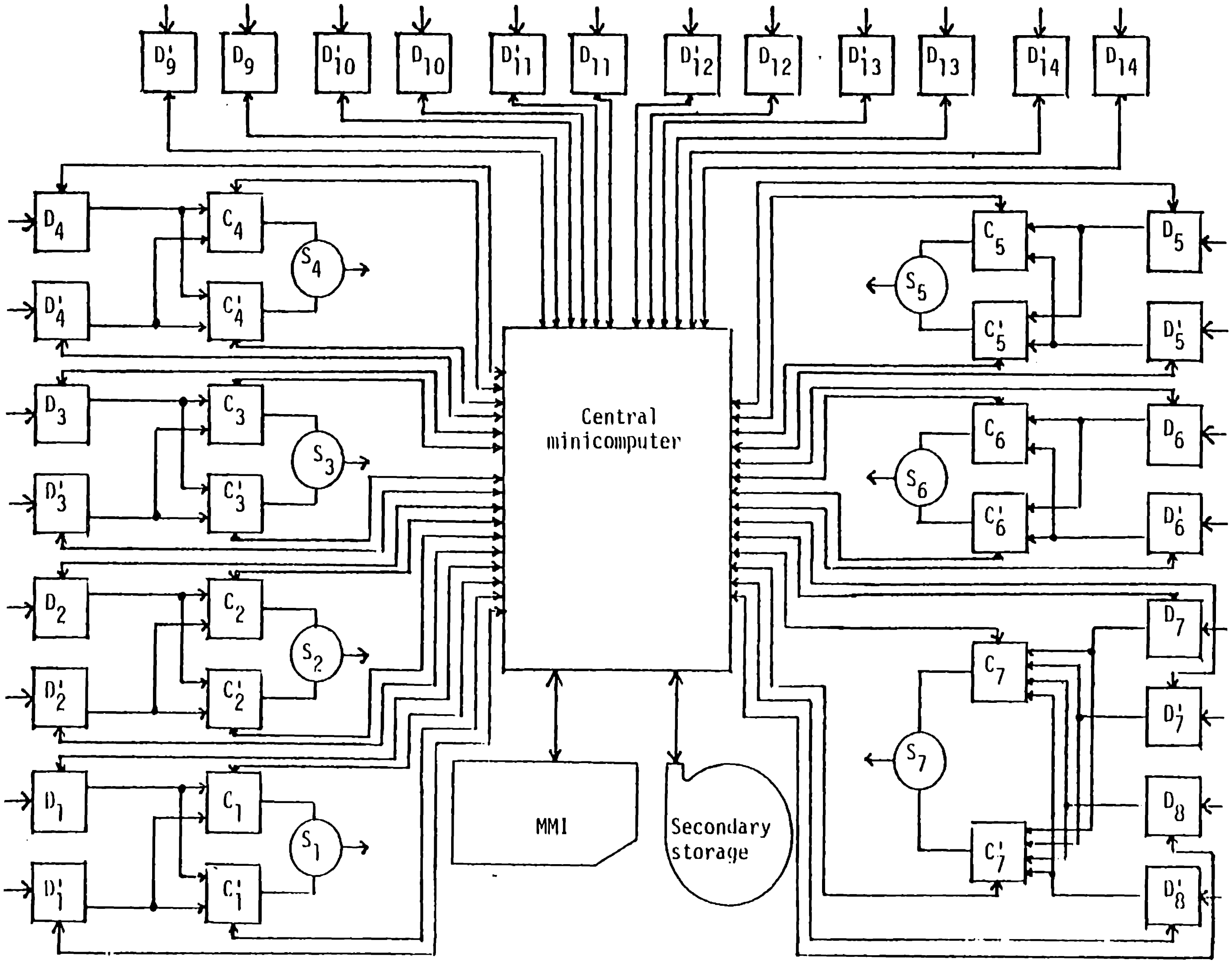


Figure 2.4.5 Star architecture, block diagram.

speed of the information.

Also the Star architecture has dual options consisting of adding a complete central computer as a hot standby and connecting it to every microprocessor. When dual Star architecture is considered, the communication protocol chosen defines a change in the hardware Figure 2.4.6) shows a dual Star architecture using parallel communications. This specific option requires a hardware switch to change from one computer to the other. On the other hand, a dual Star architecture using serial communications (Figure 2.4.7) does not require the switch.

2.5 IMPLEMENTATION OF THE ALTERNATIVES

The standard procedure to choose appropriate hardware is to examine the whole computer market and make the selection on purely technical grounds. This procedure proves to be difficult to perform because most vendors are not unwilling to supply confidential reliability data about their products. In addition, choosing one vendor for all the devices assumes component compatibility and simplifies the problem. Therefore it was decided to use one component manufacturer as the component supplier for the purpose of this design study. This decision by no means implies that only one supplier would be used in the case of an actual implementation; the purpose of this work is to find the best architecture and not to make a final installation. The actual devices used for doing that is a matter for further study. Moreover, in order to protect the propietary reference condition of the data supplied by the manufacturer, only generic names will be related with the

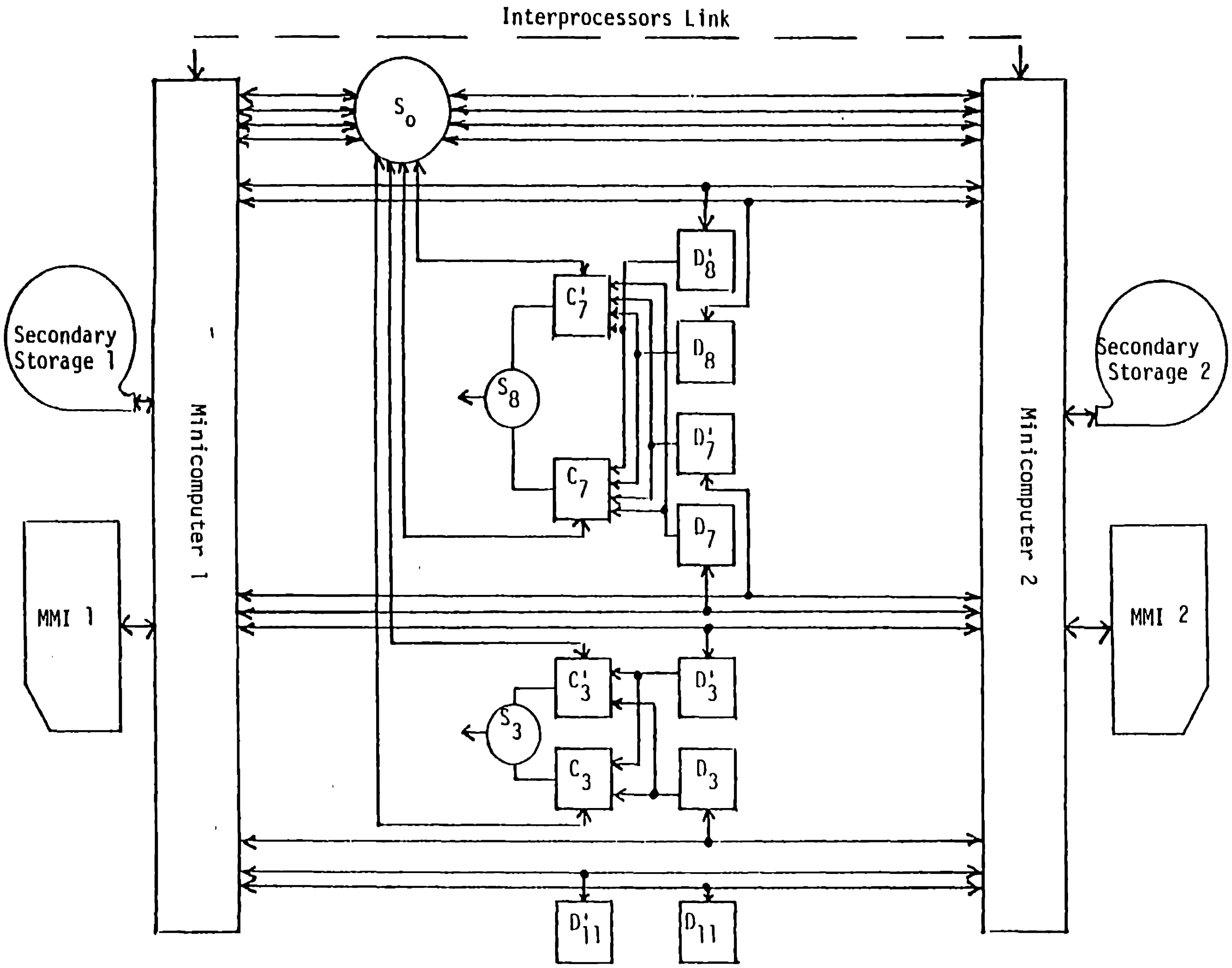


Figure 2.4.6 Dual star architecture, parallel transmission (partial design).

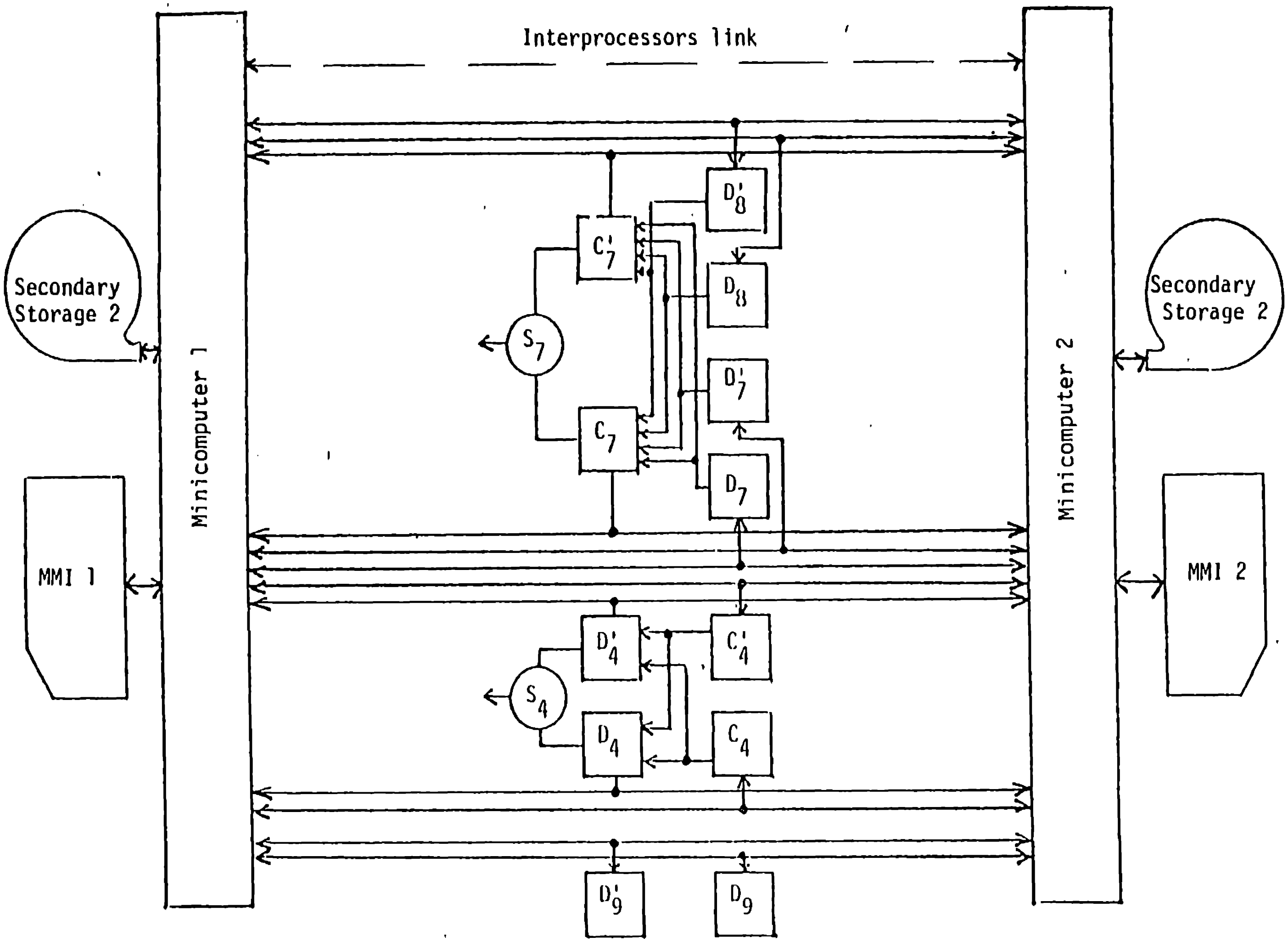


Figure 2.4.7 Dual star architecture, serial transmission, partial block diagram.

reliability data.

The procedure followed in choosing the proper components is first, to calculate the memory capacity and data rate requirements, and with that information, to choose the appropriate devices. Finally, the configuration sheets are filled out for every architecture.

To estimate the memory capacity requirements is particularly troublesome, since the actual software has not yet been developed. Therefore, in order to estimate the memory required, a general theory developed by Maurice H. Halstead (Ref. B.1) is used. This is a general theory, and the actual application could differ from the outcome given by the theory, but nevertheless it is the best tool available to quantify the size of a software not yet developed. The reader is referred to Appendix B to see how the theory is applied to our particular case.

The following subsections analyze particular architectures.

2.5.1 CENTRAL COMPUTER ARCHITECTURE

The design of this architecture is based on the experiece acquired by using central computers in process control (Reference 2.5). The actual design has the reductions appropriated for the size and lower complexity of the N.S. Savannah nuclear plant.

Peripheral devices are:

1 disk system (non-volatile memory)

1 tape system (back-up memory)

3 consoles (CRT plus keyboards)

1 line printer

1 card reader.

To calculate the total amount of memory required, it will be assumed that it is equal to the summation of all individual memory requirements. From Table B.2 this amount is 1482.54 (kby). Also only the advanced control algorithm needs to store data in non-volatile systems. From past experience it has been noted that only 15 percent of total memory is held in solid state memories, the remaining goes on disks. From the above considerations, the SDCS algorithm requirement is approximately 175 kby. plus 317 kby. for control and validation, or 492 kby total solid state memory and approximately 989 kby in volatile systems. (The values are rounded.)

A system from DEC which meets the above requirements is a PDP 11/70 system. With this model and using an updating time of 2 seconds, each signal will share an average of 735 instructions. Figure 2.5.1 shows the details of the design and calculations appear in the corresponding design sheet in Appendix C.

2.5.2 DUAL CENTRAL COMPUTER ARCHITECTURE

This kind of architecture is intended to improve the fault tolerance of central computer architecture. The back-up computer is designed exactly in the same way as the single central computer. The architecture is based on a reliable switch system, which selects the outputs coming from both computers. The selection process is a combination of the switch hardware and a special software implemented in

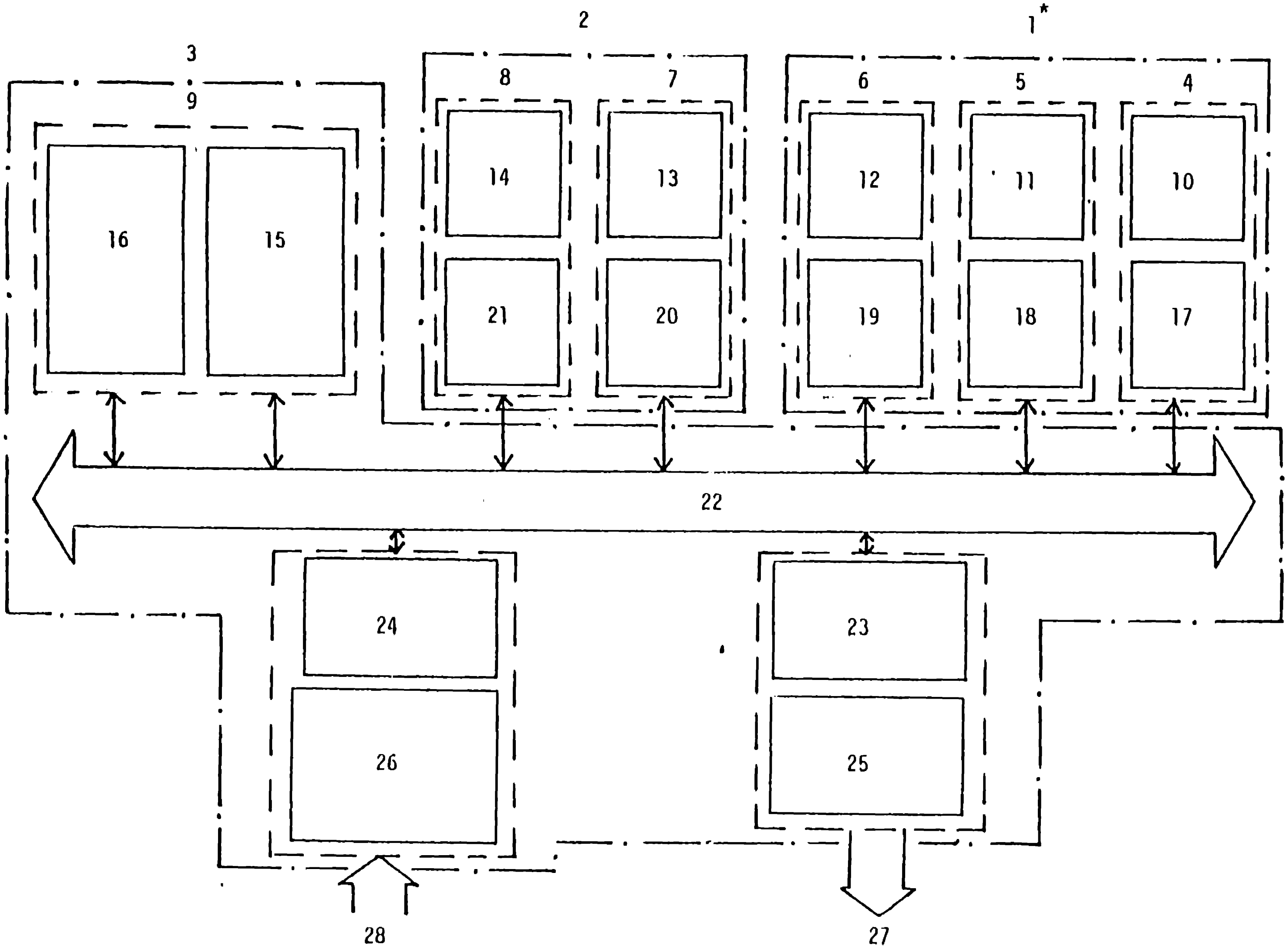


Figure 2.5.1 Central computer architecture, detailed design.
*See legend on next page.

1. MMI
2. Secondary storage
3. Processor
4. VS11-AP (3)(monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-NA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/70 NK (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA magnetic tape drive
14. RL01-AK disk drive
15. MK11-CA (1) memory
16. PDP 11/70 (1) CPU
17. VS11-AA
    VRV02
18. Documation M200 controller
19. LP11 controller
20. TS03 master
21. RL11 controller
22. Unibus
23. LPA11-K (9)
    A/D controller
24. LPA11-K (27)
    D/A controller
25. AD11-K (18) (A/D interface)
    AM11-K (18) (multiplier)
26. AA11-K (27) (D/A interface)
27. Control line
28. Diagnosis line

both processors. An inter-computer link is provided to facilitate the decision process.

The dual computer feature is widely used in control applications, especially in nuclear power plants (References 2.5, 2.6). The switch has been designed to be one for each analog output (after the D/A devices). The switches are simply analog multipliers whose driving signal comes from the computers in service. With this design, a partial failure will make shift only the switches involved in that failure, thus both computers will be working on-line, sharing the processing task. Although this situation could happen with some frequency, the current assumption will be to consider a total shift when a failure occurs.

The final architecture is shown in Figure 2.5.2; the design sheets appear in Appendix C.

2.5.3 STAR ARCHITECTURE

As explained previously, Star architecture is a distributed architecture. The basic control functions and the data validation processes are distributed in dedicated microprocessors installed near the plant. The advanced control function remains in a central minicomputer installed in the control room. This minicomputer requires less memory than the previous control computers because of its process-sharing feature.

To improve the fault tolerance of the architecture, the dedicated microprocessors are designed to be redundant. Control microprocessors follow the same pattern of dual central computers by using a switch to

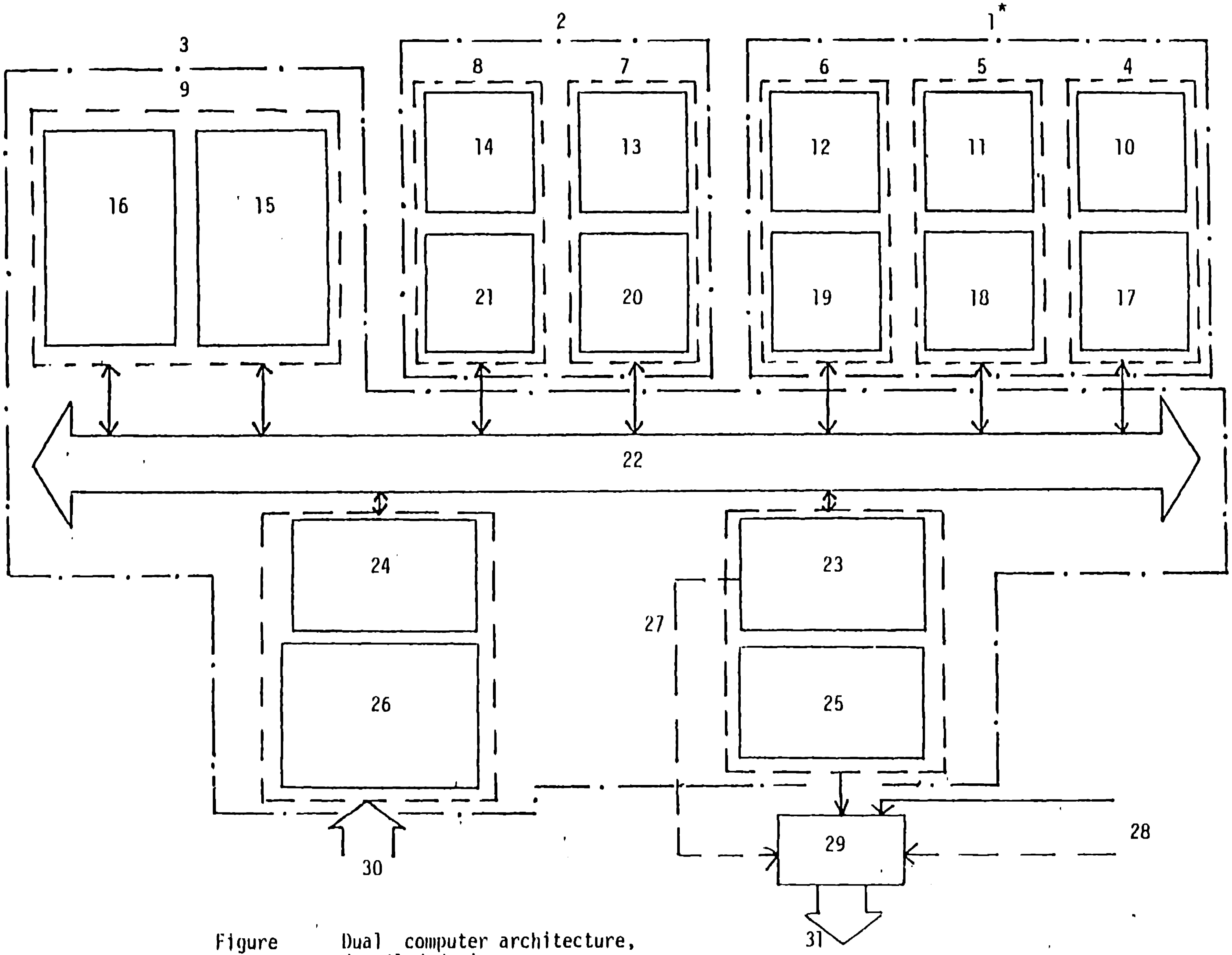


Figure 2.5.2 Dual computer architecture, detailed design.
*See legend on next page.

1. MMI 1
2. Secondary storage 1
3. Processor 1
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/70 NK (memory and CPU)
10. 19" color monitor
11. CR04-A
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MK11-CA (1) memory
16. PDP 11/70 (1) CPU
17. VS11-AA, VRV02-BA
18. Controller documation M200
19. LP11 controller
20. TS03 master
21. RL11 controller
22. UNIBUS
23. LPA11-K (27) (D/A controller)
24. LPA11-K (9) (A/D controller)
25. AA11-K (27) D/A (interface)
26. AD11-K (18) A/D (interface)
    AM11-K (18) multiplexer
27. Switch control signal
28. Signals from processor 2
29. MPC8S
30. Diagnosis line
31. Control line

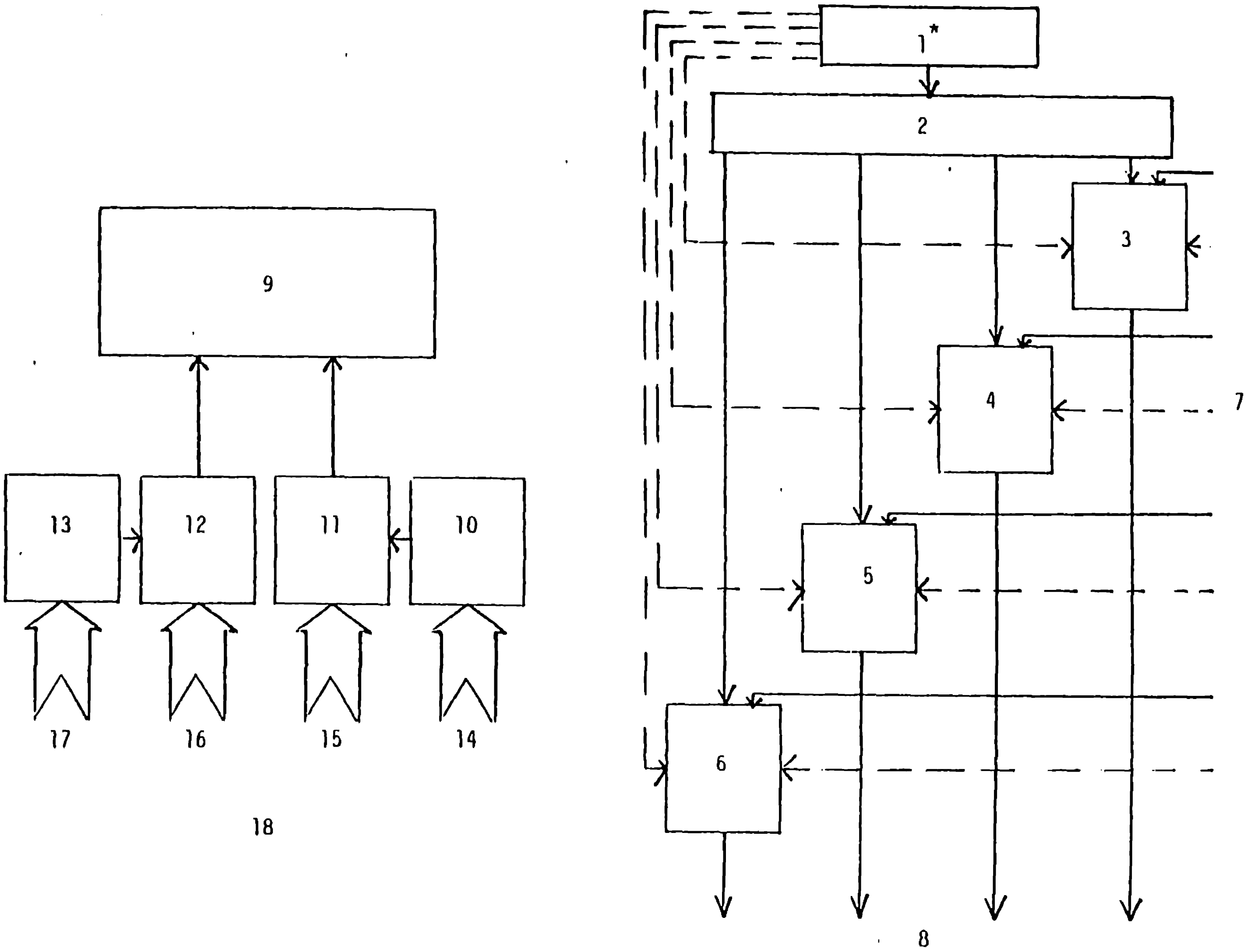


Figure 2.5.2 (continued) Details on D/A and A/D interfaces.
*See legend on next page.

1. LPA11-K (A/D controller)
2. AA11-K (D/A interface)
3. MPC8S (Motorola analog multiplexer)
4. MPC8S
5. MPC8S
6. MPC8S
7. Signals from the other processor
8. Central lines (4)
9. LPA11-K
10. AM11-K (multiflexer
11. AD11-K (A/D interface)
12. AD11-K
13. AM11-K
14. 48 lines
15. 16 lines
16. 16 lines
17. 48 lines
18. Diagnosis line

shift the duty.

The validation microprocessors send their outputs to the respective control microprocessors and to the central minicomputer. The control microprocessors are also connected to the central minicomputer.

The central minicomputer has the same peripherals as the central computer architecture because requirements are independent of the chosen architecture.

The memory requirements for the minicomputer given in Table B.2 are exactly equal to the memory requirements for the advance control (AC) algorithm. The division between volatile and non-voltaile memory follows the same policy as central computers (15 percent for solid state memory). Thus

volatile memory = 175 kby

non-voltaile memory = 989 kby

total memory = 1164 kby.

A PDP 11/60 system is the best equipment choice for these requirements.

From Table B.2 it is clear that every algorithm requires different amounts of memory and possibly different kinds of processors.

In order to achieve a standardization the microprocessors will be divided in two groups, the control microprocessors and the validation microprocessors. The former will be implemented by using LSI-11/02 CPU, and the latter by using LSI-11/23 CPU. Furthermore, the microprocessors are implemented with full memory capacity.

Control microprocessor	16 kby
diagnostic microprocessor	64 kby.

It should be noted that microprocessor C3 (Table B.1) is slightly over the maximum capacity. The above standardization will not be done in practice, because in the case of an actual implementation only the real amount of memory required is installed. This approximation facilitates further calculations but introduces a factor against the distributed architectures by raising the total cost and the probability of failure. The effects of the approximations and assumptions will be discussed in the section dedicated to sensitivity analysis.

It should be noted that the choice of LSI-11 technology implies 16 bit word format. This means more powerful instructions and lower processing time.

Two alternatives of communications can be designed for a Star architecture, parallel communications, and serial communications. Each choice means different interfacing devices, but the essential elements remain the same. Figure 2.5.3 shows the detailed design for the parallel communications alternative and Figure 2.5.4 shows the serial one. Appendix C has the work sheets for both alternatives.

2.5.4 DUAL STAR ARCHITECTURE

In the Dual Star architecture, a complete minicomputer plus its peripherals is added to the single Star design in order to improve the fault tolerance of the architecture.

Unlike the actual computer architecture where the outputs to plants are switched, in the Dual Star architecture the control microprocessors are switched. This switch can be made by a hardware switch as in the

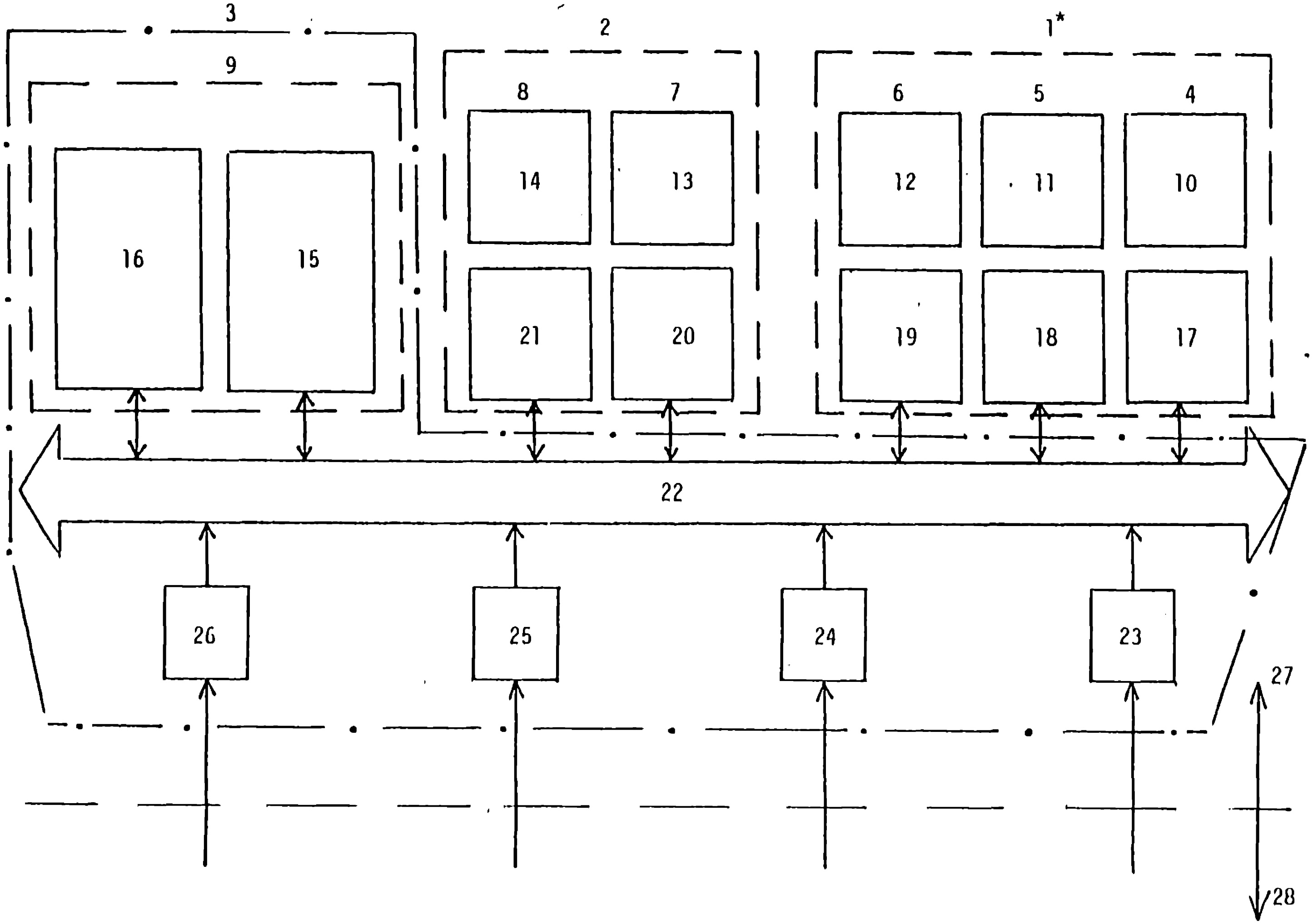


Figure 2.5.3 Star architecture, parallel transmission, detailed design.
*See legend on next page.

1. MMI
2. Secondary storage
3. Processor
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/60 EA (1) (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MS11-KE (3) memories
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Controller documation M200
19. LP11 controller
20. TS03 master
21. RL11 controller
22. UNIBUS
23. DR11-B, M7230 (parallel interface)
24. DR11-B, M7230
25. DR11-B, M7230
26. DR11-B, M7230
27. Control room
28. Machinery room

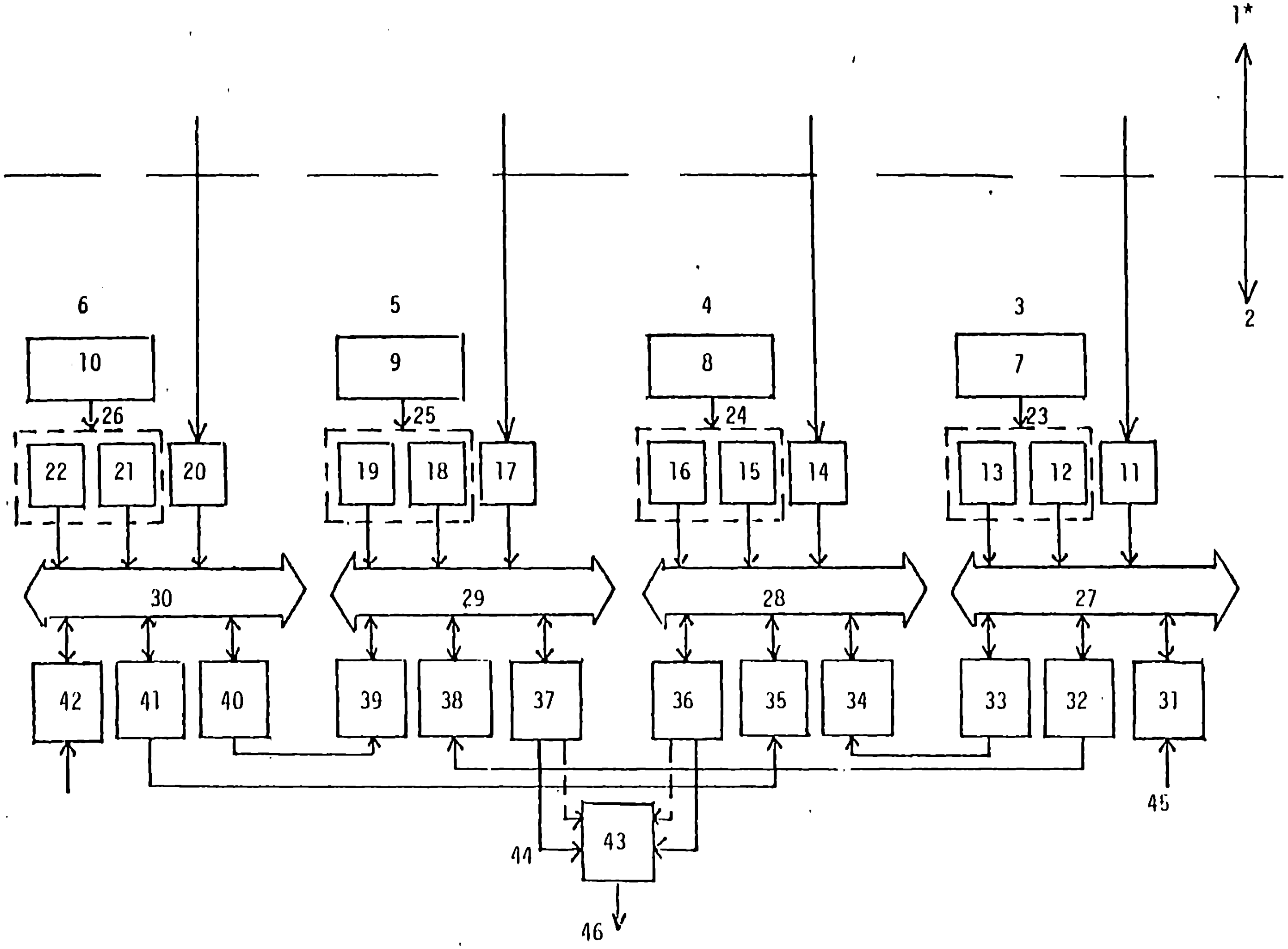


Figure 2.5.3 (continued)
*See legend on next page.

1. Control room
2. Machinery room
3. μPD' (stand-by diagnosis microprocessor)
4. μPC' (stand-by control microprocessor)
5. μPC (control microprocessor on service)
6. μPD (diagnosis microprocessor on service)
7. H9270 (2) (power supply)
8. H9270 (3)
9. H9270 (3)
10. H9270 (2)
11. DRV11-B, M5927 (parallel interface)
12. MSV11-DD (memory)
13. KDF11-AC (CPU)
14. DRV11-B, M5927
15. MSV11-DB (memory)
16. KD11-HA (CPU)
17. DRV11-B, M5927
18. MSV11-DB
19. KD11-HA
20. DRV11-B, M5927
21. MSV11-DD
22. KDF11-AC
23. KDF11-HD (CPU and memory)
24. KD11-HB (CPU and memory)
25. KD11-HB
26. KDF11-HD
27. Q-BUS
28. Q-BUS
29. Q-BUS
30. Q-BUS
31. ADV11-A (5) (A/D interface)
32. DRV11-B (parallel interface)
33. DRV11-B
34. DRV11-B
35. DRV11-B
36. AAV11-A (4) (D/A interface)
37. AAV11-A (4)
38. DRV11-B
39. DRV11-B
40. DRV11-B
41. DRV11-B
42. ADV11-A (5)
43. MPC8S (Motorola analog multiplexer)
44. Switch
45. Sensors
46. Actuators

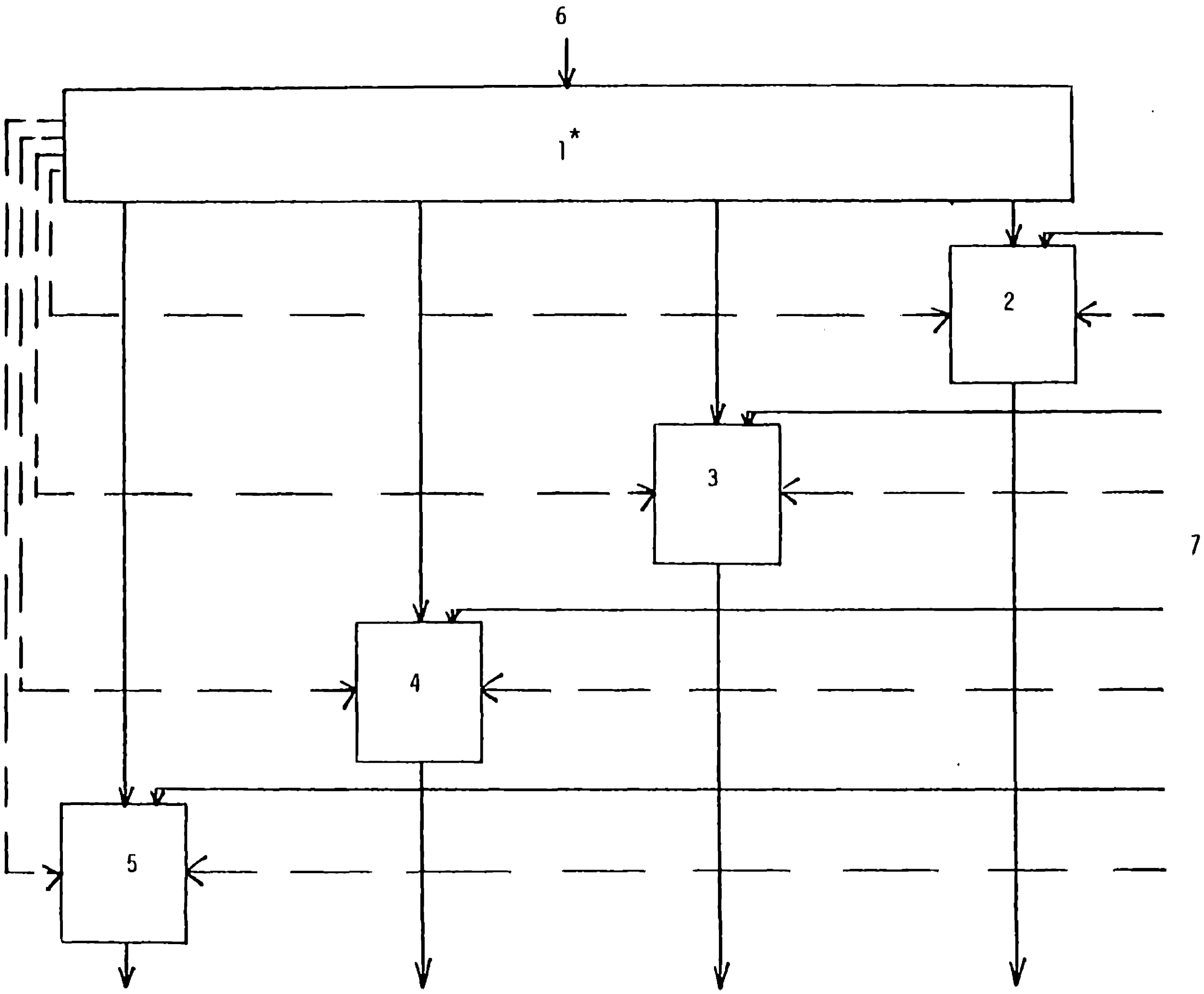


Figure 2.5.3 (continued) Detailed design of D/A interface.
*See legend on next page.

1. AAV11-A (D/A interface)
2. MPC8S (Motorola analog multiplexer)
3. MPC8S
4. MPC8S
5. MPC8S
6. From μPC
7. From μPC'

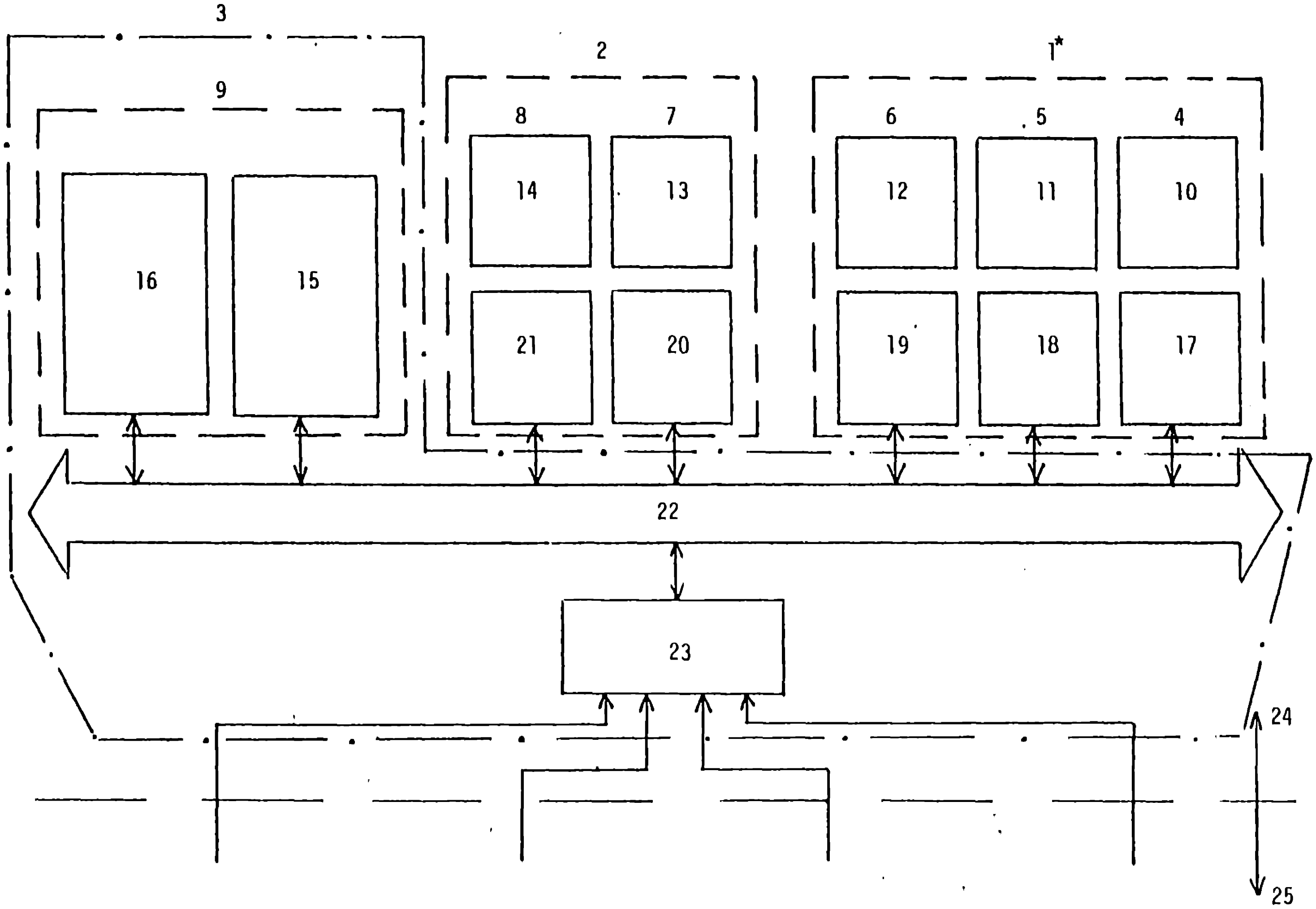


Figure 2.5.4 Star architecture, serial transmission alternative, detailed design.
*See legend on next page.

1. MMI
2. Secondary storage
3. Processor
4. VS11-AP (3) (monitor and keyboard system)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/60 EA (1) (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MS11-KE (3) memory
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Controller documation M-200
19. LP11 controller
20. TS03 master
21. RL11 controller
22. UNIBUS
23. DZ11-C (6) (serial interface)
24. Control room
25. Machinery room

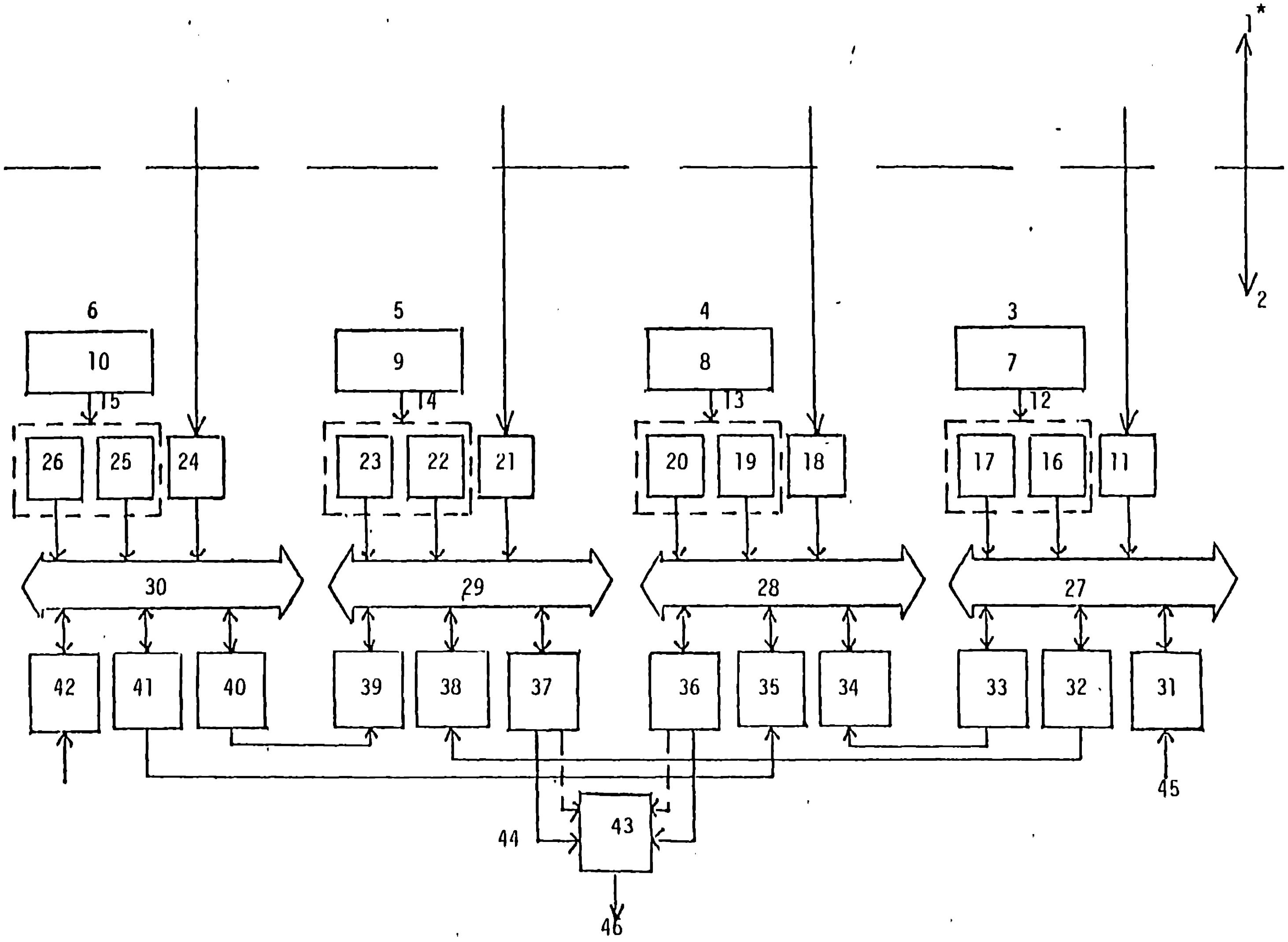


Figure 2.5.4 (continued).
*See legend on next page.

1. Control room
2. Machinery room
3. μPD' (stand-by diagnosis microprocessor)
4. μPC' (stand-by control microprocessor)
5. μPC (control microprocessor on service)
6. μPD (diagnosis microprocessor on service)
7. H9270 (2) (power supply)
8. H9270 (3)
9. H9270 (3)
10. H9270 (2)
11. DLV-11 (serial interface)
12. KDF11-HD (CPU and memory)
13. KD11-HB (CPU and memory)
14. KD11-HB
15. KDF11-HD
16. MSV11-DD (memory)
17. KDF11-AC (CPU)
18. DLV-11
19. MSV11-DB (memory)
20. KD11-HA (CPU)
21. DLV-11
22. MSV11-DB
23. KD11-HA
24. DLV-11
25. MSV11-DD
26. KDF11-AC
27. Q-BUS
28. Q-BUS
29. Q-BUS
30. Q-BUS
31. ADV11-A (5) (A/D interface)
32. DRV11-B (parallel interface)
33. DRV11-B
34. DRV11-B
35. DRV11-B
36. AAV11-A (4) (D/A interface)
37. AAV11-A (4)
38. DRV11-B
39. DRV11-B
40. DRV11-B
41. DRV11-B
42. ADV11-A (5)
43. MPC8S (Motorola analog multiplexer)
44. Switch
45. Sensor
46. Actuators

case of the parallel transmission alternative, or a pure software switch as in the case of the serial transmission alternative.

The validation microprocessors are connected directly with both minicomputers, without any need for switches. All the dedicated microprocessors are redundant, as was the case in the single architecture. Figure 2.5.5 shows the design for the Dual Star parallel transmission alternative. Figure 2.5.6 shows the design for the Dual Star serial transmission alternative. The worksheets for both are in the Appendix C.

2.5.5 GLOBAL BUS ARCHITECTURE

The global bus architecture differs from Star architecture in the communications process. The Star architecture has a dedicated link with each one of the distributed microprocessors. The global bus architecture has only one link shared by every microprocessor in the design. Apart from that, the basic design is the same: the same minicomputer, the same peripherals, the same microprocessors. Only the interfacing elements are different.

This architecture does not require a special link to communicate validation microprocessors with the control microprocessors. The communication is achieved by the common bus. Typically this architecture uses serial communications and the talking through the bus is regulated by the central minicomputer. The detailed design of the architecture is shown in Figure 2.5.7. The worksheets are in Appendix C.

2.5.6 DUAL GLOBAL BUS ARCHITECTURE

Following the same pattern of other dual designs, the dual global

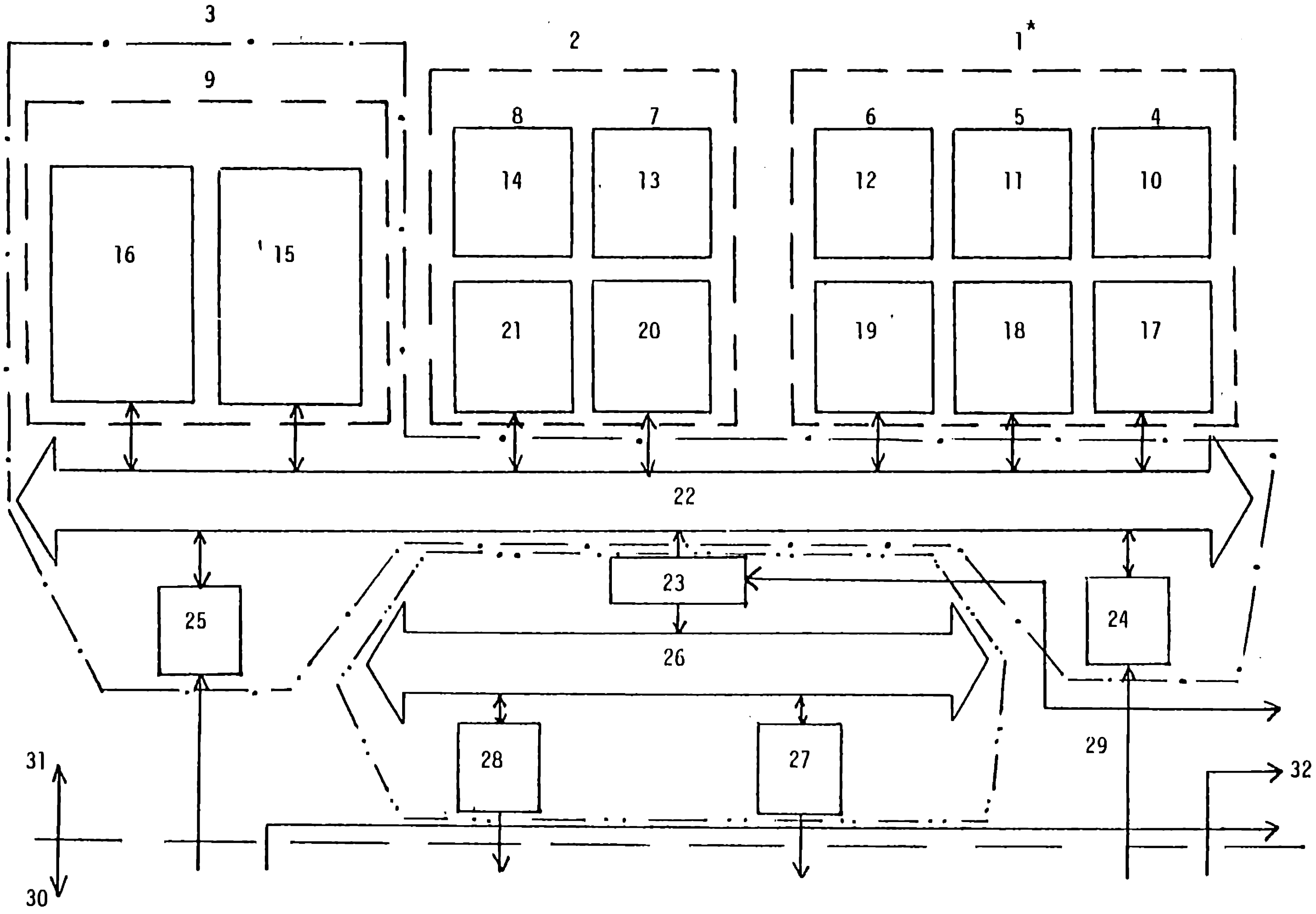


Figure 2.5.5 Dual star architecture, parallel transmission, detailed design.
*See legend on next page.

1. Control room
2. Machinery room
3. μPD' (stand-by diagnosis microprocessor)
4. μPC' (standpby control microprocessor)
5. μPC (control microprocessor on service)
6. μPD (diagnosis microprocessor on service)
7. H9270 (2) (power supply)
8. H9270 (2)
9. H9270 (2)
10. H9270 (3)
11. DRV11-B, M5927 (parallel interface)
12. DRV11-B , M5927
13. KDF11-HD
14. MSV11-DD (memory)
15. KDF11-AC (CPU)
16. DRV11-B, M5927
17. MSV11-DB (memory)
18. KD11-HB (CPU and memory)
19. KD11-HA (CPU)
20. DRV11-B, M5927
21. KD11-HB
22. MSV11-DB
23. KD11-HA (CPU)
24. DRV11-B, M5927
25. DRV11-B, M5927
26. KDF11-HD
27. MSV11-DD
28. KDF11-AC
29. Q-BUS
30. Q-BUS
31. Q-BUS
32. Q-BUS
33. ADV11-A (5) (A/D interface)
34. DRV11-B (parallel interface)
35. DRV11-B
36. DRV11-B
37. DRV11-B
38. AAV11-A (4) (D/A interface)
39. AAV11-A (4)
40. DRV11-B
41. DRV11-B
42. DRV11-B
43. DRV11-B
44. ADV11-A (5)
45. MPC8S (Motorola analog multiplexer)
46. Switch
47. Sensors
48. Actuators

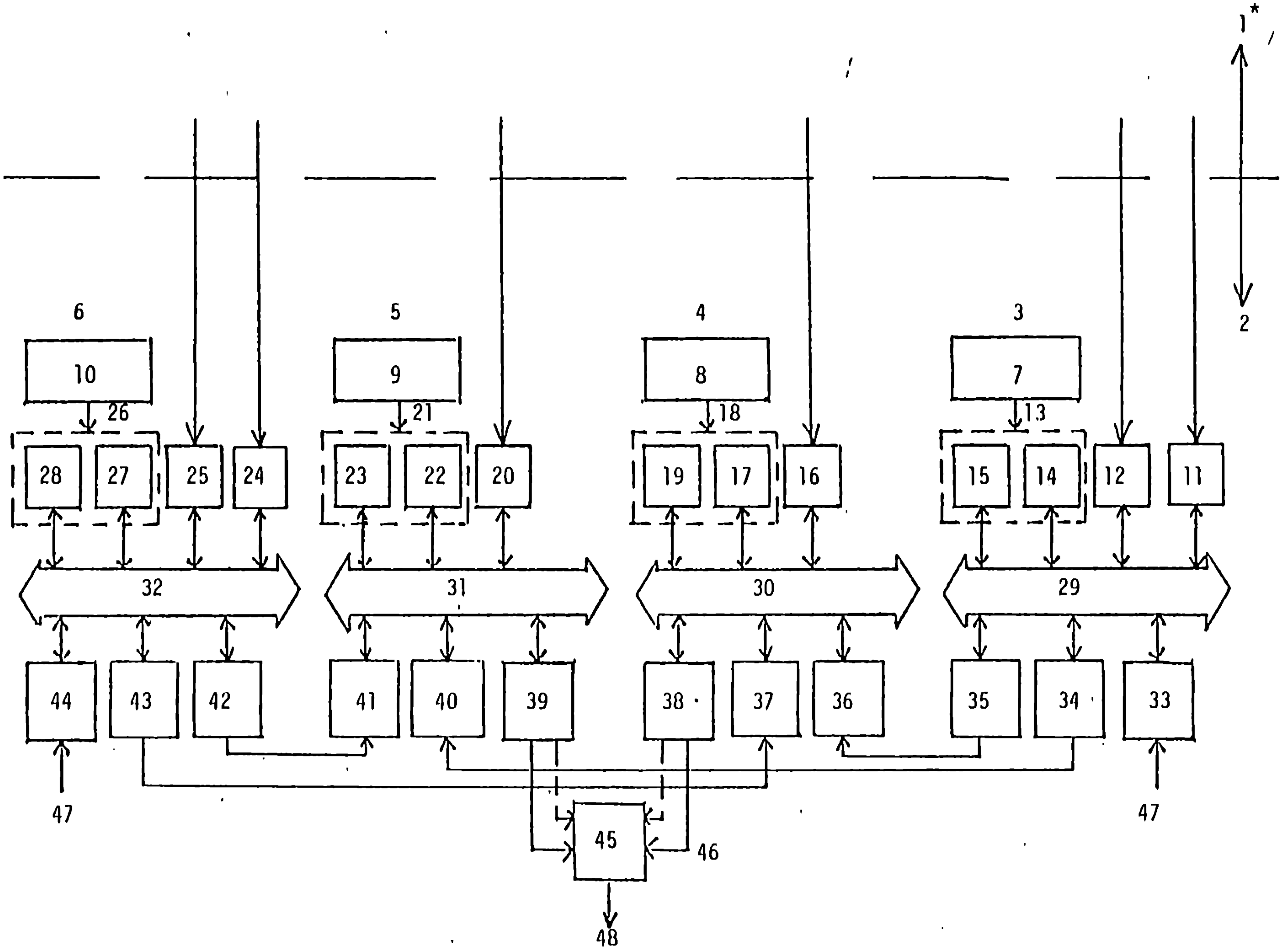


Figure 2.5.5 (continued).
*See legend on next page.

1. MMI
2. Secondary Storage
3. Processor
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/60 EA (1) (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MS11-KE memory
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Controller documation M200
19. LP11 controller
20. TS03 master
21. RL-11 controller
22. UNIBUS 1
23. DT07 (switch)
24. DR11-B, M7230 (parallel interface)
25. DR11-B, M7230
26. UNIBUS 0
27. DR11-B, M7230
28. DR11-B, M7230
29. Switch 0
30. Machinery room
31. Control room
32. To UNIBUS 2

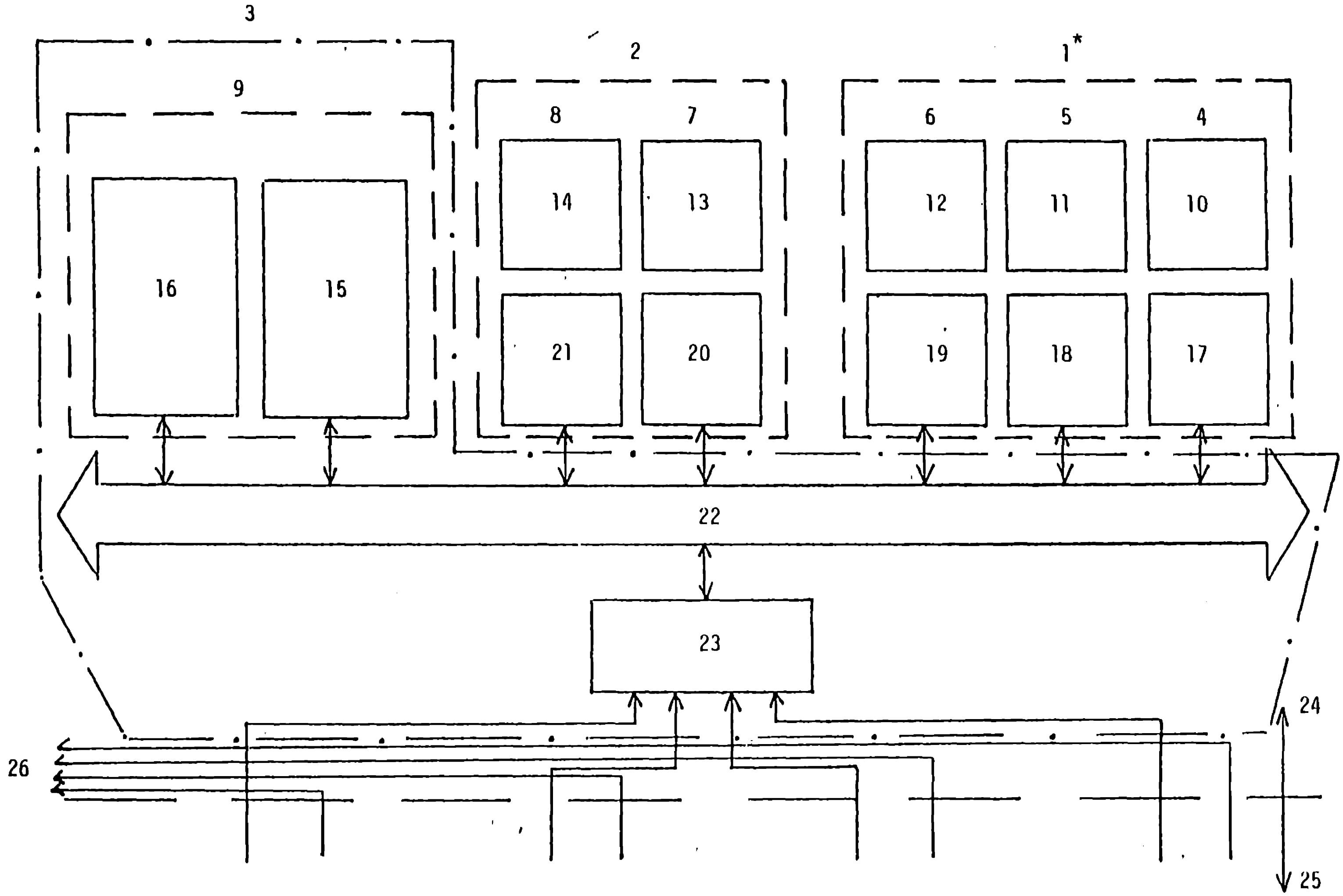


Figure 2.5.6 Dual star architecture serial transmission, detailed design.
*See legend on next page.

1. MMI 1
2. Secondary storage 1
3. Processor 1
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/60 EA (1) (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MS11-KE memory
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Control documation M200
19. LP11 controller
20. TS03 master
21. RL-11 controller
22. UNIBUS 1
23. DZ11-C (serial interface)
24. Control room
25. Machinery room

26 To UNIBUS 2

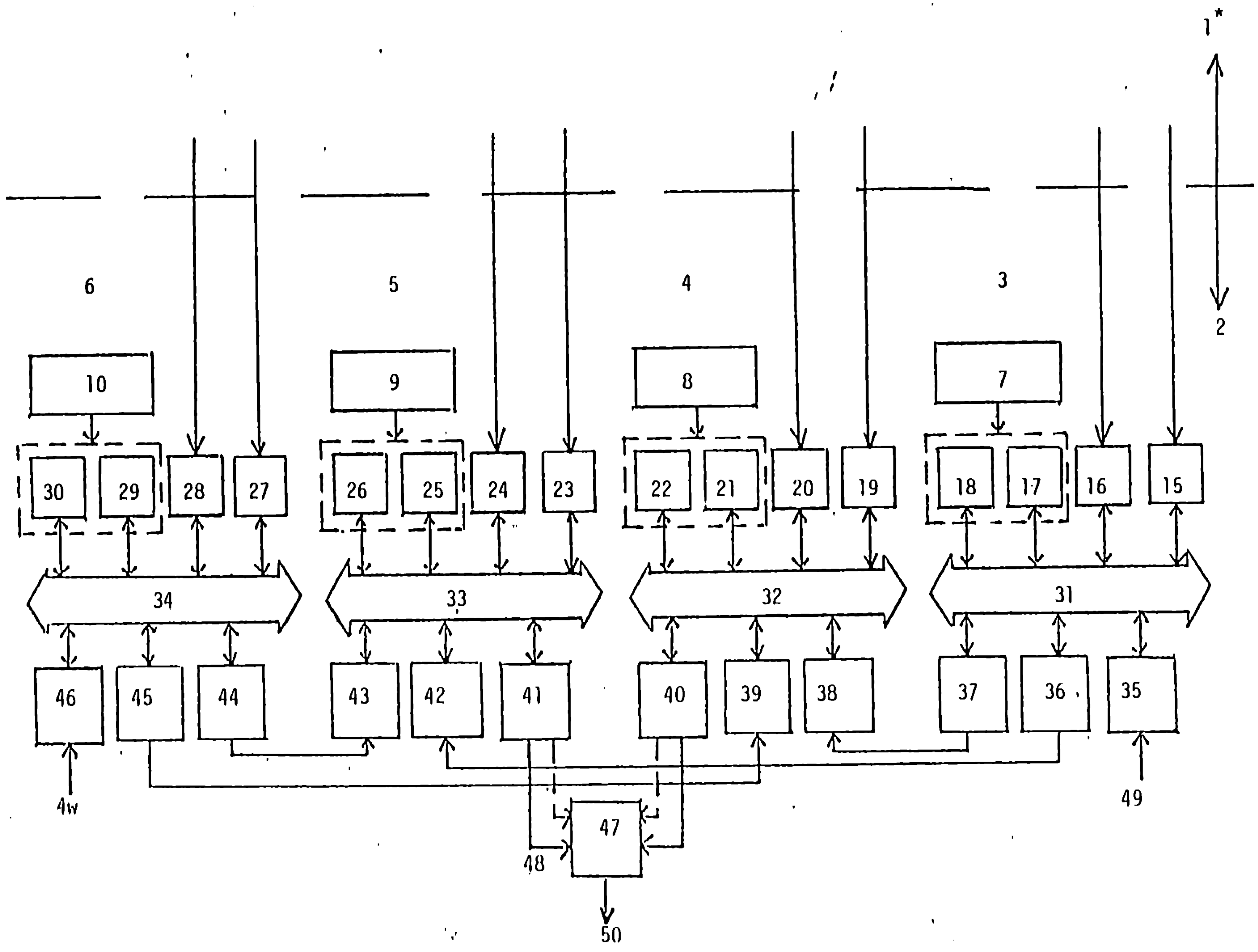


Figure 2.5.6 (continued)
*See legend on next page.

1. Control room
2. Machinery room
3. μPD' (stand-by diagnosis microprocessor)
4. μPC' (stand-by control microprocessor)
5. μPC (control microprocessor on service)
6. μPD (diagnosis microprocessor on service)
7. H9270 (3) (power supply)
8. H9270 (2)
9. H9270 (2)
10. H9270 (3)
11. KDF11-HD (CPU and memory)
12. KDF11-HB (CPU and memory)
13. KDF11-HB
14. KDF11-HD
15. DLV-11 (serial interface)
16. DLV-11
17. MSV11-DD (memory)
18. KDF11-AC (CPU)
19. DLV-11
20. DLV-11
21. MSV11-DB (memory)
22. KD11-HA (CPU)
23. DLV-11
24. DLV-11
25. MSV11-DB
26. KD11-HA
27. DLV-11
28. DLV-11
29. MSV11-DD
30. KDF11-AC
31. Q-BUS
32. Q-BUS
33. Q-BUS
34. Q-BUS
35. ADV11-A (5) (A/D interface)
36. DRV11-B (parallel interface)
37. DRV11-B
38. DRV11-B
39. DRV11-B
40. AAV11-A (5) (D/A interface)
41. AAV11-A (4)
42. DRV11-B
43. DRV11-B
44. DRV11-B
45. DRV11-B
46. ADV11-A (5)
47. MPC8S (Motorola analog multiplexer)
48. Switch
49. Sensors
50. Actuators

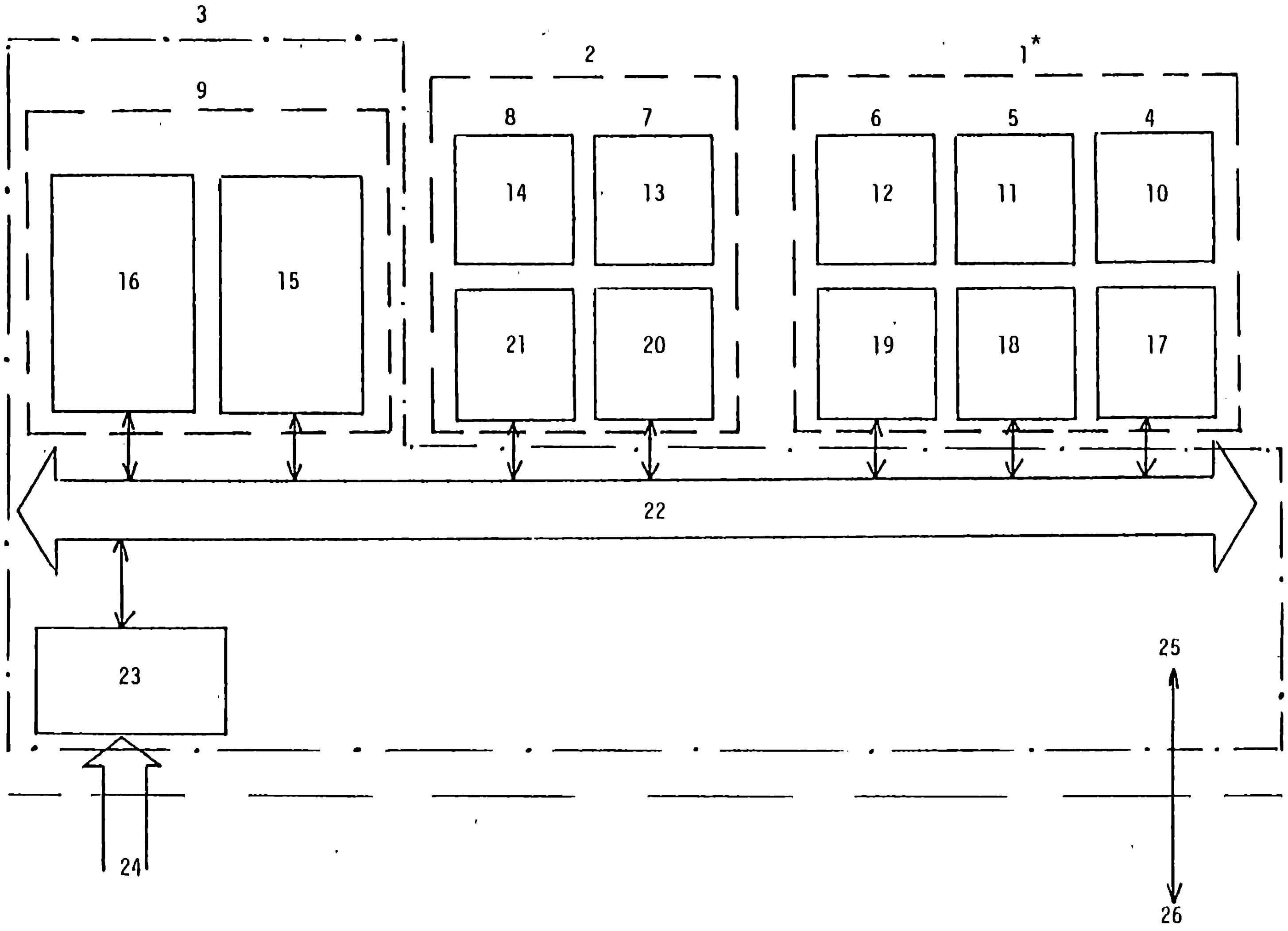


Figure 2.5.7 Global bus architecture, block diagram.
*See legend on next page.

1. MMI
2. Secondary storage
3. Processor
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. TS03-MA (1) (magnetic tape system)
8. RL11-AK (1) (disk system)
9. 11/60 EA (CPU and memory)
10. 19" color monitor
11. CR04-A card reader
12. LP05-VA printer
13. TS03-SA tape driver
14. RL01-AK disk drive
15. MS11-KE memory
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Controller documation M200
19. LP11 controller
20. TS03 master
21. RL-11 controller
22. UNIBUS
23. Megalink 11-0016 (Computrol serial interface)
24. Global data bus
25. Control room
26. Machinery room

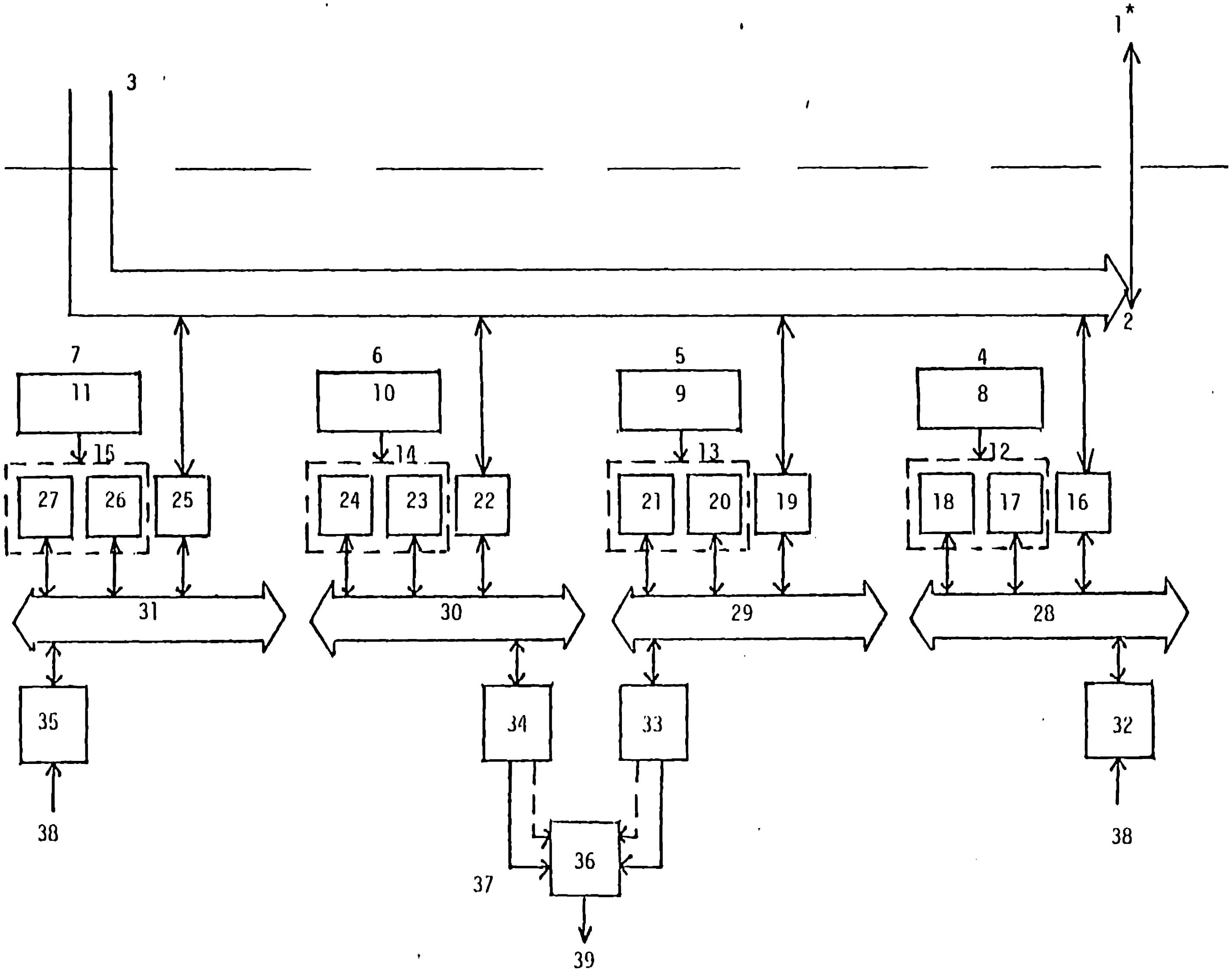


Figure 2.5.7 (continued)
*See legend on next page.

1. Control room
2. Machinery room
3. Global data bus
4. μPD' (stand-by diagnosis microprocessor)
5. μPC' (stand-by control microprocessor)
6. μPC (control microprocessor on service)
7. μPD (diagnosis microprocessor on service)
8. H9270 (2) (power supply)
9. H9270 (2)
10. H9270 (2)
11. H9270 (2)
12. KDF11-HD (CPU and memory)
13. KDF11-HB (CPU and memory)
14. KDF11-HB
15. KDF11-HD
16. 11-0011 (computrol serial interface)
17. MSV11-DD (memory)
18. KDF11-HC (CPU)
19. 11-0011
20. MSV11-DB (memory)
21. KD11-HA (CPU)
22. 11-0011
23. MSV11-DB
24. KD11-HA
25. 11-0011
26. MSV11-DD
27. KDF11-AC
28. Q-BUS
29. Q-BUS
30. Q-BUS
31. Q-BUS
32. ADV11-A (5) (A/D interface)
33. AAV11-A (4) (D/A interface)
34. AAV11-A (4)
35. ADV11-A (5)
36. MPC8S (Motorola analog multiplexer)
37. Switch
38. Sensors
39. Actuators

bus has a complete minicomputer plus its peripherals or a back-up system. Also a redundant global bus is added. The switching is accomplished by special software. Every microprocessor is connected to both buses, but control microprocessors only communicate with the active minicomputer. The detailed design for this architecture is shown in Figure 2.5.8. The worksheets are in Appendix C.

2.6 FAULT TREE FORMULATION

Once the alternative architectures are available, the fault tree analysis can be performed (Ref. 2.10). Fault trees can be developed to almost any degree of detail but a very refined analysis will result in a cumbersome and extremely lengthy effort. For that reason a reasonable set of assumptions is therefore made in order to reduce the amount of data processing and theoretical development without losing the generality of the work.

The following considerations have been taken into account:

1. In order to give more flexibility to the analysis, the fault trees are developed in two different situations. These situations represent conditions which the architecture could be subjected during the operating life.

- Situation One: the surveillance and control system together with the plant are operating under normal conditions. The top event is to find out the probability of the control system failure.

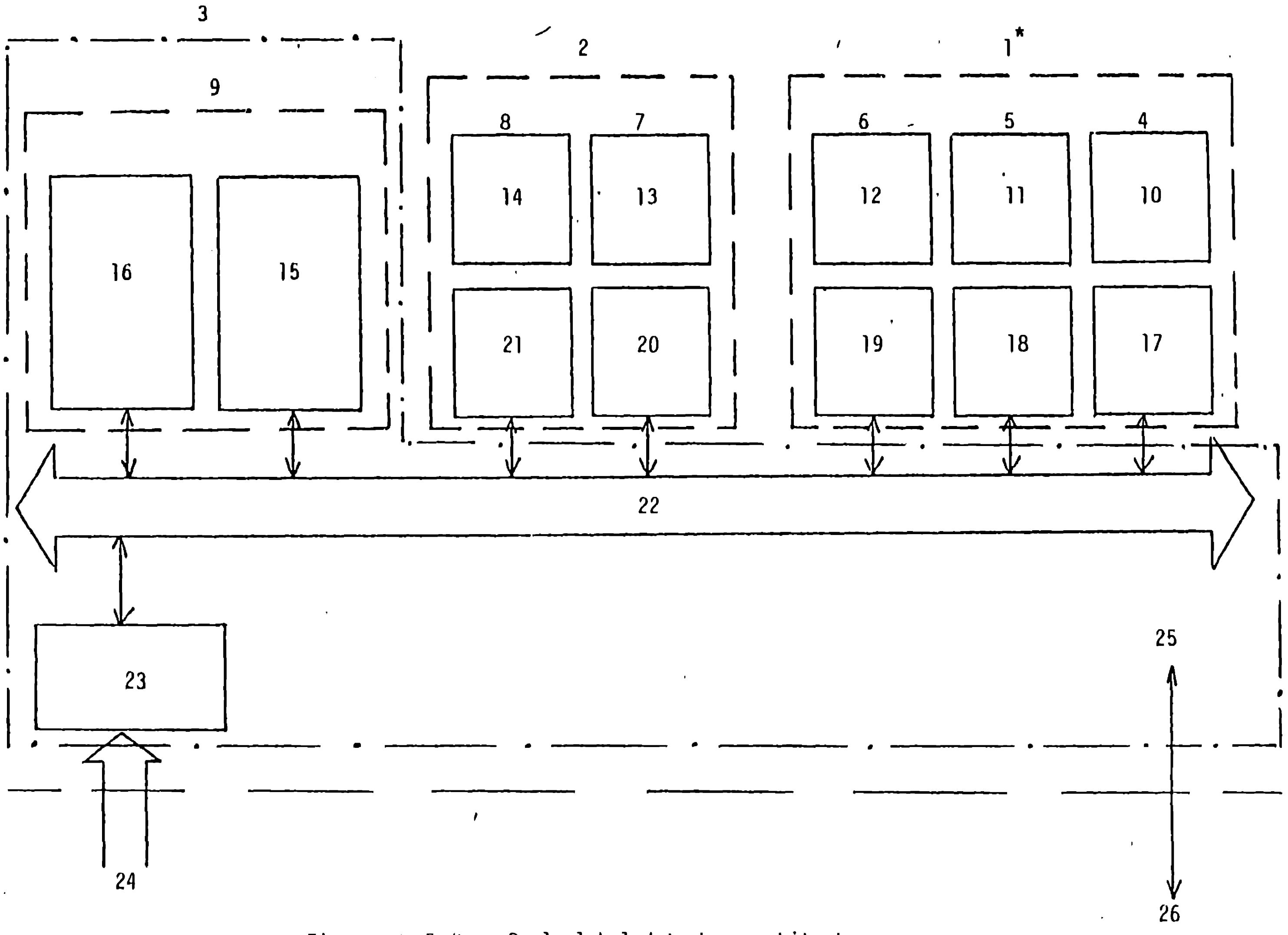


Figure 2.5.8 Dual global data bus architecture, detailed design.
*See legend on next page.

1. MMI
2. Secondary storage
3. Processor
4. VS11-AP (3) (monitors and keyboards)
5. CR-11 (1) (card reader system)
6. LP11-VA (1) (printer system)
7. RL11-AK (disk system)
8. TS03-MA (magnetic tape system)
9. 11/60 EA (CPU and memory)
10. 19" color monitor
11. CR011-A card reader
12. LP05-VA printer
13. TS03-SA tape drive
14. RL01-AK disk drive
15. MS11-RE memory
16. KD11-K CPU
17. VS11-AA, VRV02-BA
18. Controller documation M200
19. LP11 Controller
20. TS03 Master
21. RL-11 Controller
22. UNIBUS 1
23. Megalink 11-0016 (Computrol serial interface)
24. Global data bus 1
25. Control room
26. Machinery room

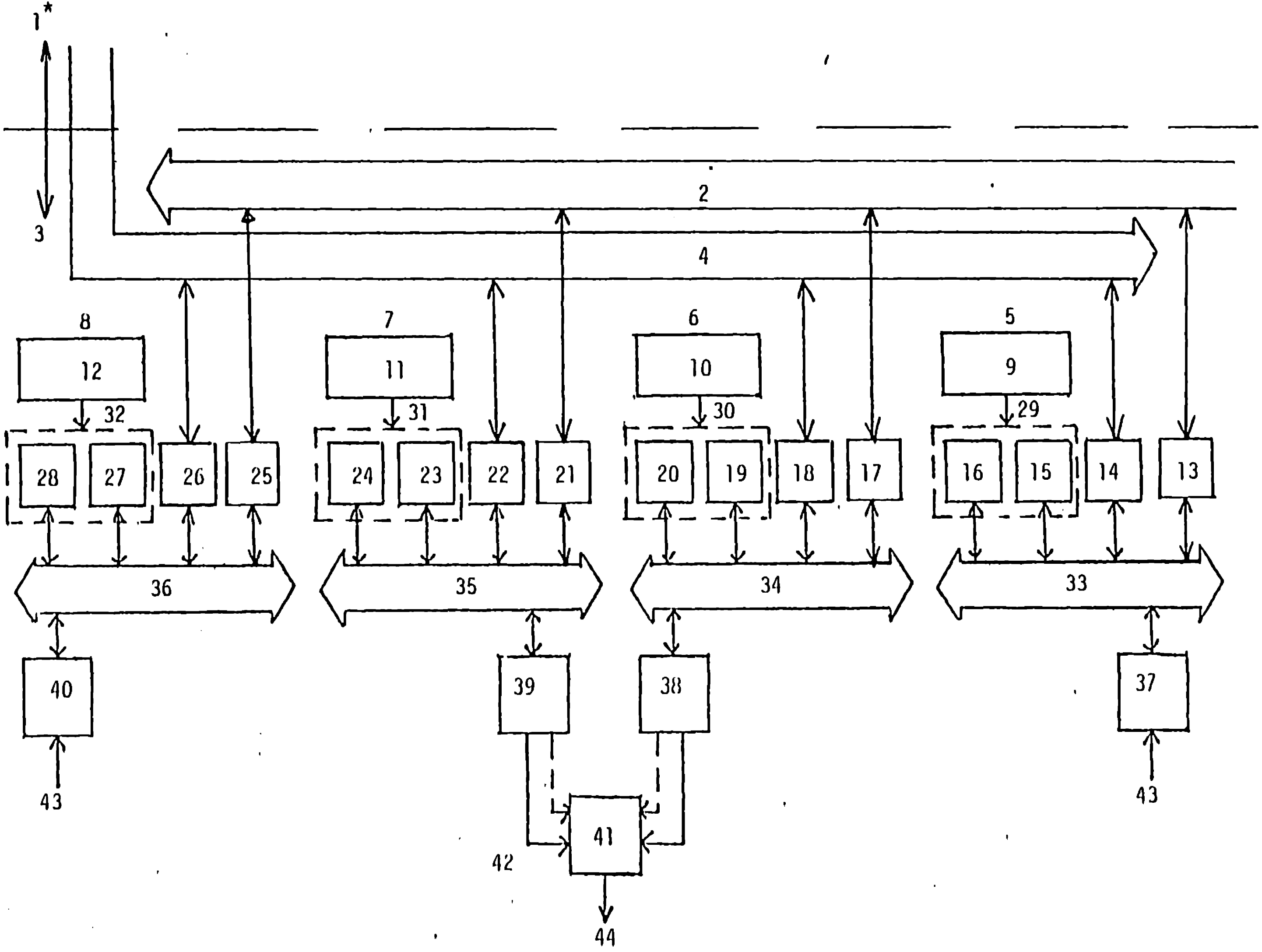


Figure 2.5.8 (continued).
*See legend on next page.

1. Control room
2. Global data bus 2
3. Machinery room
4. Global data bus 1
5. μPD' (stand-by diagnosis microprocessor)
6. μPC' (stand-by control microprocessor)
7. μPC (control microprocessor on service)
8. μPD (diagnosis microprocessor on service)
9. H9270 (2) (power supply)
10. H9270 (2)
11. H9270 (2)
12. H9270 (2)
13. 11-0011 (Computrol serial interface)
14. 11-0011
15. MSV11-DD (memory)
16. KDF11-AC (CPU)
17. 11-0011
18. 11-0011
19. MSV11-DB (memory)
20. KD11-HA (CPU)
21. 11-0011
22. 11-0011
23. MSV11-DB
24. KD11-HA
25. 11-0011
26. 11-0011
27. MSV11-DD
28. KDF11-AC
39. KDF11-HD (CPU and memory)
30. KD11-HB (CPU and memory)
31. KD11-HB
32. KDF11-HD
33. Q-BUS
34. Q-BUS
35. Q-BUS
36. Q-BUS
37. ADV11-A (5) (A/D interface)
38. AAV11-A (4) (D/A interface)
39. AAV11-A (4)
40. ADV11-A (5)
41. MPC8S (Motorola analog multiplexer)
42. Switch
43. Sensors
44. Actuators

- Situation Two: the plant is in an accident situation or an accident is going on. The analysis of the top event is to find the probability of failure for the diagnosis and surveillance system to advise the operator properly.
- There is a third important situation--to estimate the probability of the diagnostic system to detect and prevent an accident in the plant. This situation is very complex to analyze, and is beyond the scope of this thesis. Nevertheless, for the goals of the present work, that situation does need to be evaluated in a preliminary manner.

2. Any failure mode which is common to all alternatives is not included (i.e., external power supply failure, sensor failure, plant failures in general).
3. The failure of one component of a subsystem will be considered as making the subsystem fail unless there is a backup device.
4. The procedure followed is first to make a fault tree for each alternative under situations one and two. Next the corresponding boolean equations are obtained by applying boolean laws, the latter equations take a reduced form. Finally the probability equations are calculated. When the probability equations apply to low probability events they are approximated by the commonly used approach

   $p(A + B) \simeq p(A) + p(B)$

   When the events have high probability no approximation is made.

   $p(A + B) = p(A) + p(B) - p(A)p(B)$

Another implicit assumption is to consider all events independent, thus
$p(A \times B) = p(A)p(B)$.

5. The probability of a device failing in such a way as to hold the data bus is so low that the event is neglected in the fault trees.

2.6.1 CENTRAL PROCESSOR ARCHITECTURE

The fault tree and its corresponding probability equations are in Appendix D. The following comments apply to the fault tree development.

1. Communications control and data validation are done by the central processor
2. The operator has questioning capabilities over the communications; he also receives the validated data
3. The event "man-machine interface fails" implies bad data reception or transmission of wrong commands because of console failure.
4. Secondary storage covers disk drives, magnetic tape units, and their controllers.
5. The fault tree for situation two is different from condition one because the hardware involved in each situation is different. For example, the D/A interface and control microprocessor do not take part in the operator advisory process.
6. The probability of software failure is a fixed value determined

by the designer. When this value is stated, the program has to be debugged up to that value. All software will be considered with the same failure rate (see Appendix E).

Figures D.1 and D.2 show the fault trees, the legend is in Tables D.1 and D.2. Finally, equations D.1 and D.2 are the probabilistic equations for these fault trees.

2.6.2 DUAL CENTRAL PROCESSOR ARCHITECTURE

The following comments apply to this architecture.

1. The dual central processor has a data link between both CPUs which is not included in the fault tree due to its low probability of failure.
2. The processor's hardware failure related with the switch is only the hardware which works with the switch.
3. For the software related to the switch a conservative viewpoint has been taken, namely any software failure fails the switch.
5. It is assumed that if individual switches fail, the switch system fails (another conservative measure).
6. The same comments in 2.6.1 apply in this architecture.

The fault trees are presented in Figures D.3 and D.4; the legend for the fault trees is in Tables D.3 and D.4. Finally the probabilistic equations are D.3 and D.4, all in Appendix D.

2.6.3 STAR ARCHITECTURE

The following comments apply to these architectures.

1. It is included fault trees for the parallel and serial transmission alternatives (situations one and two).

2. Dedicated systems C_1, C_2, C_3, C_4, C_5, and C_6 are assumed to have the same hardware. Therefore, it is only necessary to calculate one to estimate the others.

3. In situation one the failure of D_9, D_{10}, D_{11}, D_{12}, and D_{13} do not contribute to the top event.

4. The lines from D/A, A/D to microprocessor are too short to be included.

5. A conservative approach is taken assuming the failure of one subsystem causes failure of the whole system.

6. The switches at the microprocessor level were treated in the same manner as the switches for the dual processor alternative.

7. Software failure is considered a constant for every processing device (by designer decision). The parallel transmission has the following special comments.

   -In situation two "mc hardware fails" does not include the parallel interfaces with the microprocessors

   -Also in condition two "μPD_3 hardware fails" does not include the parallel interface with the μPC_3.

The serial transmission alternative has the following special comments:

-"mC hardware fails" does not include the serial interface to the microprocessor (condition two)

-"μPD_3 hardware fails" does not include the parallel interface to the μPC_3 (condition two)

Figures D.5 and D.6 show the fault trees for the parallel and serial architectures. Equations D.5 and D.6 are the probabilistic equations for the fault trees. Tables D.5 and D.6 have the legend for the parallel transmission case. Tables D.7 and D.8 have the legend for the serial transmission case.

2.6.4 DUAL STAR ARCHITECTURE

All the comments given for the single architecture apply in this case.

1. The switch used in the parallel transmission alternative has the same properties as the switch used in the dual central computer.
2. The software switch used in the serial transmission alternative assumes only a failure in the mC hardware which is related to the switching functions.

Figures D.9 and D.10 show the fault trees for the parallel transmission case. Tables D.9 and D.10 give the legends applied to these figures. Equations D.9 and D.10 are the probabilistic equations related with the D.9 and D.10.

Figure D.11 shows the fault tree for the serial alternative situation one. Figure D.10 also represents the fault tree for the serial alternative situation two. The legend for these figures is in Tables D.11, D.10, and D.12, respectively. Equation D.11 is the probabilistic equation for condition one. Equation D.10 is the probabilistic equation for condition two.

2.6.5 GLOBAL BUS ARCHITECTURE

The following comments apply to this case.

1. The cables from switches to microprocessors or from microprocessors to the bus (coaxial cable) are too short to be included.
2. All the general comments related with microprocessors and minicomputers apply.
3. The mC hardware for conditions one and two is the same.

Figures D.13 and D.14 show the fault trees for conditions one and two; the legend is in Tables D.13 and D.14. The equations D.13 and D.14 are the probabilistic equations.

2.6.6 DUAL GLOBAL BUS ARCHITECTURE

The following comments apply:

1. It is assumed that every validation microprocessor works simultaneously with both minicomputers.
2. The comments in Section 2.6.5 also apply here.

Figures D.15 and D.16 show the corresponding fault trees; the legend is in Tables D.15 and D.16. Equations D.13 and D.14 are the probabilistic equations for this case.

Greater insight on what devices are included in each calculation is obtained by looking at Section 2.7.

2.7 PROBABILITIES OF FAILURE OF COMPONENTS AND SOFTWARE

Up to this point, the hardware configuration and the fault trees are known. The next step is to find the basic probablities of failures in order to input them into the probabilities equations.

The event probabilities related with hardware are calculated by assuming the failure rates provided by the vendor as a constant during the time between maintenance. The expression for the reliability of a component is given by:

$$R(t) = \exp[-\int_{t_1}^{t_2} h(t)dt] \qquad (2.7.1)$$

where

$R(t)$ = reliability (success probability during the mission time)

$h(t)$ = hazard rate (instantaneous failure rate) (f/h)

t_1 = time when mission begins

t_2 = time when mission ends

Generally $\Delta T = t_2 - t_3$ is considered as the time between maintenance.

If the hazard rate is constant or equal to λ, equation (2.7.1) takes the form of

$$R(t) = \exp(-\lambda t) \qquad (2.7.2)$$

and $\overline{R}(t) = 1 - R(t)$ (2.7.3)

where $\overline{R}(t)$ is called unreliability or probability of failure.

The probability of software failure has been introduced because of the huge software development task that an effort of this kind involves. It is almost inconceivable to reach an error-free software for this job, therefore the estimated software failure rate is another input to the probability equations. In fact, software failure is included from the beginning in the fault trees.

For the purposes of this thesis, the software failure rate will be considered a fixed value stated by the designer as a goal that has to be achieved by the programmers and debuggers. To reach the given level of reliability means a corresponding effort in debugging man-hours, therefore the complexity of one algorithm will not only appear in its reliability but in its costs. Appendix E explains how the debugging time can be obtained starting from a given software hazard function.

The following subsections are devoted to the calculation of failure rates for each basic event. Once a basic event failure rate is calculated in one architecture, if it appears in another architecture the calculation will not be repeated.

2.7.1 CENTRAL COMPUTER ARCHITECTURE

Each basic event is analyzed separately and the resultant failure rate is recorded in the corresponding table in Appendix D under the name "generic failure rate."

The columns of the tables given in Appendix D deserve special explanation:

-Generic failure rate (λ_G)--this is the basic failure rate generally given by the vendors and calculated from their own tests under laboratory conditions.

-Quality factor (π_Q): This factor multiplies the generic failure rate, introducing a correction which takes into account the degree of quality control during the manufacturing process.

-Environmental factor (π_E): This factor also multiplies the generic failure rate, introducing a correction which considers the effect of the actual environment in which the devices are placed.

-Learning factor (π_L): This factor also multiplies the generic failure rate, introducing the degree of technical development undergone by the component before it reaches the market. The values for each factor are given in Ref. 2.8.

It should also be noted that the data supplied by DEC already have a π_Q = 16, then at the tables this factor will appear as a 1.0. Therefore

$$\lambda = \lambda_G \times \pi_Q \times \pi_E \times \pi_L$$

where λ = estimated component failure rate. λ is also stated in the tables. Listed under the title "event probability" is the result of transforming λ by Equations 2.7.2 and 2.7.3. This is the estimated event probability of failure. The remaining colums are self-explanatory.

2.7.1.1 SITUATION ONE

A. Control line fails: The most common practice is to assume a zero failure rate for the cables, but a high number of them and their length (approximately 35m) makes it advisable to choose a conservative value for these components. The number given in Table D.1 and others comes from reference 2.8.

Under the assumption that a failure in a cable makes the control line fail (a conservative assumption), the probability of failure for the control cables is calculated as:

$$P_t = 1 - \exp(-N\lambda t)$$

P_t = probability of failure

N = number of cables (100 control case)

λ = estimated failure rate

t = time between maintenance.

Initially the maintenance policy will be assumed as one test every day. Later the weight of this assumption will be assessed.

B. Central processor fails: It is assumed a failure in the central processor when any of its components fails, e.g., the total failure rate is equal to the summation of the components' failure rates. A list of the components, their number, and the failure rates multiplied by the component number follows:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU	1	226.397
A/D controllers	9	694.93
Memory	1	80.095
A/D devices	18	98.12
Backplanes	14	0.21
A/D multiplexers	18	68.1
Unibus repeaters	4	21.967
D/A controllers	27	2084.79
Power supplies	5	57.55
D/A devices	27	225.041
		TOTAL 3557.2

D. MMI fails: the man-machine interface failure of most concern involves the three consoles; thus when the three consoles fail together it will be assumed to be an MMI failure. This means the final probability of failure is the probability of failure for one console to the third power.

Console (1)	173.392

E. Control software fails: The software will be required to be very reliable; for calculation purposes it will be assumed as 0.5 failure during the hardware lifetime (10 years), or $\lambda = 5.71 \times 10^{-6}$.

F. Diagnosis lines fails: The same explanation for control cables holds but now N = 1089.

2.7.1.2 SITUATION 2

G. Central processor hardware fails: The failure rate is calculated including only the components involved in the diagnosis problem.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	306.493
Backplanes	14	0.21
Unibus repeaters	4	21.967
A/D devices	18	98.106
Multiplexers	18	68.102
Power supplies	5	57.55
		TOTAL 1247.36

H. Secondary storage system fails: The system is made up of a disk storage drive plus a magnetic tape drive as a back-up. A failure in the secondary storage appears when both drives fail together. In other words,

P_t(secondary storage) = P_t(disk) x P_t(tape)

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
Disk drive	1	181.80198
Controller	1	17.71678
Total disk		199.51876
Magnetic tape (complete)	1	203.33456

Then P_t(disk unit) = 2.97167×10^{-2}

P_t(tape unit) = 3.0276×10^{-4}

I. Diagnosis software fails: The failure rate for software is already stated.

2.7.2 DUAL CENTRAL COMPUTER

2.7.2.1 SITUATION ONE

J. Switch hardware fails: Each analog output line has its own switch. Taking a conservative measure it will be assumed that the failure of one switch causes failure of the switch system. The switch system failure rate is the summation of the individual failure rates.

Switch	1	.155

K. Processor 1 hardware fails (SR): This event only includes the hardware related to the switch.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	306.49
Unibus repeaters	4	21.967

Backplanes	14	0.21
D/A controllers	27	2084.79
Power supplies	5	57.55
D/A devices	27	225.041
		TOTAL 2696.05

L. Processor 2 hardware fails: The same as event A.

M. Processor 2 hardware fails (SR): The same as event L.

2.7.2.2 SITUATION TWO

N. Central processor hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	306.49
Unibus repeaters	4	21.967
A/D controllers	9	694.932
Backplanes	14	0.21
A/D devices	18	98.106
Multiplexers	18	68.102
Power supplies	5	57.55
		TOTAL 1247.36

2.7.3 STAR ARCHITECTURE

2.7.3.1 PARALLEL COMMUNICATIONS

2.7.3.1.1 SITUATION ONE

C. Central mC hardware fails: It is assumed that any component of the minicomputer makes the mC fail, thus,

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.617
Unibus repeaters	3	16.475
Power supplies	1	11.50994
Parallel interfaces	42	311.9172
Backplanes	24	0.36
Extra memory	1	8.22293
	TOTAL	539.108

E. C_3 - mC line fails: This is the cable which connects the microprocessor with the central minicomputer: $\lambda = 0.6(f/10^6 h)$.

F. μPC_3 hardware fails: All the microprocessor components are included in this calculation. For the effects of considering the interfaces, an average number will be assumed. This assumption is more reasonable than to assume the number of interfaces needed by the most required microprocessor, which would be an overly conservative measure and could distorts the final results due to the high comparative cost of these interfaces.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	49.78366
Parallel interfaces	3	23.07084
D/A devices	4	21.54176
Backplanes	2	0.0003
Power supplies	2	12.43876
	TOTAL	106.837

H. μPD_3 hardware fails: Same considerations are used as for μPC_3.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Parallel interfaces	3	23.07084
A/D devices	5	36.9377
Backplanes	3	0.0045
Power supplies	2	12.43876
	TOTAL	101.0653

M. Switch hardware fails: Assuming that the failure of one switch makes the switch system fail, the individual failure rates is .155 (f/10^6h) and each system has 8 switches.

PP. μPC_3 hardware fails (SR): Only the hardware related with the switch is included.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	49.78366
Power supplies	2	12.43876
Backplanes	2	0.0003
D/A device	1	5.38544
	TOTAL	67.6105

2.7.3.1.2 SITUATION TWO

GG. mC hardware fails: In this situation the parallel interfaces with the μPCs are not included, thus,

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.617
Extra memory	1	8.22293

Unibus repeaters	3		16.475
Parallel interfaces	28		207.946
Backplanes	24		0.36
Power supplies	1		11.50994
		TOTAL	435.131

JJ. μPD_3 hardware fails: This event does not include the parallel interfaces with the μPC.

COMPONENT	NUMBER		FAILURE RATE/10^6 Hours
CPU and memory	1		28.61452
Parallel interfaces	1		7.42666
A/D devices	5		36.9377
Power supplies	2		12.43826
Backplanes	3		0.00045
		TOTAL	85.4216

2.7.3.2 SERIAL COMMUNICATIONS

The overall architecture is very similar to the parallel case; only a few components are different to make up the serial asynchronous communications. This fact makes the fault trees similar and also the probabilistic equations. Only a few values change, the remaining evaluation is exactly equal to the corresponding parallel situation.

2.7.3.2.1 SITUATION ONE

C. Central mC hardware fails: The components included in this event are:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.61766
Serial interfaces	6	153.8538
Extra memory	1	8.22993
		TOTAL 352.6944

F. μPC_3 hardware fails.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	49.78366
Power supplies	2	12.43826
Backplanes	2	12.43826
A/D devices	4	21.54176
Parallel interfaces	2	14.8534
Serial interfaces	1	5.67810
		TOTAL 352.6944

I. μPD_3 hardware fails.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Parallel interfaces	2	14.8534
A/D devices	4	36.9377
Power supplies	2	12.43826
Serial interfaces	1	5.6781
Backplanes	3	0.0045
		TOTAL 98.52648

2.7.3.2.2 SITUATION TWO

GG. mC hardware fails: This event does not include the serial interfaces connecting the mC or the μPCs (one).

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	49.78366
Serial interfaces	5	128.2115
Extra memory	1	8.22293
		TOTAL 327.052

JJ. μPD_3 hardware fails: The parallel interfaces connecting with μPCs are not included.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Power supplies	2	12.43876
Backplanes	3	0.0045
Serial interface	1	5.6871
A/D devices	5	36.9377
		TOTAL 83.6731

2.7.4 DUAL STAR ARCHITECTURE

The design of the dual star architecture is fairly similar to the single star one. In the parallel transmission case, a switch which controls the communication flow between the central minicomputer and the control microprocessors has been added. The use of this switch eliminates the need of unibus repeaters for the control microprocessors. The serial communications alternative does not use a hardware switch.

2.7.4.1 SITUATION ONE

C. Central mC_1 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.61766
Power supplies	2	23.0199
Backplanes	22	0.33
Unibus repeater	1	4.49171
Parallel interfaces	28	207.9465
Extra memory	1	8.22293
		TOTAL 435.629

H. μPD_3 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Parallel interfaces	4	30.76112
A/D devices	5	36.9377
Power supplies	2	12.43826
Backplanes	3	0.0045
		TOTAL 108.7561

EE. Switch S_0 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
Switch	3	38.35223
Parallel interfaces	14	103.97324
		TOTAL 132.32547

AAA. mC_1 hardware fails (SR)

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.61766
Extra memory	1	8.22293
Power supplies	2	23.01988
Backplanes	2	0.105
	TOTAL	221.965

2.7.4.1.2 CONDITION TWO

VV. mC_2 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.61766
Extra memory	1	8.22293
Power supplies	1	23.01988
Unibus repeater	1	5.49171
Parallel interfaces	28	178.23984
Backplanes	14	0.21
	TOTAL	405.802

MM. μPD_3 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Power supplies	2	12.43826
Backplanes	3	0.0045
Parallel interfaces	2	15.38
A/D devices	5	36.9377
	TOTAL	93.37498

2.7.4.2 SERIAL COMMUNICATIONS

This dual architecture differs from the single only because it has a complete minicomputer set as a backup, and the microprocessors have an extra series interface to communicate with both minicomputers

2.7.4.2.1 SITUATION ONE

F. μPC_3 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	48.78366
Power supplies	2	12.43826
Backplanes	2	0.0003
Serial interfaces	2	11.3562
Parallel interfaces	2	15.38056
D/A devices	4	21.54176
	TOTAL	110.50344

H. μPD_3 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.761452
Power supplies	2	12.43826
Backplanes	3	0.0045
Serial interfaces	2	11.3562
Parallel interfaces	2	15.38056
A/D devices	5	36.9397
	TOTAL	104.731

2.7.4.2 CONDITION TWO

VV. mC_2 hardware fails:

COMPONENT	NUMBER		FAILURE RATE/10^6 Hours
CPU and memory	1		190.61766
Extra memory	1		8.22293
Power supplies	2		23.01988
Unibus repeater	1		5.49171
Serial interfaces	4		102.5692
Backplanes	15		0.225
		TOTAL	330.1464

MM. μPD_3 hardware fails:

COMPONENT	NUMBER		FAILURE RATE/10^6 Hours
CPU and memory	1		28.61452
Power supplies	2		12.43826
Serial interfaces	2		11.3562
Backplanes	3		0.0045
A/D devices	5		36.9377
		TOTAL	89.3502

2.7.5 GLOBAL BUS ARCHITECTURE

2.7.5.1 SITUATION ONE

A. Global bus fails: The global bus is a coaxial cable of about 35 meters in length; its generic rate, taken from references 2.8, is
$\lambda_G = 0.6\ (f/10^6 h)$

D. mC hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	190.61766
Extra memory	1	8.2293
Control of communications and serial interface	1	25.0
		TOTAL 223.84

F. μPC_3 hardware fails:

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	48.78366
Power supplies	1	6.219
Backplanes	2	0.0003
Serial interfaces	1	25.0
D/A devices	4	21.5415
		TOTAL 102.547

J. μPD_3 hardware fails.

COMPONENT	NUMBER	FAILURE RATE/10^6 Hours
CPU and memory	1	28.61452
Power supplies	1	6.219
Backplanes	2	0.0003
Serial interface	1	25.0
A/D interfaces	5	36.9377
		TOTAL 96.776

2.7.5.2 SITUATION TWO

GG. mC hardware fails: same as situation one.

J. μPD_3 hardware fails: same as situation one.

2.7.6 DUAL GLOBAL BUS

For this alternative the microprocessors have an extra serial interface to communicate with both central minicomputers.

2.7.6.1 SITUATION ONE

H. μPC_3 hardware fails:

COMPONENT	NUMBER		FAILURE RATE/10^6 Hours
CPU and memory	1		49.78366
Power supply	1		6.219
Backplanes	2		0.0003
Serial interfaces	2		50.0
D/A interfaces	4		21.5415
		TOTAL	127.547

H. μPD_3 hardware fails:

COMPONENT	NUMBER		FAILURE RATE/10^6 Hours
CPU and memory	1		28.61452
Power supply	2		12.4383
Backplanes	2		0.0003
Serial interfaces	2		50.0
A/D devices	5		36.9377
		TOTAL	127.9935

2.7.6.2 SITUATION TWO

The components have the same failure rate as situation one.

The tables of Appendix D contain all the estimated failure rates. The next step is to calculate the probability of failure of each event; this step is done using the event failure rate in equations 2.7.2 and 2.7.3. The time between maintenance s arbitrarily set at 24 hours, the weight of this assumption will be discussed later during senstivity analysis.

The results are shown in the corresponding table under the title "Event probability of failure."

The final step is to input the "event probabilities of failure" to the corresponding probabilistic equations. The calculational results are the probability of failure for the respective architecture. Tables 2.9.1 and 2.9.2 show the estimated probability of failure for each architecture, obtained by the fault tree method.

2.8 COST OF THE ARCHITECTURES

As was explained, the costs for each architecture do not include figures for items which are seen as common expenses. Therefore, the final numbers do not represent the true final cost of each architecture, rather they show a composite number to facilitate comparative analysis.

All costs given in this section are net present values (NPV) for the year 1980. The cost for each architecture is divided into three categories:

- basic hardware cost

- basic software cost
- special software cost.

The basic hardware cost is obtained from the corresponding worksheet in Appendix C. The cost of the basic software is given by the vendor. These cost figures are for the individual device; substantial reductions can be obtained by large-scale buying, but because it is a relative situation, for each alternative will be assumed that the total hardware cost is the summation of the individual costs.

Only the special software has to be addressed in more detail. This cost is represented by the following equation:

$$C_S = T_P C_P + T_D C_D \qquad (2.8.1)$$

where

T_P = programming time (hours)

C_P = programmer cost (US$/hour)

T_D = debugging time (hours)

C_D = debugger cost (US$/hour)

T_P is a value obtained from Table B.2 and T_D is obtained by using the following equation, developed in Appendix E:

$$T_D = \frac{1}{7.381 \times 10^{-4}} \ln\left(\frac{C}{7.381 \times 10^{-4}\ B}\right) \qquad (2.8.2)$$

C has been set as 5.71 (failures/10^6h) and B as a quantity given for each algorithm in Table B.2.

The particular cost for every architecture is now calculated.

2.8.1 CENTRAL COMPUTER ARCHITECTURE COST

The first step is to obtain the special software cost. To do so two assumptions are made:

- The required failure rate for the software will be 0.5 failures during the hardware life cycle (10 years), which implies C = 5.71 x 10^{-6} [f/h].

- As it was assumed that the total memory required is equal to the summation of the individual requirements, the total number of estimated errors buried in the software is equal to the summation of the individual estimated numbers of errors.

From Table B.2

T_p = 533,498.11 (h)

B = 4041.92.

Finally, it is assumed that the programmer and the debugger have the same cost--18.75 (US$/hour).

Replacing all the values in equations 2.8.1 and 2.8.2, the estimated special software cost is 10,338,562 US$. The digital system is running under the RSX-11M operative system and it will require a FORTRAN IV compiler:

RSX-11M	7800
FORTRAN IV	700
Basic Software cost	8500 (US$)

Finally, the hardware cost is 568,198 (US$). The costs are displayed in the following table.

Hardware	568,198	
Basic Software	8,500	
Special Software	10,338,562	
Total Cost	10,915,260	US$

It is difficult not to realize the higher cost implied by the special software compared with the basic software and the hardware. Also there is an implicit assumption in the cost structure of not considering the cost of developing the theoretical models to be implemented in the computers. This cost figure could be reduced depending on the number of repeated algorithms which are the same for each processing block. Thus although the special software cost is an estimated one, this cost is going to be the dominant cost in the design process. Because the software does not degrade with time, and also can be used without any extra costs in a serial production of the same control system, the special software cost will be amortized with serial production, and with time when the hardware degenerates. For the problem at hand, the corresponding net present value of the special software is charged to each architecture, making a fair comparison and leaving the subject of how to amortize the cost to further works.

2.8.2 DUAL CENTRAL COMPUTER ARCHITECTURE COST

The hardware cost is the double of the single case plus the cost of the switches. The basic software cost is equal to the first plus the cost of a second package (which has a reduced price).

Hardware	1,137,827

Basic Software	11,650
Special Software	10,338,562
Total Cost	11,488,039 US$

2.8.3 STAR ARCHITECTURE COST

The hardware costs also come from the worksheets in Appendix C.

2.8.3.1 PARALLEL TRANSMISSION

Central processor (1)	242,888
Control microprocessors (14)	156,352
Diagnosis microprocessors (28)	416,080
Hardware cost	815,320
RSX-11M	7,800
RSX-11S	33,820
FORTRAN IV	700
Basic software cost	43,320
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,196,202 (US$)

The special software cost has been assumed similar to the other architectures because the estimated programming time and estimated debugging time have also been assumed similar. In the actual implementation the special software cost can be higher because of the extra cost in making the talking protocols between the central unit and the distributed microprocessors.

2.8.3.2 SERIAL COMMUNICATIONS

Central processor (1)	128,452
Control microprocessors (14)	152,012
Diagnosis microprocessors (28)	407,400
Hardware cost	687,864
Basic software cost	42,320
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,068,746 (US$)

2.8.4 DUAL STAR ARCHITECTURE COST

2.8.4.1 PARALLEL COMMUNICATIONS

Central processors (2)	354,400
Switch (1)	65,958
Control microprocessors (14)	156,352
Diagnosis microprocessors (28)	433,440
Hardware cost	1,010,150
Basic software cost	45,470
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,394,182 (US$)

2.8.4.2 SERIAL COMMUNICATIONS

Central processors (2)	256,904
Control microprocessors (14)	154,840
Diagnosis microprocessors (28)	416,080
Hardware cost	827,824
Basic software cost	45,470
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,211,856 (US$)

2.8.5 GLOBAL BUS ARCHITECTURE COST

Central processor (1)	106,895
Control microprocessors (14)	151,802
Diagnosis microprocessors (28)	401,380
Hardware cost	660,077
Basic software cost	42,320
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,040,959 (US$)

2.8.6 DUAL GLOBAL BUS ARCHITECTURE COST

Central processor (2)	213,790
Control microprocessors (14)	183,092
Diagnosis microprocessors (28)	483,560
Hardware cost	880,442
Basic software cost	45,470
Special software cost	10,338,562
TOTAL ARCHITECTURE COST	11,264,474 (US$)

2.9 EXPECTED MONETARY VALUE (EMV) ANALYSIS

2.9.1 INTRODUCTION

Up to this point, two important factors used in the EMV analysis have been obtained, the architecture's cost and the corresponding probability of failure (both sets of values are summarized in Tables 2.9.1 and 2.9.2). What is left is to establish formally the decision tree faced by the decision maker, and the payoffs involved by any decision if it is made. Once it is done the EMV analysis is performed.

2.9.2 DECISION TREE

The designer faces a decision tree with 8 initial branches (Figure 2.9.1), after that, because of the nature of the problem, the decision tree follows different paths according to the situation.

2.9.2.1 SITUATION ONE

In this case, each decision branch is followed by only one chance fork, say, the architecture fails or succeeds. The decision tree is shown in Figure 2.9.1. The key to the figure follows:

C = cost of the architecture
PS = probability of success
POS = payoff of success
POF = payoff of failure

Subscripts:

1 central computer architecture
2 dual central computer architecture
3 star parallel architecture
4 star serial architecture
5 dual star parallel architecture
6 dual star serial architecture
7 global bus architecture
8 dual global bus architecture

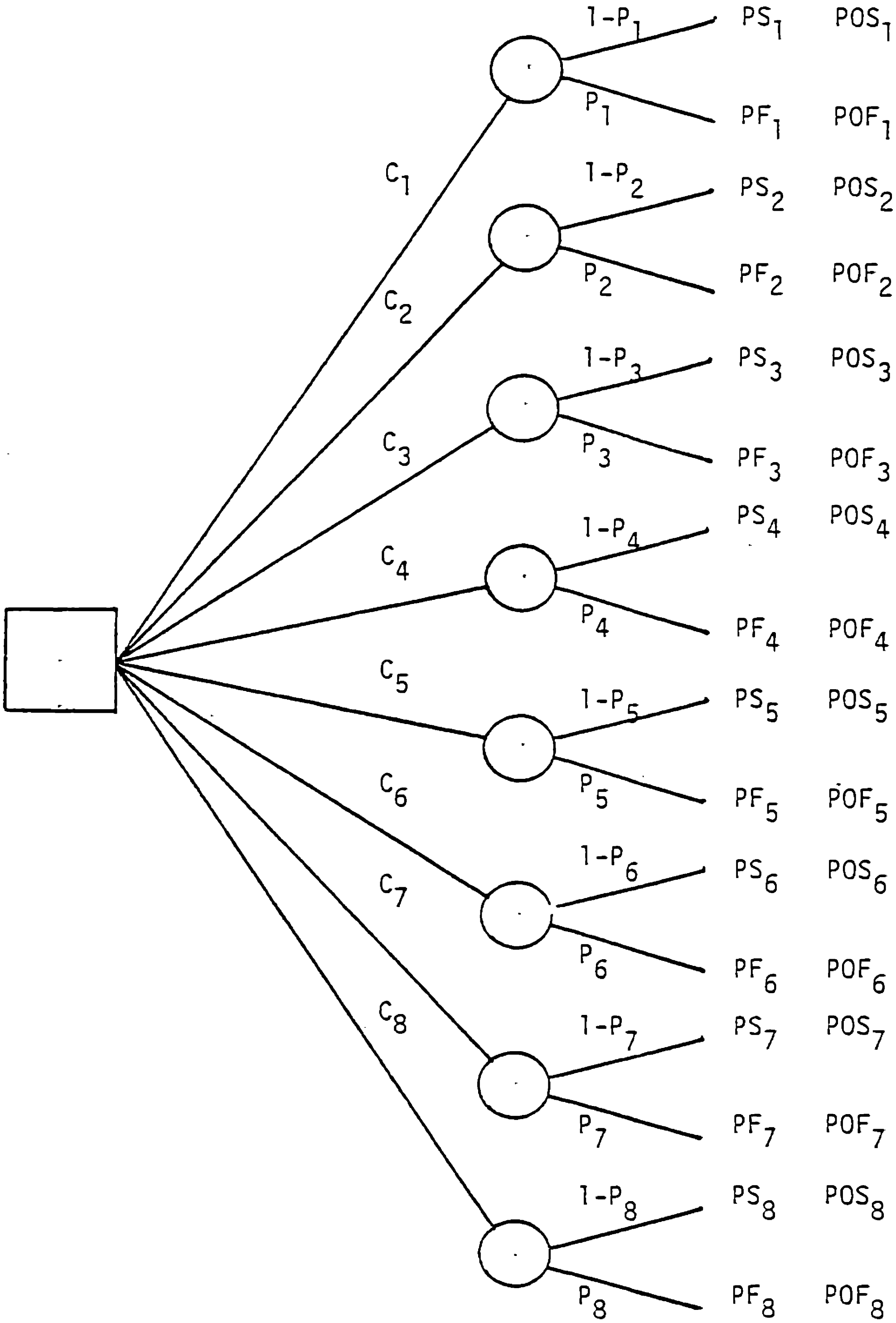


Figure 2.9.1 Decision tree for situation one.

2.9.2.2 SITUATION TWO

The decision tree corresponding to this situation differs from the previous one because now, after the computer system fails, the operator has a chance to handle the accident, or a chance of realizing that an accident is going on. The operator may succeed or fail, and that is the second chance fork shown in Figure 2.9.2

The extra nomenclature given in 2.9.2 is p_0, which represents the probability of failure for the operator.

2.9.3 PAYOFF CALCULATIONS

Payoff is another form for consequences. The actual analysis is only concerned with relative economic consequences. As far as the decision analysis theory is concerned, the study could be broadened to see how other attributes of the problem could affect the final decision, but to make such broadening is beyond the scope of this project. Thus in order to simplify the problem, and also to handle commonly used figures, the attributes in this analysis will be only the economic ones (costs, expected revenues, expected losses).

Next comes the very critical point of defining the consequences in terms of the figure of merit

2.9.3.1 SITUATION ONE

Recall that situation one refers to the case where the SDCS system and the plant are operating under normal conditions. Certain assumptions are unavoidable in order to frame the problem. In this case we assume

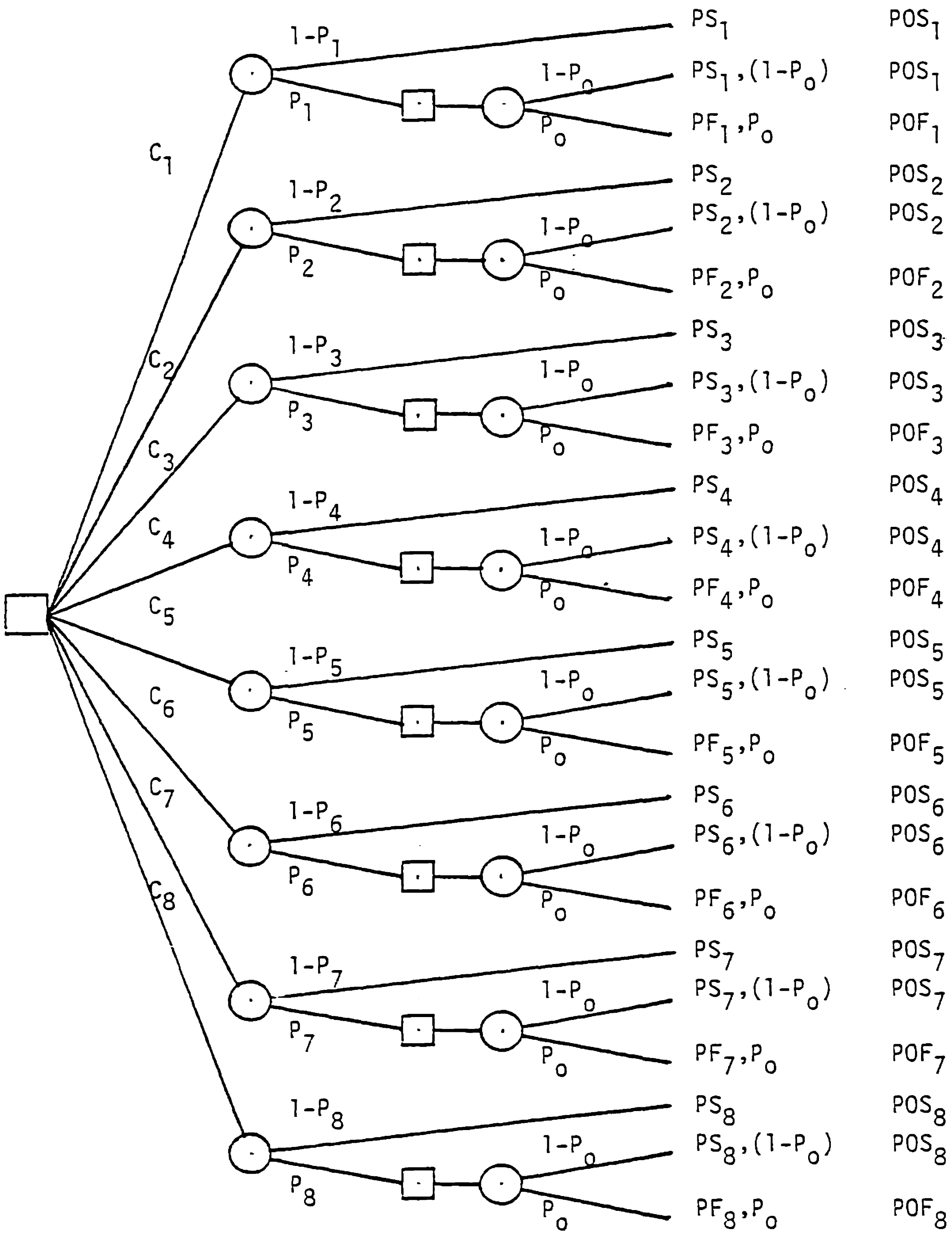


Figure 2.9.2 Decision tree for situation two.

the following:

1. All the money figures are in their NPV terms and the rate of inflation will be assumed equal to the discount rate all over the time span.
2. The ship will fail to sail, and will lose revenues if the control system fails.
3. Other reasons keeping the ship from sailing are not considered.
4. The cost of repairing the control system is negligible.
5. The revenues will be calculated in NPV during the life cycle of the hardware (10 years).
6. The consequences are similar for each architecture; what makes the difference is the expected value of the consequences and the cost of the alternative.
7. One way to estimate the approximate loss of revenue when the ship is out of service is by using the revenues obtained during operation, and correcting this value by the accumulated inflation index. After doing so the annual revenues of the ship could be approximately 6,700,000 US$. The next assumption is to say the NPV of the revenues will be exactly the same each year during the life cycle of the hardware (10 years). Because we have previously assumed a rate of inflation equal to the discounting rate during this 10 years, the total NPV of the revenue is approximately 67,000,000 US$.

Summarizing in situation one:

POS = 67,000,000 US$

POF = 0

2.9.3.2 SITUATION TWO

To specify the consequences of the failure in the surveillance, diagnostic and advising system, a set of assumptions is also established:

1. It will be assumed that if the diagnostic system fails to advise the operator correctly, and the operator consequently makes a mistake, the NSGS is lost, and the owner has to buy a new one to keep the ship in business.
2. If the system succeeds in spotting an accident and advising the operator correctly of the problem, there is no loss of plant but the ship should stop to repair the problems.
3. The first two assumptions lead to the following approximate values: POF = 1.89×10^6 US\$

   POS = 0
4. The probability of an operator's making an error is approximately 10^{-3}/action, assuming 10 actions/hour; the operator will have a failure rate of 0.01 (f/h). With a duty time of four hours (equivalent to the time between maintenance), it is possible to conclude with an operator probability of failure of 0.04.

2.9.4 EMV ANALYSIS

From the decision analysis theory and using Figures 2.9.1 and 2.9.2, the figures of merit (EMV) are:

Condition one:

$$EMV_1 = \max[(1 - PF_i)POS_i - C_i] \qquad (2.9.1)$$

Condition two:

$$EMV_2 = \max[(PF_i) \times (POF_i) \times P_o - C_i] \tag{2.9.2}$$

All the values involved in these calculations are obtained by now, thus after performing the operations required by equations 2.9.1 and 2.9.2, the figure of merit is obtained. The inputs and the results are shown in Tables 2.9.1 and 2.9.2, respectively.

Table 2.9.1

EMV ANALYSIS SITUATION ONE

ALT	PS	$POS\times10^6$	PF	POF	$C(\times10^6)$	$EMV(\times10^6)$
Central	0.5804	67	0.4197	0	10.915	27.971
Dual central	0.7961	67	0.2039	0	11.488	41.850
Star parallel	0.9173	67	0.0827	0	11.196	50.205
Star serial	0.9436	67	0.0563	0	11.069	52.156
Dual star parallel	0.9905	67	0.0093	0	11.394	54.966
Dual star serial	0.9965	67	0.0035	0	11.212	55.553
Global bus	0.96238759	67	0.0038	0	11.041	53.439
Dual global bus	0.99323765	67	0.0068	0	11.264	55.282

Table 2.9.1 shows the following rankings:

ORDER	EMV	PF	C
1	dual star serial	dual star serial	central
2	dual global bus	dual global bus	global bus
3	dual star parallel	dual star parallel	star serial
4	global bus	global bus	star parallel
5	star serial	star serial	dual star serial
6	star parallel	star parallel	dual global bus
7	dual central	dual central	dual star parallel
8	central	central	dual central

Table 2.9.2

EMV ANALYSIS SITUATION TWO

ALT	PS	POSx10^6	PF	POF(x10^6)	Cx 10^6	EMV(x10^6)
Central	0.8234	0	0.1766	-18.9	10.915	-11.046
Dual central	0.9688	0	0.0312	-18.9	11.488	-11.511
Star parallel	0.9331	0	0.0669	-18.9	11.196	-11.246
Star serial	0.9487	0	0.0514	-18.9	11.069	-11.107
Dual star parallel	0.9960	0	0.0040	-18.9	11.394	-11.397
Dual star serial	0.9975	0	0.0025	-18.9	11.212	-11.214
Global bus	0.9628	0	0.0372	-18.9	11.041	-11.069
Dual global bus	0.9937	0	0.0063	-18.9	11.264	-11.269

Table 2.9.2 shows the following rankings:

ORDER	EMV	PF	C
1	central	dual star serial	central
2	global bus	dual star parallel	global bus
3	star serial	dual global bus	star serial
4	dual star serial	dual central	star parallel
5	star parallel	global bus	dual star serial
6	dual global bus	star serial	dual global bus
7	dual star parallel	star parallel	dual star parallel
8	dual central	central	dual central

Legend:

PS	Probability of success	POF	Payoff of failure
POS	Payoff of success	C	Cost (US$)
PF	Probability of failure	EMV	Expected monetary value (US$)

The priorities order already shown deserves some comment:

1. In situation one the EMV figure favors dual distributed alternatives
2. In situation two the EMV figure favors single alternatives
3. in both studies the probability of failure favors the dual distributed alternatives
4. In both situations the costs favor the single alternatives

Final comments and conclusions are more meaningful after the sensitivity analysis in Section 2.10 has been discussed.

2.9.5 EMV ANALYSIS WITH A FAULT TOLERANT COMPUTER

Analysis of the addition of fault tolerant computers is introduced only as an illustrative example because:

- Fault tolerant computers are not standard market products and therefore by using them, the initial design requirement of using only market product is violated.

- The data supplied to the decision model are unreliable, and the technical assumptions made to fit the fault tolerant computer inside the model are too crude. Nevertheless, the results can be seen as trends and a measure of the relative magnitudes involved.

The following is the set of assumptions applied to this case.

- As an example of a fault tolerant computer, the Charles Stark Draper Laboratory fault tolerant computer will be used. Its memory capability makes it fit only in distributed architecture as a central minimcomputer.

- The CPU and memory of the standard designs are substituted by the fault tolerant CPU and memory.

- The data obtained for this fault tolerant CPU and memory are as follows:

Cost ≃ 500,000 (US$)

Failure rate ≃ 10^{-3} ($f/10^6 h$)

This failure rate substitutes the failure rate under the name "CPU and memory" in the Section 2.7 calculations (only for distributed alternatives).

After performing a new round of calculations with the probabilistic equations, the estimated probabilities of failure are written in Tables 2.9.3 and 2.9.4.

Similar procedure was followed for costs, and the new costs also appear in the tables.

Table 2.9.3

EMV ANALYSIS CONDITION ONE (FAULT TOLERANT CASE)

ALT	PS	POS($x10^6$)	PF	POF	C($x10^6$)	EMV($x10^6$)
Central	0.5804	67	0.4196	0	10.915	27.971
Dual central	0.7961	67	0.2039	0	11.488	41.850
Star parallel	0.9945	67	0.0547	0	11.661	54.972
Star serial	0.9724	67	0.0275	0	11.534	53.621
Dual star parallel	0.9939	67	$6.05x10^{-3}$	0	11.859	54.735
Dual star serial	0.9991	67	$8.67x10^{-4}$	0	11.677	55.265
Global bus	0.9918	67	$8.23x10^{-3}$	0	11.506	54.942
Dual global bus	0.9944	67	$5.61x10^{-3}$	0	11.729	54.895

Table 2.9.4

EMV ANALYSIS SITUATION TWO (FAULT TOLERANT CASE)

ALT	PS	POS	PF	POF($x10^6$)	C($x10^6$)	EMV($x10^6$)
Central	0.8234	0	0.1766	-18.9	10.915	-11.046
Dual central	0.9688	0	0.0312	-18.9	11.488	-11.511
Star parallel	0.9612	0	0.0383	-18.9	11.661	-11.690
Star serial	0.9775	0	0.0224	-18.9	11.534	-11.550
Dual star parallel	0.9981	0	0.0012	-18.9	11.859	-11.860
Dual star serial	0.9996	0	0.0004	-18.9	11.677	-11.677
Global bus	0.9922	0	$7.8x10^{-3}$	-18.9	11.505	-11.512
Dual global bus	0.9948	0	$5.19x10^{-3}$	-18.9	11.729	-11.733

With the aim of making only a rough comparison, a ranking of the first eight architectures combining fault tolerant and standard design follows:

CONDITION ONE

ORDER	EMV	PF	COST
1	dual start serial (S)	dual star serial (FT)	central (S)
2	dual global bus (S)	dual star serial (S)	global bus (S)
3	dual star serial (FT)	star parallel (FT)	star serial (S)
4	star parallel (FT)	dual global bus (FT)	star parallel (S)
5	dual star parallel (S)	dual star parallel (FT)	dual star serial (S)
6	global bus (FT)	dual global bus (S)	dual global (S)
7	dual global bus (FT)	global bus (FT)	dual star parallel (S)
8	dual star parallel(FT)	dual star parallel (FT)	dual central (S)

CONDITION TWO

ORDER	EMV	PF	COST
1	central (S)	dual star serial (FT)	central (S)
2	global bus (S)	dual star parallel (FT)	global bus (S)
3	star serial (FT)	dual star serial (S)	star serial (S)
4	dual star serial (S)	dual star parallel (S)	star parallel (S)
5	star parallel (S)	dual global bus (S)	dual global bus (S)
6	dual global bus (S)	global bus (FT)	dual global bus (S)
7	dual star parallel (S)	global bus (FT)	dual star parallel (S)
8	dual central (S)	star serial (FT)	dual central (S)

The ranking orders shown deserve the following comments:

1. The figure of merit in situation one favors standard distributed architectures. In situation two, it favors single standard architectures.
2. The probability of failure favors in both situations distributed fault tolerant alternatives.
3. The cost favors in both situations single standard alternatives.

2.10 SENSITIVITY ANALYSIS

2.10.1 INTRODUCTION

From the figure of merit viewpoint, the results obtained in Section 2.9 favor the use of dual star serial architecture for situation one, and central computer for situation two. The results obtained by introducing a fault tolerant computer are not included because of their uncertainty.

Nevertheless, there are several facts that should be commented upon:

1. The failure rate data input to the model is considered accurate to the first two significant numbers.
2. The fault trees are made under conservative assumptions which increases the estimated probability of failure for the distributed alternatives.
3. The conservative assumptions made about the switches increase the estimated probability of failure for the architectures which use switches.
4. The costs for the distributed architecture are calculated based on an "average" microprocessor, thus the precise cost can be different. Also the final cost of the architectures can be decreased when large-scale purchases are made.
5. The software failure rate chosen is a number set by heuristic approach.
6. The time between maintenance policy is an arbitrary number.
7. The operator probability of failure is a number that can be modified considering the actual training state of the operators.

These seven comments clearly indicate that some uncertainty is tied with the obtained results. In order to identify how the variation of these parameters could change the final conclusions, a sensitivity analysis of the parameters on the figure of merit was performed.

To perform the sensitivity analysis, one parameter was varied over a reasonable range while the other parameters of the model are kept fixed at their "best estimate" previously obtained values.

Appendix F shows the results of the sensitivity analysis in Tables F.1 and F.2. These numbers are graphically represented in Figures 2.10.1 through 2.10.8 and 2.10.9 through 2.10.15.

2.10.2 DISCUSSION OF THE RESULTS

Clearly the core of the whole work is given in Figures 2.10.1 to 2.10.15. In order to clarify the discussion, the analysis will be divided into three groups, one for each situation and one for features common to both situations.

2.10.2.1 SITUATION ONE

1. From the figure of merit viewpoint the winning architecture is the dual star serial communications.
2. The sensitivity analysis shows that the assumptions made to simplify the problem do not change the final conclusion.
3. The dual star serial architecture only presents a sizable sensitivity to the cost, payoff of success and time between maintenance.
4. The shape of the sensitivity curve for P(soft) suggests a maximum point which will give the optimal P(soft) required. This matter was investigated further for the winner architecture, and the results are shown in Figure 2.10.16. This figure indicates that a P(soft) $\simeq 5.0 \times 10^{-3}$ is the optimum required for the architecture (from the point of view of the figure of merit). The reason the P(soft) curve is not monotonic is the cost of debugging the code. In other words, when the

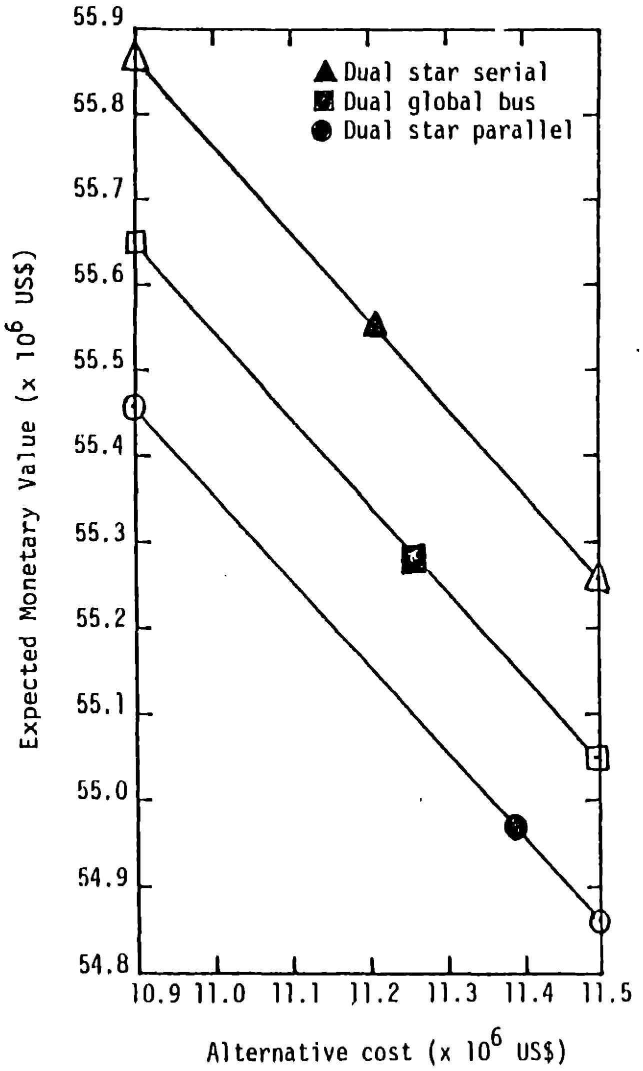


Figure 2.10.1 EMV sensitivity to cost variations (situation one)

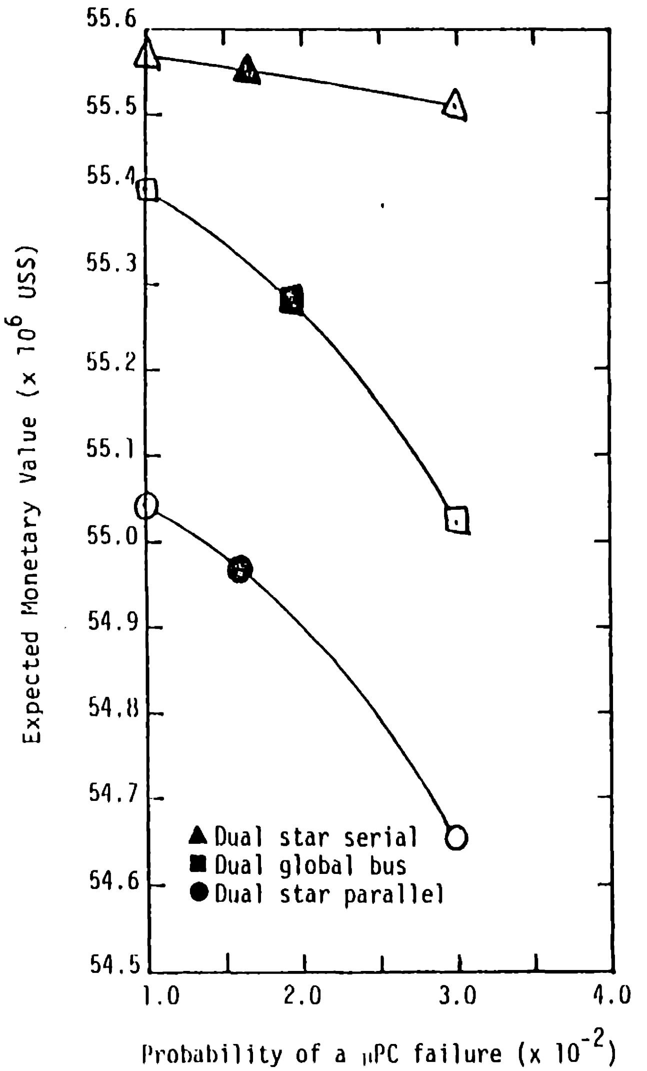


Figure 2.10.2 EMV sensitivity to probability of a control microprocessor failure (situation one)

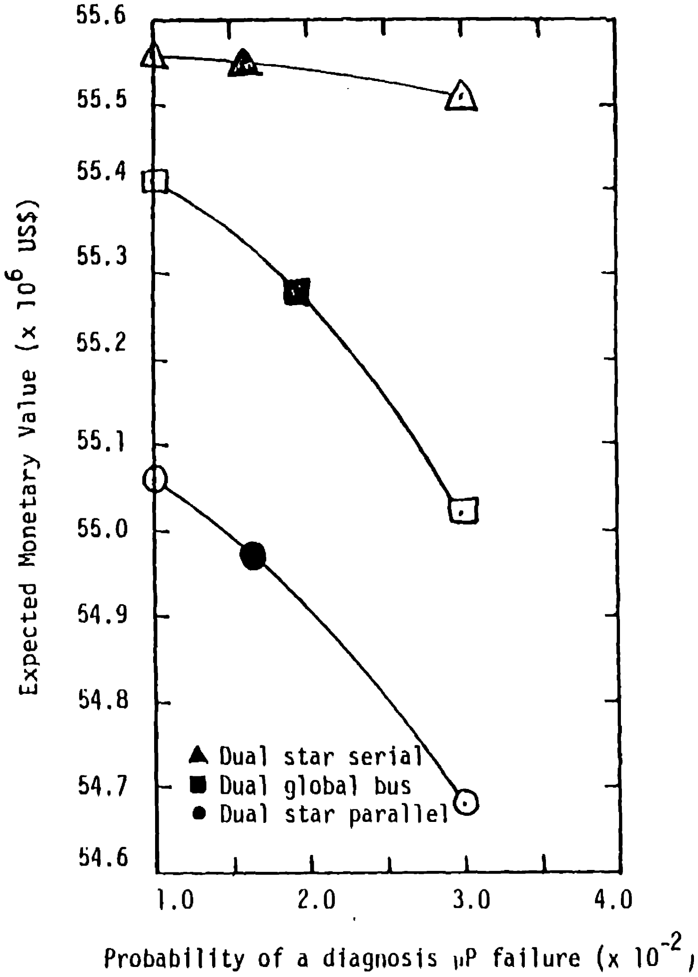


Figure 2.10.3 EMV sensitivity to probability of a diagnosis microprocessor failure (situation one)

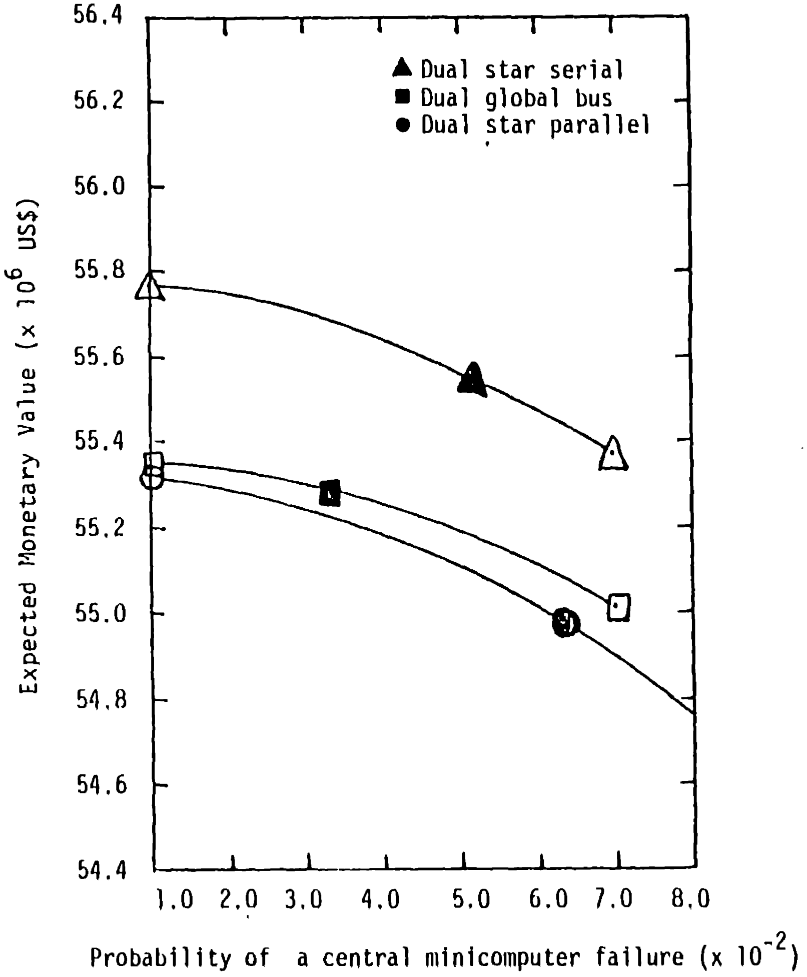


Figure 2.10.4 EMV sensitivity to probability of a central minicomputer failure (situation one)

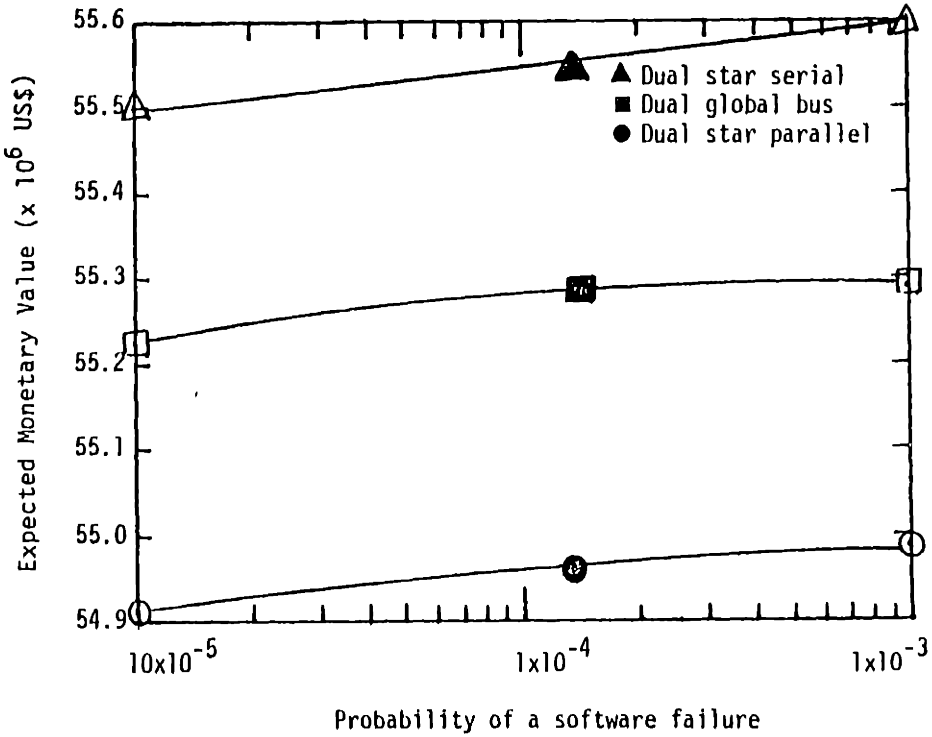


Figure 2.10.5 EMV sensitivity to a software failure (situation one).

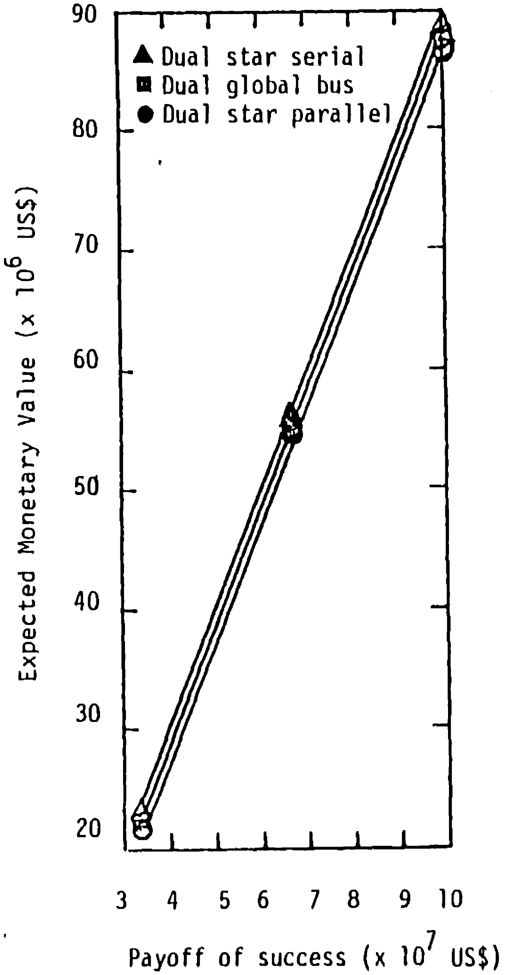


Figure 2.10.6 EMV sensitivity to payoff of success (situation one).

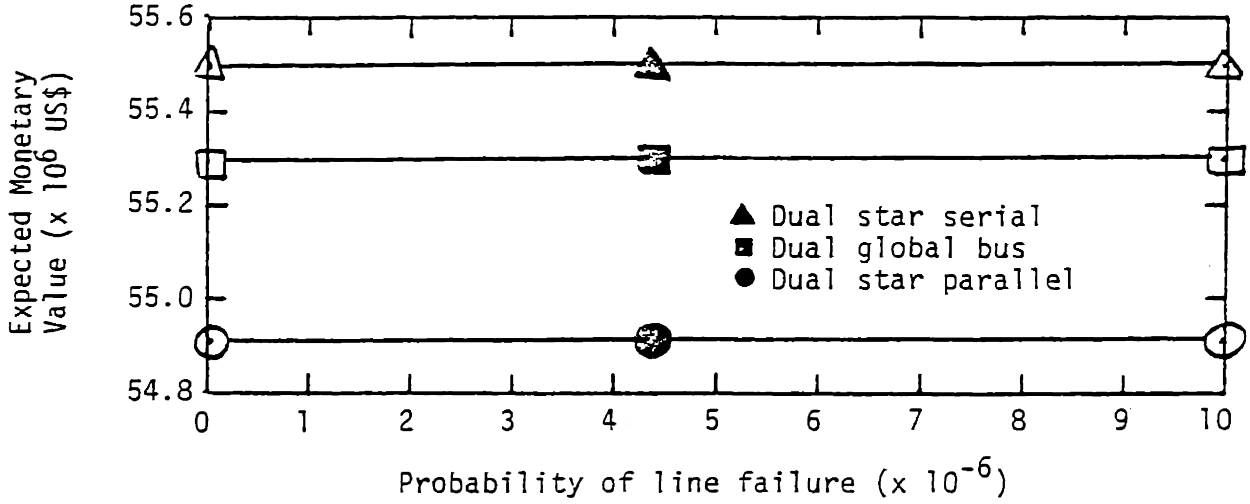


Figure 2.10.7 EMV sensitivity to probability of line failure (situation one).

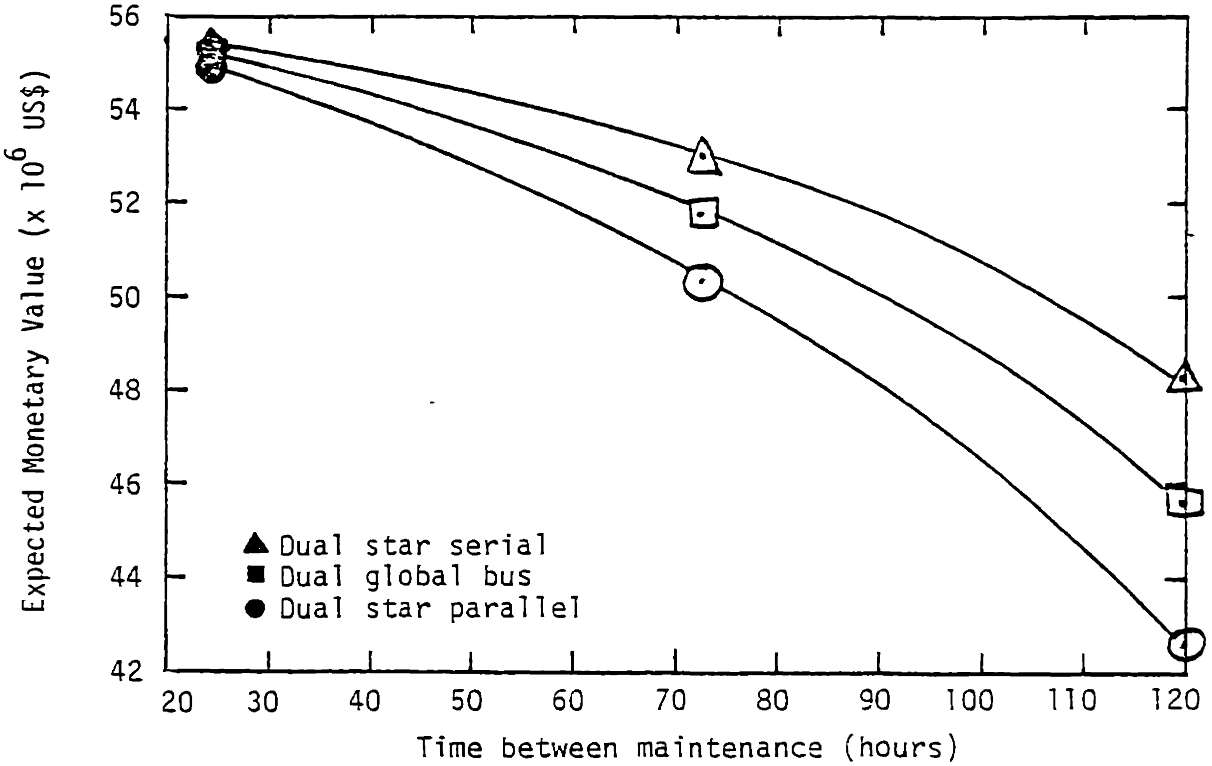


Figure 2.10.8 EMV sensitivity to time between maintenance policy (situation one)

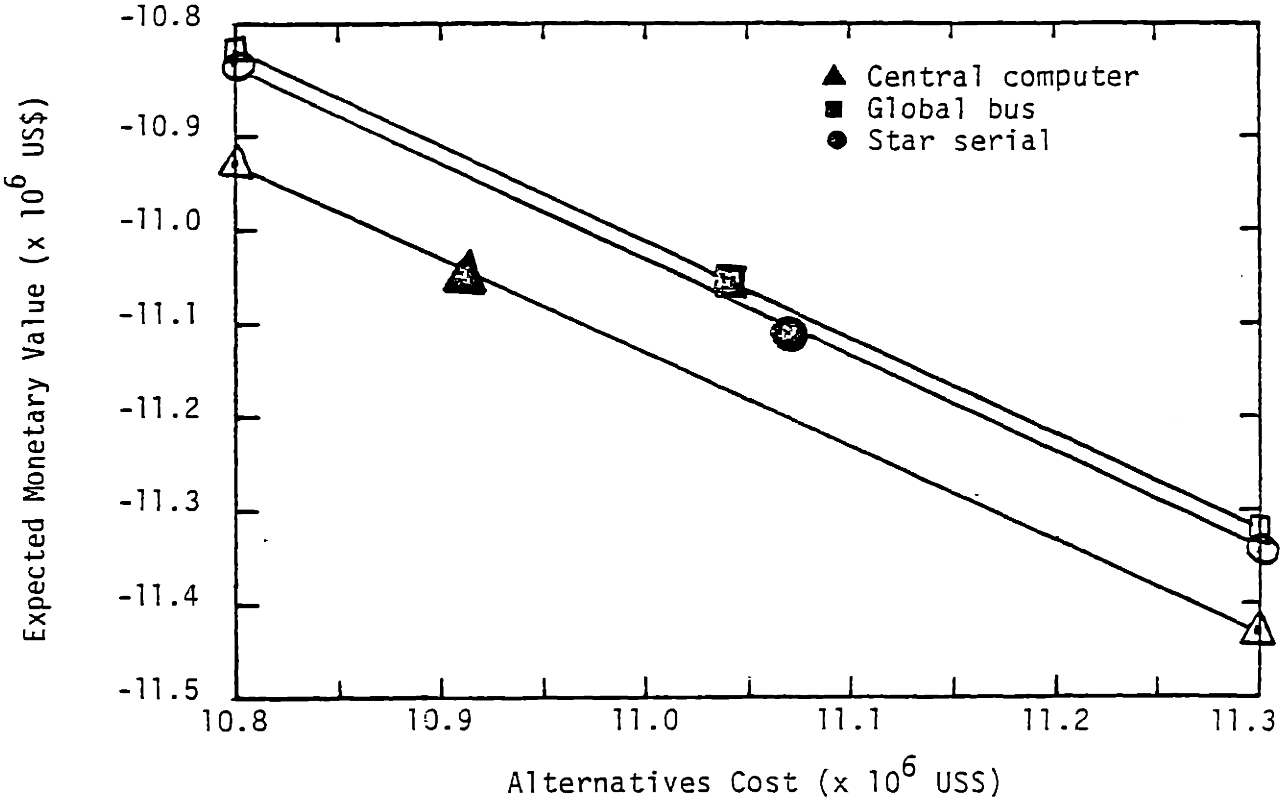


Figure 2.10.9 EMV sensitivity to alternative cost (situation two).

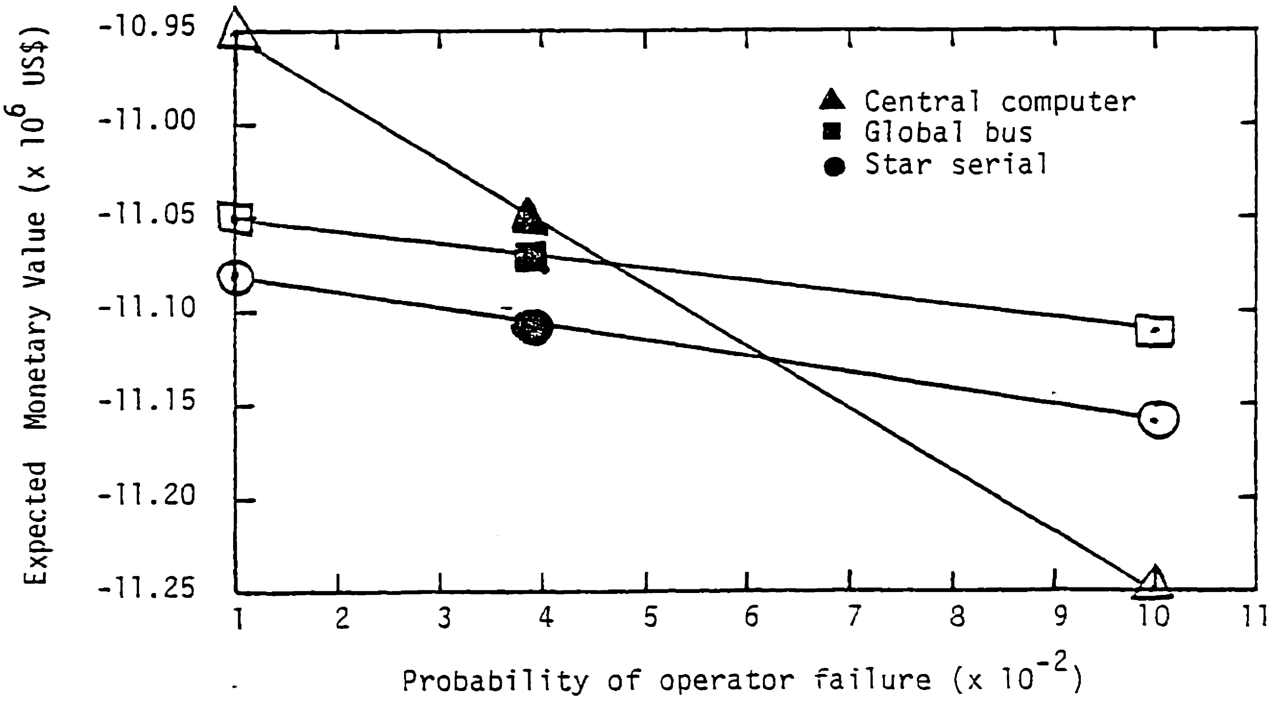


Figure 2.10.10 EMV sensitivity to operator failure (situation two).

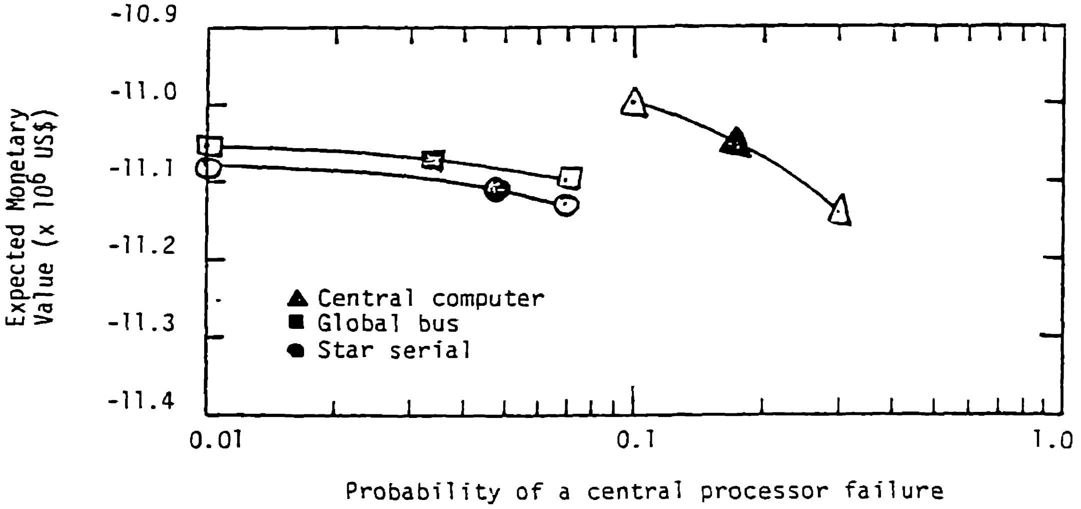


Figure 2.10.11 EMV sensitivity to a central processor failure (situation two)

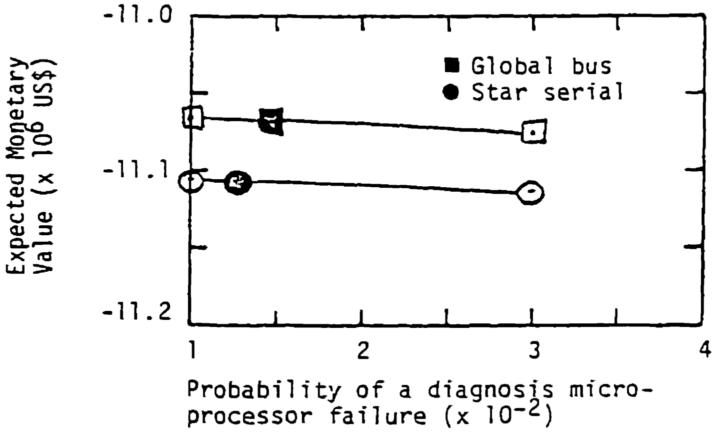


Figure 2.10.12 EMV sensitivity to a diagnosis microprocessor failure (situation two)

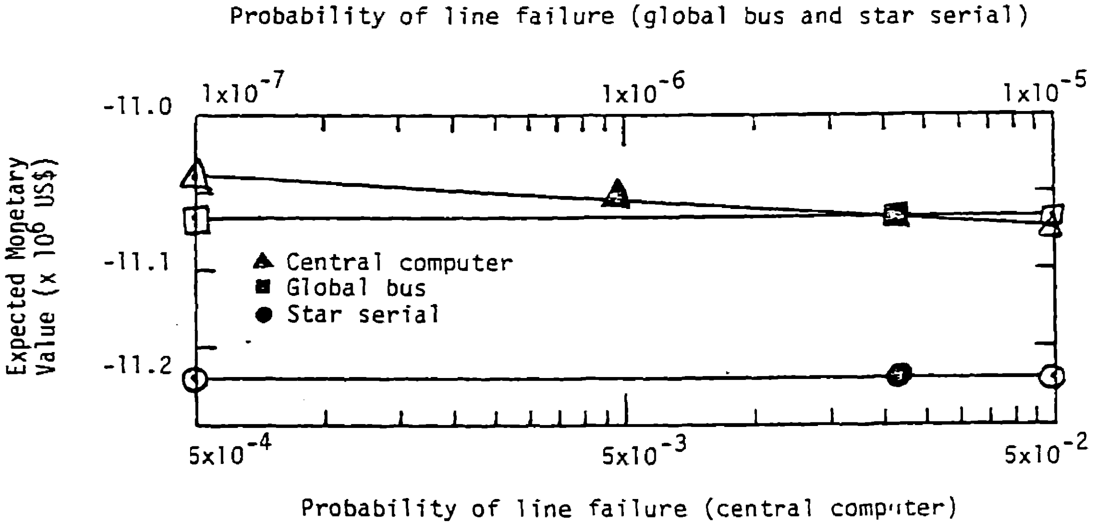


Figure 2.10.13 EMV sensitivity to line failure (situation two).

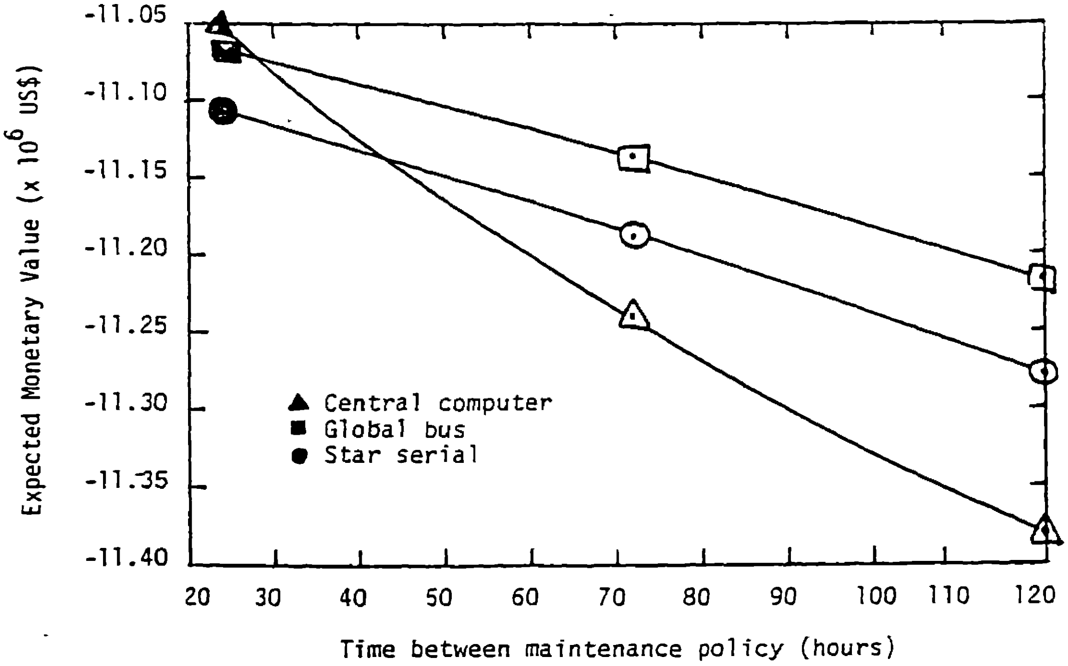
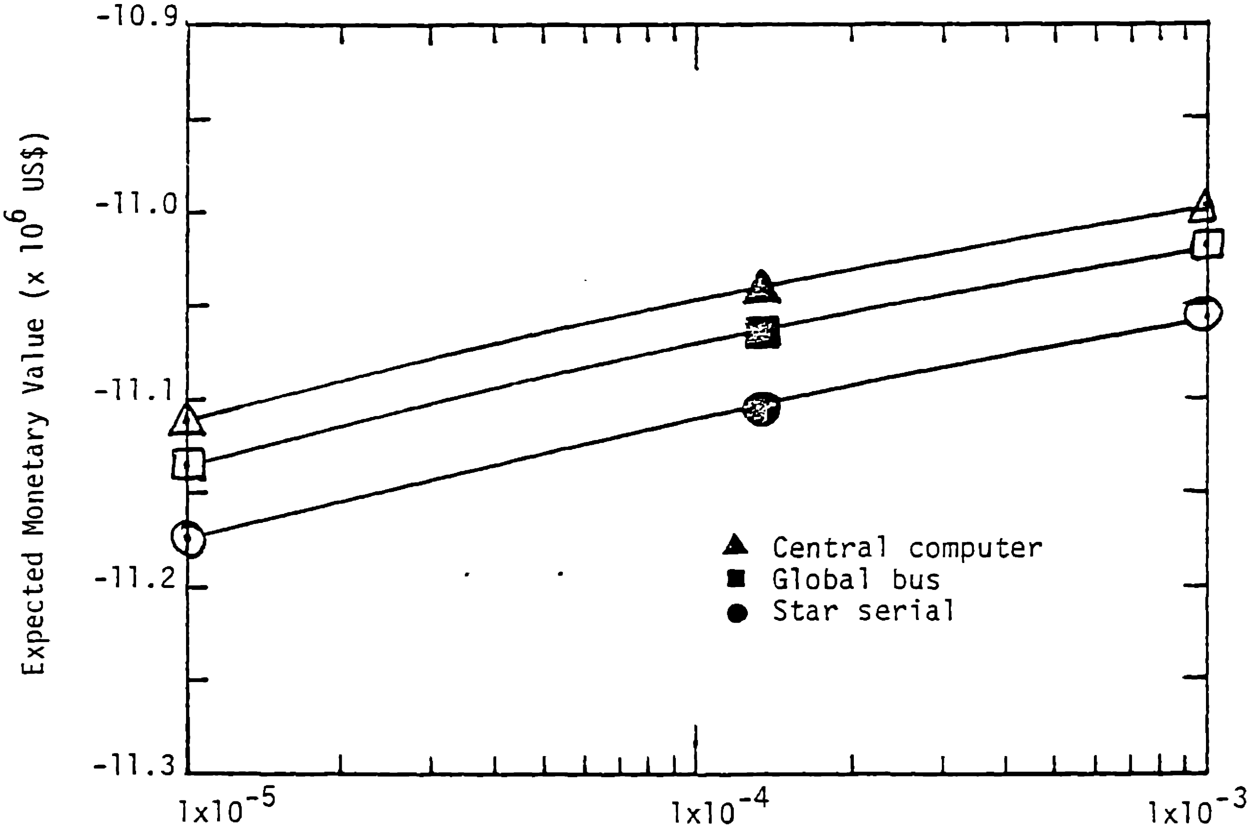


Figure 2.10.14 EMV sensitivity to time between maintenance policy (situation two)



Probability of software failure

Figure 2.10.15 EMV sensitivity to software failure (situation two).

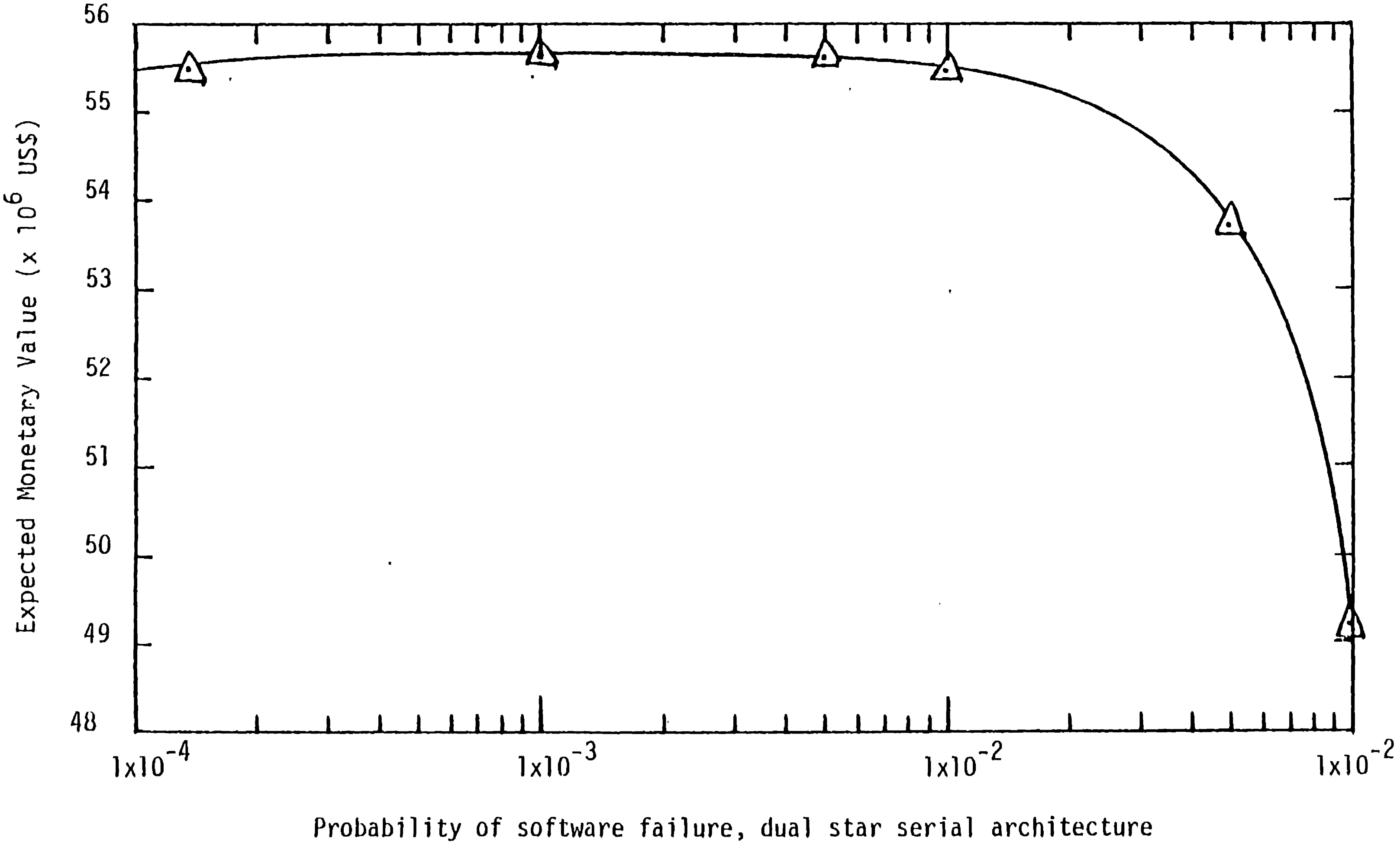


Figure 2.10.16 EMV sensitivity to probability of software failure, dual star serial architecture (situation one).

curve reaches the left side of the graph, the marginal improvement in probability of software success is outweighed by the marginal cost to reach that improvement.

5. If the probability of success is regarded alone as a figure of merit, the dual star serial architecture is also the winner.
6. If the cost alone is regarded as a figure of merit, the central computer architecture would be the winner.

2.10.2.2 SITUATION TWO

1. From the figure of merit viewpoint, the winner is the central computer architecture.
2. When the sensitivity studies are considered, the only curve in which the central computer architecture keeps its supremacy is with P(soft) variations.
3. Figure 2.10.9 tells us that for the same cost the central computer architecture runs in third place.
4. Figure 2.10.10 shows that the higher the operator training, the more preferable the central computer. On the other hand, the lower the operator training the more preferable the distributed alternatives.
5. Because of the huge amount of cables involved with the central computer alternative, the higher the probability of a cable failure, the more attractive become the distributed alternatives. Figure 2.10.13 proves that point, and it should be noted that there is a general lack of sensitivity to the

cable failure.

6. The time between maintenance policy is critical in the selection process for situation two. The central computer architecture shows great sensitivity to this parameter. This being the case, the central computer architecture keeps its supremacy over the global bus only in the range from 0 to 48 hours time between maintenance.

2.10.2.3 BOTH SITUATIONS

If one architecture should be selected for each situation, the star serial is the clear choice for automatic controlling purposes (situation one).

In the case of data validation, surveillance, diagnostic and operator adivising function (situation two), it is not so clear. Considering first the costs, it is unlikely they could change relative positions because the costs are reasonably accurate. If the costs do not change relative positions, the expected conclusion from Figure 2.10.9 is the central computer architecture still is the winner.

In the second place the question arises about the time between maintenance. Twenty-four hours can be a reasonable time range for shore-based power plants, but at sea the environment often gets rough and such a strict maintenance policy could not be kept up easily. The great sensitivity to T_{maint} changes makes the central computer unattractive to marine applications.

In the third place is the sensitivity to operator failures. The number used to calculate the base case is the estimated probability per action for one operator in normal conditions. In accident situations, this number varies from 10^{-3} to 10^{-2} per action. Under the same assumption of 10 actions per hour on four-hour duty. The probability of making a mistake increases from .04 to approximately 0.33. The latter places the central computer far below the distributed alternatives.

For all the reasons explained above, even though the central computer is the winner in the base case, the sensitivity studies pointed out the global bus (second winner) would be a better choice for diagnosis, data validation, surveillance, and operator advice.

But the main problem is that typically the digital system will be wanted to handle both situations. Making the best choice then is a matter of trade-offs between the dual star serial and global bus architectures, and the final decision has much to do with the personal risk attitude of the decision maker, assuming he has a risk averse behavior, the choice has to be the dual star serial architecture which has the best performance in condition one, and in both situations, the dual star serial offers the lowest probability of failure.

REFERENCES

2.1 Distributed, hierarchical process control, functions before form. Dennis J. Trchka and Raymond H. Ash, ISA, 1978.

2.2 Requirements and concepts for a nuclear plant surveillance and diagnostic system. P.J. Nicholson and D.D. Lanning. IAEA Meeting on Distributed Computer Systems for Nuclear Power Plants, Chalk River, Ontario, Canada, May 14, 1980.

2.3 Large systems are in control. Richard Merritt. Instruments and Control Systems, November 1978.

2.4 Distributed-processor communications architecture. Kenneth J. Thurber and Gerald M. Masson. D.C. Heath and Company, 1979.

2.5 Computer control at Bruce nuclear generating station. D.J. Morris. Nuclear Safety, vol. 15, no. 6, 1974.

2.6 Application of Pickering experience to future condition nuclear power stations. E.M. Yaremy and D.E. Anderson, IAEA-SM-168/A-8.

2.7 Control and instrumentation on nuclear power plants. A. Pearson. IAEA-PL-431/2, 1972.

2.8 Reliability and maintainability of electronic systems. J.E. Arsenault and J.E. Roberts. Computer Science Pres, 1980.

2.9 Nuclear merchant ship reactor, final safeguards report. Volume I, description of the N.S. Savannah, BAW-1164 (Vol. I).

2.10 Reactor safety study, WASH-1400 (NUREG-75/D14).

2.11 On-line power plant and disturbance analysis system. EPRI NP-613, Project 891, February 1978.

CHAPTER 3

MODEL OF N.S. SAVANNAH NUCLEAR REACTOR PRESSURIZER

3.1 INTRODUCTION

As we stated in Chapter 2, one of the closed feedback control loops that the system has to have is the pressure and volume control at the pressurizer. The design process will go further taking this loop and making a new design which introduces a digital processor as a controller. This example has the aim of presenting a method which can be used later on in other loops. The pressure and volume control loop will be redesigned and the pressure and level responses will be analyzed by digital simulation.

Because it is intended to isolate the control problem from the data validation problem which is the subject of another thesis, it will be assumed that all the data coming to the controller have been previously validated by the appropriate data validation process.

A detailed description of the N.S. Savannah pressurizer is given in Appendix I. More information can be found in references 3.1 and 3.2.

3.2 MATHEMATICAL MODEL FOR THE PRESSURIZER

One of the most important considerations that should be made when modeling a system is the exact degree of compromise between the accuracy and the algorithm size. The required compromise is even more important in this case because if microprocessors are to be chosen for the job, they are always limited in their processing capability. Thus, a mathematical model has to be developed for the pressurizer with a balance between accuracy and complexity. The chosen model is the "two control volumes approach." This model consists of:

- steam volume
- water volume.

The spray effect on the steam volume will be taken as a direct contact heat exchanger. The heat exchanger takes a steam flow w_c from the steam volume and adds a water flow ($w_c + w_{sp}$) to the water volume. This approach has been previously used in references 3.3, 3.4, and 3.5.

3.2.1 STEAM CONTROL VOLUME

The steam control volume has the following variables (see Figure 3.2.1.a).

Input variable:

- flashing flow (w_{fl}) produced by evaporation from the water volume

Output variables:

- mechanical work ($P\dot{V}s$) at the control volume interfaces,
- heat leakage (Q_{ws}) through the pressurizer wall,
- steam flow condensing by the spray (w_c)
- steam flow condensing at the wall (w_r)
- steam flow escaping through the relief valve (w_{re}).

The steam control volume and its corresponding variables are shown in Figure 3.2.1.a.

The next logical step is to apply mass conservation and energy conservation laws to the steam volume.

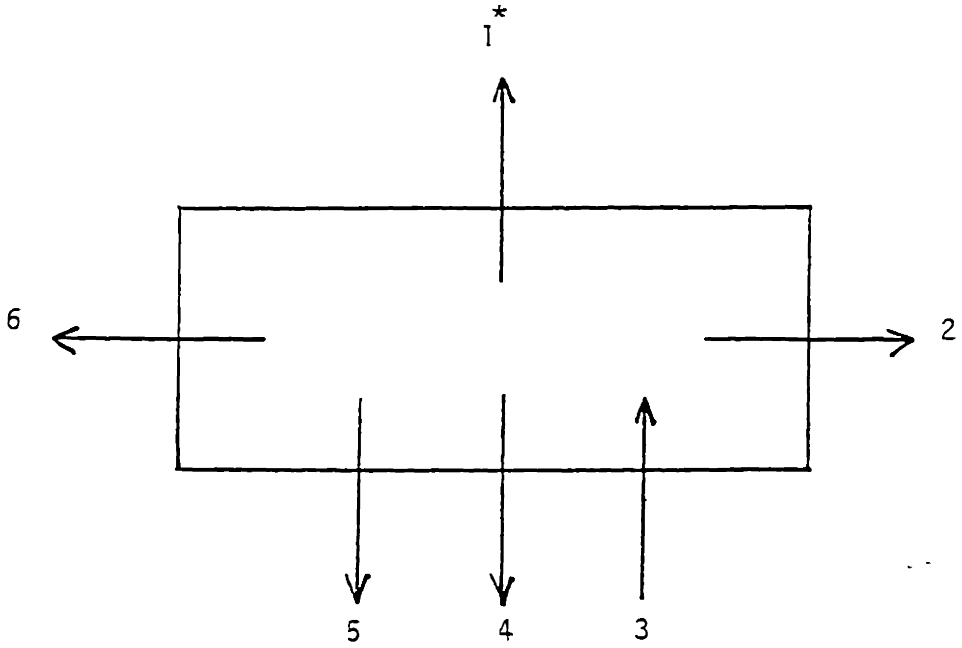


Figure 3.2.1a Steam control volume.

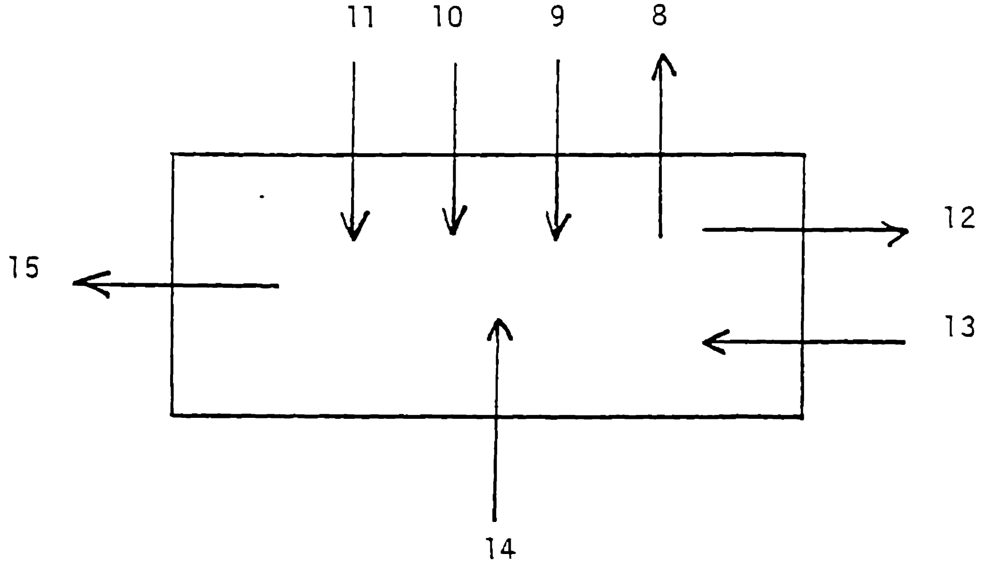


Figure 3.2.1b Water control volume.
*See legend on next page.

1. W_{re} h_{re}
2. Q_{ws}
3. w_{fl} h_{fl}
4. w_e h_s
5. w_r h_s
6. $P\bar{V}_s$
8. w_{fl} h_{fl}
9. w_r h_r
10. w_e h_e
11. w_{sp} h'_{sp}
12. Q_{ww}
13. Q_h
14. w_{su} h_{su}
15. $P\bar{V}_w$

The following nomenclature will be used in developing the equations:

w_{re}: relief steam flow

h_{re}: relief steam enthalpy

Q_{ws}: heat leakage through the wall

V_s : steam control volume

P : pressure

w_c : steam flow condensed by spray

w_r : steam flow condensed at the wall

w_{fl}: flashing flow

h_{fl}: flashing flow enthalpy

M_s : steam mass

h_s : steam enthalpy

U_s : steam internal energy

V_w : water volume

Q_h : heat supplied by the heaters

h_c : condensed water enthalpy, just when it reaches the water volume

w_{su}: surge flow from the primary system

h_{su}: surge flow enthalpy

h_r : natural condensed water enthalpy, just when it reaches the water volume

M_w : water mass

h_w : water enthalpy

U_w : water external energy

w_{sp}: spray flow

h'_{sp}: spray flow enthalpy, just when it reaches the water volume

h_{sp}: spray flow enthalpy at the nozzle

All the variables are in System International (SI) units.

Mass balance:

$$\dot{M}_s : w_{fl} - w_{re} - w_c - w_r \qquad (3.2.1)$$

Energy balance:

$$\dot{U}_s : w_{fl}h_{fl} - w_{re}h_{re} - w_c h_s - w_r h_s - Q_{ws} - P\dot{V}_s \qquad (3.2.2)$$

3.2.2 WATER CONTROL VOLUME

The water control volume has the following variables (see Figure 3.2.1.b).

Input variables

- spracy water flow (w_{sp})
- steam flow condensed by the spray (w_c)
- natural condensation of the wall (w_r)
- heaters total power (Q_h)
- surge flow from the primary system (w_{su})

Output variables

- mechanical work at the control volume interfaces ($P\dot{V}_w$)
- heat leakage (Q_{ww}) through the pressurizer wall,
- flashing flow (w_{fl})

The water control volume and its variables are shown in Figure 3.2.1.b.

In order to solve the water volume equations, a few assumptions have to be made: the pressure field is assumed to be homogeneous (gravity effects are neglected), and the travel time of the spray water and the condensed water through the steam volume is negligible.

Mass balance:

$$\dot{M}_w = w_{sp} + w_c + w_r + w_{su} - w_{fl} \tag{3.2.3}$$

Energy balance:

$$\dot{U}_w = w_{su}\, h_{su} + w_r h_r + Q_h - w_{fl} h_{fl} - Q_{ww} - P\dot{V}_w \tag{3.2.4}$$

Finally, because the pressurizer has a total constant volume

$V_s + V_w$ = constant

and hence the volumetric time derivative becomes:

$$\dot{V}_s + \dot{V}_w = 0 \tag{3.2.5}$$

3.3 STATE EQUATIONS FOR THE PRESSURIZER

So far the equations developed in Section 3.2 are general, with only a few assumptions. In order to decrease the size of these equations and make the problem more tractable, further assumptions within a reasonable framework will be stated as follows:

- The natural condensation flow is taken to be negligible ($w_r \simeq 0$)
- the relief steam flow is only present when the relief valve opens; then under normal conditions $w_{re} = 0$
- the relief steam flow has the same enthalpy as the steam volume

$(h_{re} = h_s)$

- the heat leakage through the wall is taken to be negligible $(Q_{ws} = Q_{ww} = 0)$
- the condensed steam flow exists only if the spray flow is acting i.e., $w_{sp} = 0$ implies $w_c = 0$
- the flashing enthalpy is approximately equal to the saturated steam at the pressurizer pressure

  $(h_{fl} \simeq h_g(P))$
- the condensed water enthalpy is approximately equal to the saturated water enthalpy at the pressurizer pressure

  $(h_c \simeq h_f(P))$
- a perfect and instantaneous mixture between an insurging primary water and the pressure water is assumed.

Now, from the viewpoint of the assumptions, the pressurizer behavior will be analyzed for three conditions.

- insurge condition
- outsurge condition
- quasi-steady state condition.

3.3.1 INSURGE CONDITION

In order to analyze the insurge condition, the system will be assumed at equilibrium. The equilibrium condition is defined initially as a state where the water volume and the steam volume exist as a saturated element and no changes in either pressure or level are present.

A subcooled water inflow (insurge) from the primary system generates a compression in the steam region, bringing it to a higher pressure state. At the same time, the mixture between the subcooled insurge water and the saturated pressurizer water brings the water volume to a subcooled state. Two effects are present now:

- the subcooled water does not generate flashing steam
- the rise in pressure is controlled by putting the sprays into action.

Therefore, the general equations undergo the following change:

$$\dot{M}_s = - w_{re} - w_c \tag{3.3.1}$$

$$\dot{M}_w = w_{sp} + w_c + w_{su} \tag{3.3.2}$$

$$\dot{U}_s = w_{re}\, h_s - w_c h_s - P\dot{V}_s \tag{3.3.3}$$

$$\dot{U}_w = w_{su}\, h_{su} + w_{sp} h'_{sp} + w_c h_c + Q_h - P\dot{V}_w \tag{3.3.4}$$

$$\dot{V}_s + \dot{V}_w = 0 \tag{3.3.5}$$

Note that w_{re} is different from zero only if the relief valve opens.

3.3.2 OUTSURGE CONDITION

As in the previous calculations the analysis is started at the equilibrium condition. A volume decrease in the primary systems originates a water outflow (outsurge) from the pressurizer. The reduction of water volume inside the pressurizer induces a steam expansion. This expansion produces a two-phase region in the steam volume, also the reduced pressure causes a two-phase region in the water volume.

The two-phase region in the water volume involves a natural flashing flow and the two-phase region in the steam volume involves a natural condensation.

Finally, the steam expansion, which is related with a pressure decrease, precludes any spray valve opening.

The general equations take the following form:

$$\dot{M}_s = w_{fl} \tag{3.3.6}$$

$$\dot{M}_w = w_{su} - w_{fl} \tag{3.3.7}$$

$$\dot{U}_s = w_{fl}\ h_{fl} - \ P\dot{V}_s \tag{3.3.8}$$

$$\dot{U}_w = w_{su}\ h_{su} + w_{fl} h_{fl} + Q_h - P\dot{V}_s \tag{3.3.9}$$

$$\dot{V}_w + \dot{V}_s = 0 \tag{3.3.10}$$

The outsurge condition has its own special characteristics:

- the water presents a quality gradient
- part of the heat generated by the heaters is lost to the primary system.

3.3.3 QUASI-STEADY STATE CONDITION

By definition this condition is only related with small pressure changes around the equilibrium point. Therefore the pressurizer is in a quasi-steady state condition when both water and steam are very near to their saturated state (saturated conditions corresponding to the actual pressure).

Under the quasi-steady state condition, the relief valve never opens and the spray valve and the heaters work intermittently. A graphic approach for the model in quasi-steady state is displayed in Figure 3.3.1.

The general equations take the following form:

$$\dot{M}_s = w_{fl} - w_c \qquad (3.3.11)$$

$$\dot{M}_w = w_{sp} + w_c + w_{su} - w_{fl} \qquad (3.3.12)$$

$$\dot{U}_s = w_{fl}\ h_{fl} - \ w_c h_s - P\dot{V}_s \qquad (3.3.13)$$

$$w_{sp}h_{sp} + w_c h_s = w_c h_c + w_{sp}h'_{sp} \qquad (3.3.14)$$

$$\dot{U}_w = w_{su}\ h_{su} - \ w_c h_c + w_{sp}h_{sp} - w_{fl}h_w - P\dot{V}_w \qquad (3.3.15)$$

$$w_{fl}h_{fl} + w_{fl}h_w + Q_h \qquad (3.3.16)$$

$$\dot{V}_w + \dot{V}_s = 0 \qquad (3.3.17)$$

Replacing (3.3.16) into (3.3.15) we have

$$\dot{M}_w = w_{su}h_{su} + w_c h_c + w_{sp}h'_{sp} - w_{fl}h_{gl} + Q_h - P\dot{V}_w \qquad (3.3.18)$$

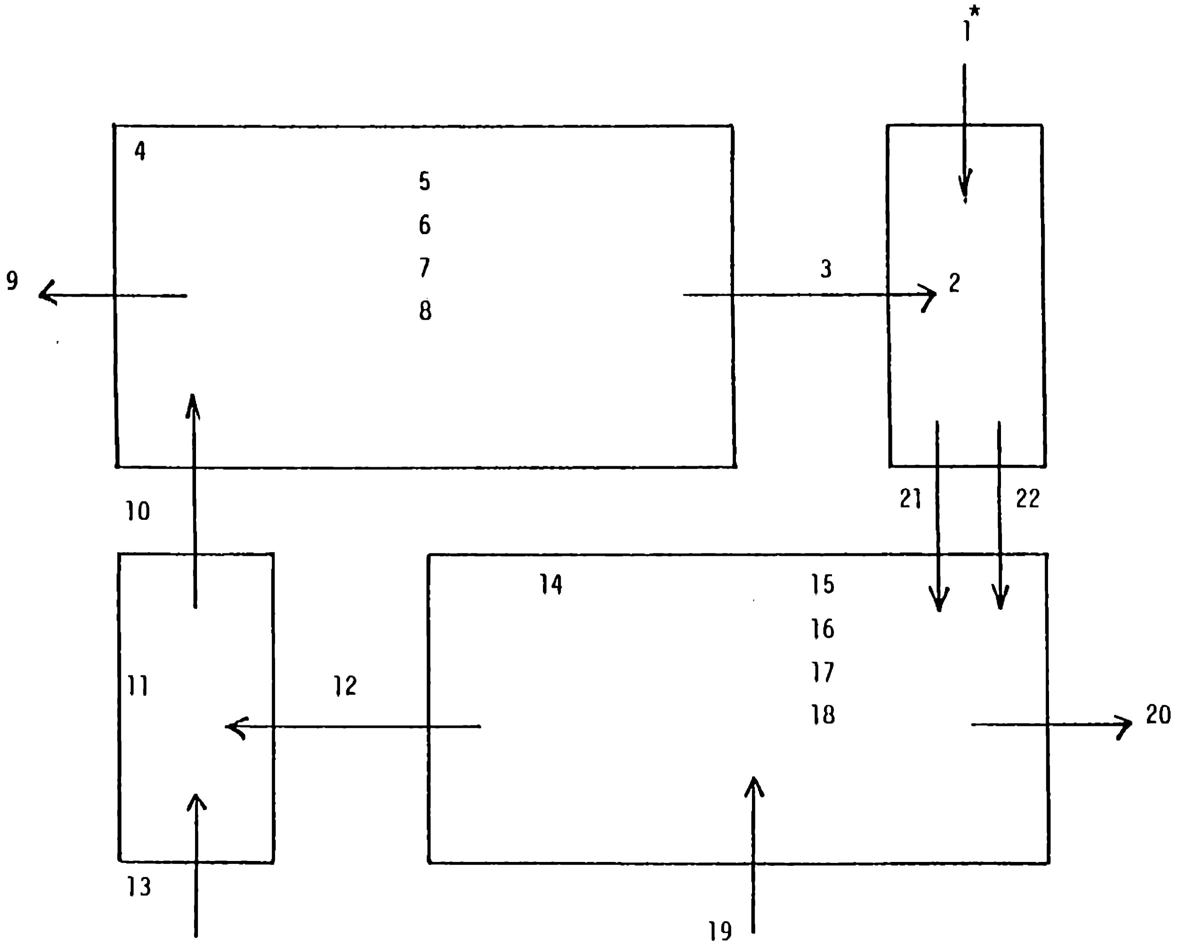


Figure 3.3.1 Quasi steady state model.
*See legend on next page.

1. w_{sp}, h_{sp}
2. Heat exchanger
3. W_e, h_s
4. Steam volume
5. M_s
6. h_s
7. V_s
8. U_s
9. $P\bar{V}_s$
10. w_{fe}, h_{fe}
11. Heat exchanger
12. w_{fe}, h_w
13. Q_h
14. Water volume
15. M_w
16. h_w
17. V_w
18. V_w
19. w_{su}, h_{su}
20. $P\bar{V}_w$
21. w_{sp}, h'_{sp}
22. w_c, h_c

Equations (3.3.11), (3.3.12), (3.3.13), (3.3.14), (3.3.17), and (3.3.18) make up a complete set for describing the pressurizer in a quasi-steady state condition.

An extra assumption made for this model is to consider a 100 percent efficient spray nozzle, e.g., the spray flow is homogeneous and overs the whole steam volume.

Also it is very common (Ref. 3.3) to assume the spray enthalpy when it reaches the water volume (h_{sp}) has approximately the same value as the condensed water enthalpy (h_c), e.g.,

$$h_{sp} = h_c.$$

This means equation (3.3.14) changes to

$$w_{sp}h_{sp} + w_c h_s = w_c h_c + w_{sp}h_c \tag{3.3.19}$$

The set of assumptions made for the model deserves the following comments:

- Because the system is at quasi-steady state condition, all the thermodynamic variables can be assumed close to their saturated values

$$h_c \simeq h_w \simeq h_f(P) \tag{3.3.20}$$

$$h_{fl} \simeq h_s \simeq h_g(P) \tag{3.3.21}$$

- Natural flashing and natural condensation are ruled by the following expressions:

$$w_{fl} = \frac{h_f(P) - h_w}{h_{fg}(P)} M_w$$

$$w_c = \frac{h_s - h_g(P)}{h_{fg}(P)} M_c$$

Making use of equation (3.3.21) w_c can be neglected. On the other hand, w_{fl} is a function of M_w and M_w is a large number. Therefore w_{fl} cannot be assumed equal to zero, and a correction has to be included in the model.

- Unde the near steady state condition the only source for flashing is the heat supplied by the heaters. Replacing (3.3.21) into (3.3.16) we have

$$w_{fl} = \frac{Q_h}{h_{fg}} \tag{3.3.22}$$

The last three assumptions are very good under quasi steady state conditions, but the farther the model gets from this condition, the worse the model behaves.

- Also the perfect mixture assumption introduces a source of inaccuracy, especially during insurges. On the other hand, it is expected the model will behave fairly well during outsurge conditons, provided the transient is not very fast.

- Because the reactor plant has a system to vent the non-condensable gases, the effect of these gases will be neglected.

- Heat transfer through the control volume interface is also neglected.

- Finally, when the pressurizer is subjected to an outsurge regime, it is assumed that all the heat supplied by the heaters remains within the water volume.

3.3.4 ANALYTIC FORMULATION

Besides the need for a small algorithm, the use of the quasi steady state condition is justified for the following reason: from the scope of this thesis, a model of the pressurizer is required as a substitute of it during the process of designing the related control system. Once the design is finished, the control elements are placed inside the real plant, and then a final turning is made.

Also the pressurizer equations are by themselves complex. Introducing the feedback equations related with the control system makes the situation even more complicated. Therefore in order to reduce the problem to a tractable level, it is customary to linearize the plant as far as possible without losing its peculiar characteristics. The quasi-steady state condition accomplishes both requirements.

Because it is required for this work to state clearly the origin of the equations used later on, a full explanation of their development follows:

3.3.4.1 STATE EQUATIONS FOR THE QUASI STEADY STATE CONDITION

The basic equations already developed are:

$$\dot{M}_s = w_{fl} - w_c \tag{3.3.11}$$

$$\dot{M}_w = w_{sp} + w_c + w_{su} - w_{fl} \tag{3.3.12}$$

$$\dot{U}_s = w_{fl}\, h_{fl} - w_c h_s - P\dot{V}_s \tag{3.3.13}$$

$$\dot{M}_w = w_{su}h_{su} + w_c h_c + w_{sp}h_c - w_{fl}h_{fl} + Q_h - P\dot{V}_w \qquad (3.3.23)$$

$$w_{sp}h_{sp} + w_c h_s = w_c h_c + w_{sp}h_c \qquad (3.3.19)$$

$$\dot{V}_w + \dot{V}_s = 0 \qquad (3.3.17)$$

The process that follows is detailed by a rather lengthy account of the steps required to reach the state equation for pressure. Such a process is shown in Appendix G. From Appendix G, the state equation for pressure is:

$$\dot{P} = \frac{-(w_{fl} - w_c)v_s(w_{sp} + w_c - w_{su} - w_{fl})v_f - \frac{dv_f}{dh_f} w_{su}(h_{su} - h_f)}{M_g(\frac{dv_g}{dh_g} v_g + \frac{dv_g}{dP}) + M_f(\frac{dv_f}{dN_f} v_f + \frac{dv_f}{dP})} \qquad (3.3.24)$$

Equation (3.3.24) is the quasi steady state model of the pressure inside the pressurizer. The next step is to linearize the thermodynamic parameters about a set point. This step is taken as a way to simplify the process memory requirements that will imply to introduce the actual steam tables.

By using a linear regression technique plus the data given in Ref. 3.6, the thermodynamic parameters were obtained as a linear function of the pressure. The following linearized expressions are valid between 11[MPa] and 13 [MPa]. The working point is 11.93 [MPa].

$$[\frac{dv_g}{dh_g}]_p = 3.63 \times 10^{-8} - 1.55 \times 10^{-9}P \qquad (3.3.25)$$

$$[\frac{dv_g}{dP}]_h = -4 \times 10^{-9} + 2.3 \times 10^{-10}P \tag{3.3.26}$$

$$[\frac{dv_f}{dh_f}]_P = -1.57 \times 10^{-10} + 1.05 \times 10^{-10}P \tag{3.3.27}$$

$$[\frac{dv_f}{dP}]_h = 4.25 \times 10^{-12} - 8.3 \times 10^{-13} P \tag{3.3.28}$$

$$h_g = 2942.2 - 21.5 P \tag{3.3.29}$$

$$h_f = 1001.5 + 40.9 P \tag{3.3.30}$$

$$h_{fg} = 1940.7 - 62.4 P \tag{3.3.31}$$

$$v_g = 3.35 \times 10^{-2} - 1.60 \times 10^{-3} P \tag{3.3.32}$$

$$v_f = 1.06 \times 10^{-3} + 3.91 \times 10^{-5} P \tag{3.3.33}$$

P is measured in $[MP_a]$.

3.3.4.2 FLASHING AND CONDENSATE FLOW EQUATIONS

Starting from the quasi steady state condition, the equations are:

$$Q_h = w_{fl} h_{fg} \tag{3.3.22}$$

and

$$w_c(h_g - h_f) = w_{sp}(h_f - h_{sp}) \tag{3.3.34}$$

The condensate flow is:

$$w_c = \frac{w_{sp}(h_f - h_{sp})}{h_{fg}} \tag{3.3.35}$$

It is worth noting that the condensate flow exists only when spray flow exists. The flashing flow is:

$$w_{fl} = \frac{Q_h}{h_{fg}} \qquad (3.3.22)$$

As explained, the quasi steady state assumption does not allow a natural flashing produced by a two-phase condition in the water volume. But the natural flashing is a function of the water mass, and this mass is a large number. Therefore even if h_w is roughly equal to h_f, the natural flashing could be significant. Because of that, the quasi steady state assumption will be relaxed, and a correction taking the natural flashing into account will be included.

From Reference 3.3:

$$w_{fl} = \frac{X_{fl}M_f}{T} [1 - \exp(\frac{\alpha T}{\tau})] \qquad (3.3.36)$$

where

$$X_{fl} = \frac{h_w - h_f}{h_{fg}}$$

M_t = water mass (kg)

T = integration time (numerical algorithm)

τ = rising time for the bubble (5 sec)

α = compressor speed factor = $\frac{w_{su}(t)}{w_{su}(max)}$

Making a series expansion and taking the first terms

$$w_{fl_{nat}} = \frac{X_{fl}M_f\alpha}{\tau}$$

From reference 3.1, $w_{su}(max) = 15.62$ [kg/s]

$$w_{fl_{nat}} = \frac{h_w - h_f}{h_{fg}} \cdot M_f \cdot \frac{w_{su}(t)}{78.1} \qquad (3.3.37)$$

Note that this equation is more elaborate than the ideal equation stated in Section 3.3.1, because it considers the bubble delay time and the effect of the compression speed.

3.3.4.3 SURGE FLOW EQUATIONS

In order to simplify the mathematical treatment, but without losing generality, it will be assumed that any change in primary water volume will be immediate noticed as a water volume change in the pressurizer. The assumption is based on the incompressibility of the water.

Thus, the surge flow is represented by the following equation:

$$w_{su} = w_{mak} + w_p - w_{let} \qquad (3.3.38)$$

where

w_{su} = surge flow, the positive sign corresponds to an insurge flow

w_{mak} = water flow coming from the buffer seals system. This water is used for making up the pressurizer water level

w_{let} = water flow leaking from the primary circuit to the letdown coolers system. It is used for lowering the pressurizer water level

w_p = water flow due to thermal expansion or thermal contractions of the water in the primary circuit.

3.4 CONTROL SYSTEM MODEL

Up to this point, the linearized equations modeling the pressurizer have been developed but the pressurizer vessel is only one device among several on the pressurizer system. All these components have the task of keeping the primary pressure around an operating set point. Therefore it is also necessary to know the equations ruling all elements making up the pressure control system.

In this section we describe the system for controlling the pressure. After that, the whole system will be modeled in a block diagram, and finally the particular equations for the N.S. Savannah plant will be developed.

3.4.1 CONTROL SYSTEM DESCRIPTION

The following description corresponds to the pressure and primary volume control furnished to the N.S. Savannah nuclear propulsion plant. A few devices have been redesigned in order to update the technology but all the changes were kept within the operational requirements.

Figure 3.4.1 shows a simplified diagram with all the devices related to the pressure and level control process.

The pressure signal is detected by a pressure sensor, then it is transformed to an electrical signal and sent to the processor. The processor compares the incoming signal with the reference signal and decides to put into action the corresponding actuator. If the pressure is over the reference the spray valve has to be opened. On the other hand, if the pressure is under the reference the heaters have to be

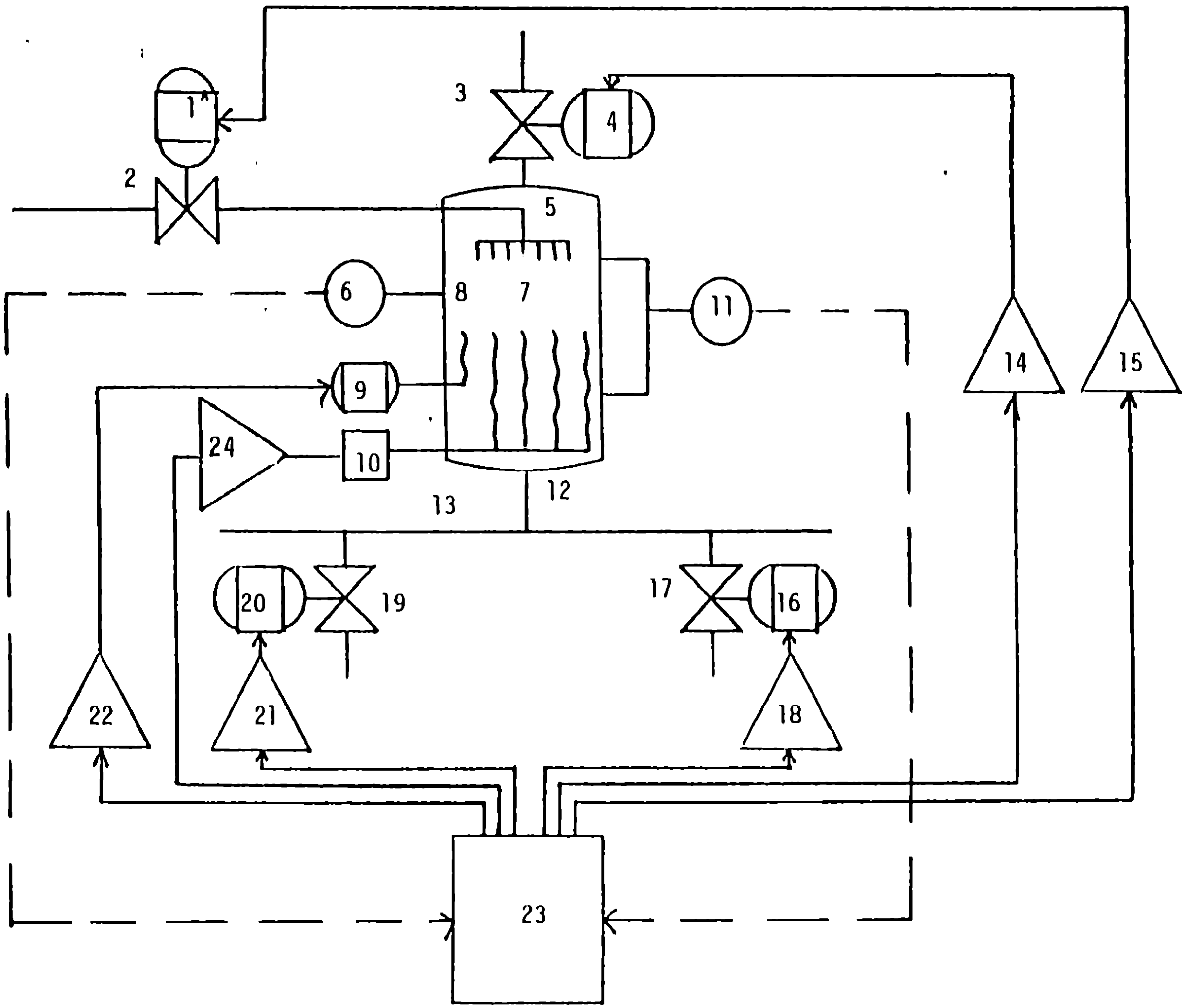


Figure 3.4.1 Pressure and volume control system.
*See legend on next page.

1. Spray valve motor
2. Spray valve
3. Relief valve
4. Relief valve motor
5. Spray nozzle
6. Pressure sensor
7. Hysteresis heaters
8. Proportional heater
9. Motor and rheostat for the proportional heater
10. Hysteresis heater relays
11. Level sensor
12. Surge line
13. Primary circuit
14. Relief valve amplifier
15. Spray valve amplifier
16. Makeup valve motor
17. Makeup valve
18. Makeup valve amplifier
19. Letdown valve
20. Letdown valve motor
21. Letdown valve amplifier
22. Proportional heater amplifier
23. Processor
24. Relay amplifier

activated.

If the first situation is the case, the processor sends a signal to the spray system. This signal is first ampified, and then it activates the spray valve DC motor. In the second case the control signal is also ampified and then it activates the heater relays (the proportional heaters have a DC motor).

The level control process follows a similar pattern. The level signal is detected by a level sensor; this is transformed into an electrical signal and sent to the processor. The processor compares the incoming signal with the reference signal and makes the decision between opening the make-up valve or the letdown valve. In either case, the processor sends a signal, the signal is amplified, and then it activates the corresponding DC motor valve.

Two comments should be made: the complete and detailed description of the old pressure control system is in references 3.1 and 3.2; the original system has not a complete level control system. The plant was designed to keep the level within the operating range by using an automatic make-up water system, but it has no automatic letdown water system. A complete level control system is added in this work in order to have an entire package, able to be used in nuclear power plants with only minor modifications.

3.4.2 BLOCK DIAGRAM REPRESENTATION OF THE CONTROL SYSTEMS

To develop the block diagram representation, the equations stated in Section 3.3 and the description in Section 3.4.1 will be used. The work is now focused at a component level, analyzing each device in detail. Figure 3.4.2 shows the relationship between the different blocks making up the control system. From Figure 3.4.2 it is noted that the forcing signal comes from the value of w_p (w_p is the water flow due to volume changes in primary circuit caused by temperature changes).

Each block will be analyzed in the following section.

3.4.3 TRANSFER FUNCTIONS

The blocks shown in Figure 3.4.2 are analyzed on the basis of their inputs and outputs. The transfer functions are studied in the more convenient mathematical domain and the results are converted to the time domain. The latter is because the analysis of the transients will be performed with the model working in the time domain.

3.4.3.1 TRANSFER FUNCTIONS FOR THE PRESSURIZER

The equations used in this section were developed in Section 3.3.4. The goal is to find a set of equations describing the pressurizer behavior, ready to be input to the processor algorithm.

Substituting equations (3.3.25) through (3.3.33) into (3.3.24):

$$\begin{aligned}\dot{P} = [&-(w_{f1} - w_c)(335 - 16P) \times 10^2 - (w_{sp} + w_c + w_{su} - w_{f1}) + V_f \times 10^6 \\ &- (105P - 157) \times w_{su}(h_{su} - h_f) \times 10^{-3}] \div [M_g(2.48P^2 + 112P \\ &-2780) + M_f(.0041P^2 - .725P + 4.08)]^{-1}\end{aligned} \tag{3.4.1}$$

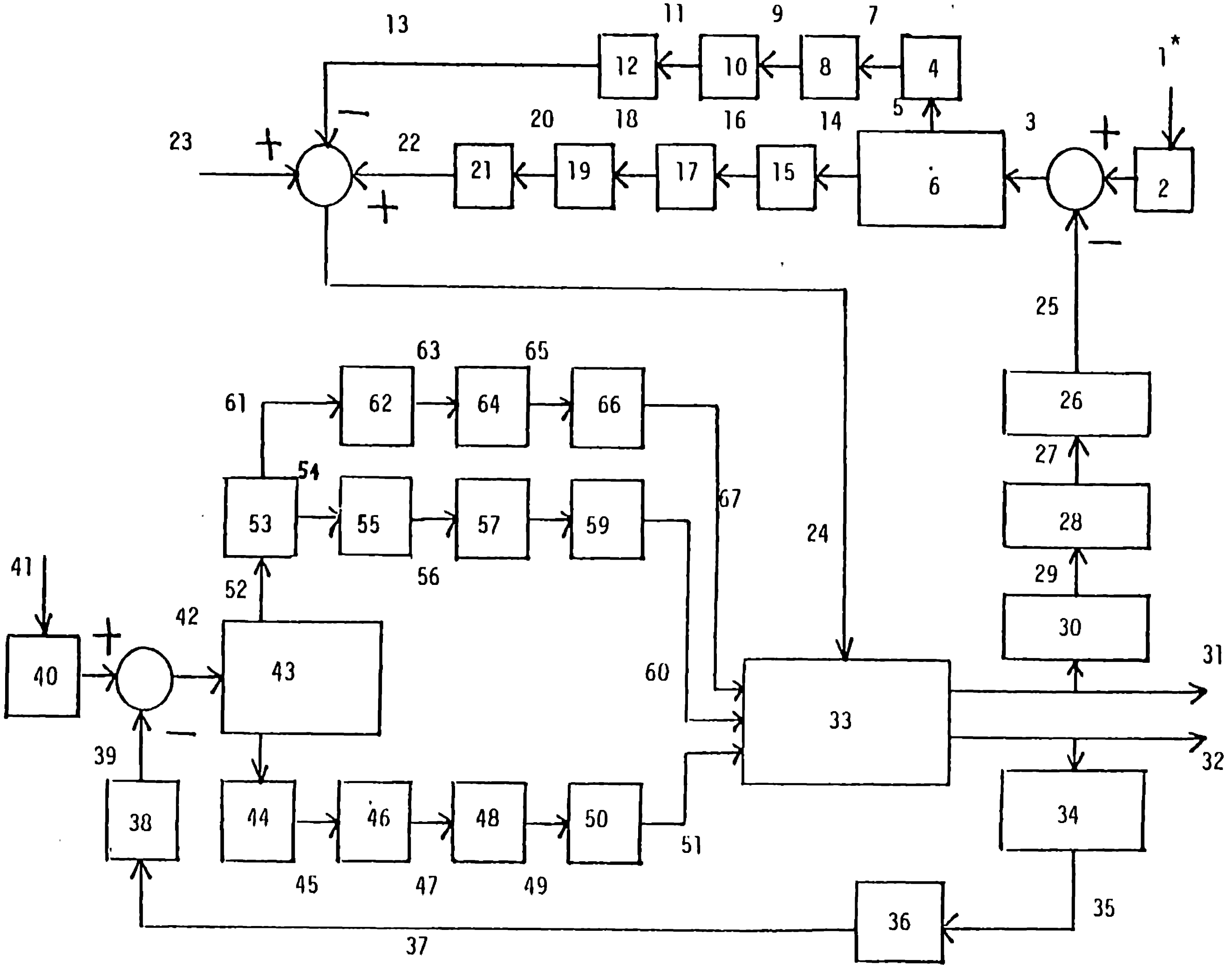


Figure 3.4.2 Pressure and volume control system, detailed block diagram.
*See legend on next page.

1. L_{ref}
2. A/D
3. $e_L^*(kT)$
4. D/A
5. $E_C^*(kT)_{let}$
6. Controller
7. $E_C(t)_{let}$
8. Letdown valve amplifier
9. $E_{CA}(t)_{let}$
10. Letdown valve motor
11. $\theta(t)_{let}$
12. Letdown valve
13. w_{let}
14. $E_C^*(kT)_{mak}$
15. D/A
16. $E_C(t)_{mak}$
17. Makeup valve amplifier
18. $E_{CA}(t)_{mak}$
19. Makeup valve motor
20. $\theta(t)_{mak}$
21. Makeup valve
22. w_{mak}
23. w_p
24. w_{su}
25. $E_L^*(kT)_{INST}$
26. A/D
27. $E_L(t)_{INST}$
28. Transmitter
29. $L(t)_{INST}$
30. Level sensor
31. $L(t)\ _{real}$
32. $P(t)_{real}$
33. Pressurizer
34. Pressure sensor
35. Transmitter
36. $P(t)_{INST}$
37. $E_p(t)_{INST}$
38. A/D
39. $E_p^*(kt)_{INST}$
40. A/D
41. $P_{ref}(t)$
42. $e_p^*(kT)$
43. Controller
44. D/A
45. $E_c(t)_{SP}$
46. Spray valve amplifier
47. $E_{CA}(t)_{SP}$
48. Spray valve motor
49. $\theta(t)_{SP}$
50. Spray valve
51. w_{SP}
52. $E_C^*(kT)_H$
53. D/A
54. $E_C(t)_{H'S}$
55. Relays amplifier
56. $E_{CA}(t)_{H'S}$
57. Relays
59. Hysteresis heaters
60. $Q_{H(2,3,4,5)}$
61. $E(t)_{HI}$
62. HI heater amplifier
63. $E_{CA}(t)_{HI}$
64. HI heater motor
65. θ(t)HI
66. HI heater (proportional)
67. Q_{HI}

Equation (3.3.38) is the working equation that is to be used as the model implementation into the computer. Notice V_f and h_f are not included in their linearized version. The reason will be apparent when the computer code is developed.

The values of M_f and M_g are calculated from integration in equations (3.3.11) and (3.3.12):

$$M_g = M_g\ (0) + \int_0^t (w_{fl} - w_c)dt, \tag{3.4.2}$$

$$M_f = M_f\ (0) + \int_0^t (w_{sp} + w_c + w_{su} - w_{fc})dt \tag{3.4.3}$$

The water enthalpy (h_w) is only allowed to be different from saturation enthalpy (h_f) in order to calculate the natural flashing incidence. The water enthalpy to be used in that situation is calculated as follows. From Appendix G:

$$M_w\dot{h}_w = w_{su}h_{su} + (w_{sp} + w_c)h_c + Q_h - w_{fl}h_{fl} + P\dot{V}_w$$
$$- (w_{sp} + w_c + w_{su} - w_{fl})h_w \quad . \tag{G.4}$$

Applying the quasi steady state conditions but keeping h_w:

$$M_w\dot{h}_w = w_{su}h_{su} + (w_{sp} + w_c)h_f + Q_h - w_{fl}h_g + P\dot{V}_w$$
$$- (w_{sp} + w_c + w_{su} - w_{fl})h_f$$

$$M_w\dot{h}_w = w_{su}h_{su} + Q_n + P\dot{V}_f + w_{fl}(h_f - h_g) - w_{su}h_f$$

$\dot{P}V_f$ is a really small quantity and can be neglected. The expression for $\dot{h}_w$ becomes

$$\dot{h}_w \simeq \frac{w_{su}(h_{su} - h_f) + w_{fl}\ (h_f - h_g) + Q_h}{M_f} \qquad (3.4.4)$$

and the relation for h_w is given by

$$h_w \simeq h_w(o) + \int_0^t \frac{w_{su}(h_{su} - h_f) + w_{fl}\ (h_f - h_g) + Q_h}{M_f}\, dt \qquad (3.4.5)$$

It should be kept in mind that this is only an approximation of the real behavior.

Finally, an equation for the level is needed. The development of an equation for the level is based on the fact that the working region of the pressurizer is cylindrical.

The level is defined as

$$L = L_{ref} + \delta L$$

$$L = L_{ref} + \frac{V_f - V_{ref}}{A_{ref}}$$

where:

L = water level (m)

L_{ref} = reference water level (m)

V_{ref} = reference volume of reference level (m^3)

A_{ref} = internal sectional area of reference level (m^3)

V_f = water volume at actual level (m^3)

From reference 3.1:

$L_{ref} = 0.69$ (m)

$V_{ref} = 1.76$ (m^3)

$A_{ref} = 1.48$ (m^3)

Therefore:

$$L(t) = 0.69 + \frac{V_f - 1.76}{1.48} \tag{3.4.6}$$

From the transfer function viewpoint the input parameters are: h_{sp}, w_{sp}, Q_h, w_{su}, h_{su}, $M_g(0)$, $M_f(0)$, $P(0)$, $h_w(0)$, $L(0)$ and the outputs are $P(t)$, $L(t)$

3.4.3.2 TRANSFER FUNCTIONS FOR THE LEVEL SENSOR

Basically a level sensor is a differential pressure sensor. But its readings are only accurate when the water is at the claibration temperature. The calibration temperature for the N.S. Savannah level sensors is 325°C. If the pressurizer water is at a different temperature, the readings should be corrected. The correction chart is given in Reference 3.7.

Furthermore, because it is a marine plant, the level readings are only accurate when the ship has zero listing. Any angle of trimming or heeling different from zero introducers an error.

In the case of a real application, the readings from the level sensor are easily corrected by implementation of the temperature correction chart, and the heel correcton functions into the validation algorithm.

Because the scope of this work does not include validation, the readings input to the control system model will be assumed to be already validated. The latter means, from the control system viewpoint, that the output of the pressurizer model represents a validated signal.

The instrument handbook (Reference 3.8) gives characteristics that are important to the modeling process. These properties are:

- the sensor has a 1 percent hysteresis
- the sensor has an 0.5 percent deviation from linearity.

The hysteresis effect appears only when the sensor reaches its maximum value (50.8 MPa). This condition is beyond the pressurizer design limits, and it is not expected to be reached by the model.

The deviation from linearity correction should be included in the validation algorithm. In other words, the sensor transfer function is:

$$L_{inst}(t) = L_{model}(t) \qquad (3.4.7)$$

3.4.3.3 TRANSFER FUNCTIONS FOR THE LEVEL SIGNAL TRANSMITTER

The level signal transmitter receives as an input a differential pressure signal, and has as an output an analog electrical signal, proportional to the pressure difference. It is also included in the transmitter transfer function the wiring required to input the electrical signal to the processor. The range of the output signal has to be compatible with the range of the A/D devices in the processor.

The following are the characteristics of the transmitter:

- range of the output signal: ± 5.12V
- signal delay: 250 (ms)

Thus the transfer function can be stated as:

$$E_{inst}(t) = \frac{\Delta E_{max}}{\Delta L_{max}} L(t - .25) \text{ (V)}$$

From the handbook:

$\Delta L_{max} = 1.62$ (m)

$\Delta E_{max} = 10.24$ (V)

$$E_{inst}(t) = 6.32\ L_{inst}(t - 0.25) \qquad (3.4.8)$$

$E_{inst}(t)$ is in volts

$L_{inst}(t)$ is in meters

t is in seconds.

3.4.3.4 ANALOG-DIGITAL, DIGITAL-ANALOG DEVICES TRANSFER FUNCTIONS

A/D devices are the components required to convert the analog signal coming from the plant into a digital signal useful to be processed. D/A devices convert the digital output coming from the processor into a real-life signal (analog) useful to be input to the plant.

The most common way to represent a D/A device is by a hold, and to represent an A/D device a sampler is used. The overall digital system and its symbols are shown in Figure 3.4.3.

The E^*_{inst} (kt) signal resembles $E_{inst}(t)$ because both signals have the same value at the sampling time.

The hold device introduces a more significant change because the sampled control signal E^*_C (kT) is held to a constant value until the new E^*_C [(k+1)T] arrives.

Thus a good approximation for the whole process is to represent it with a hold transfer function, keeping in mind that the signals flowing

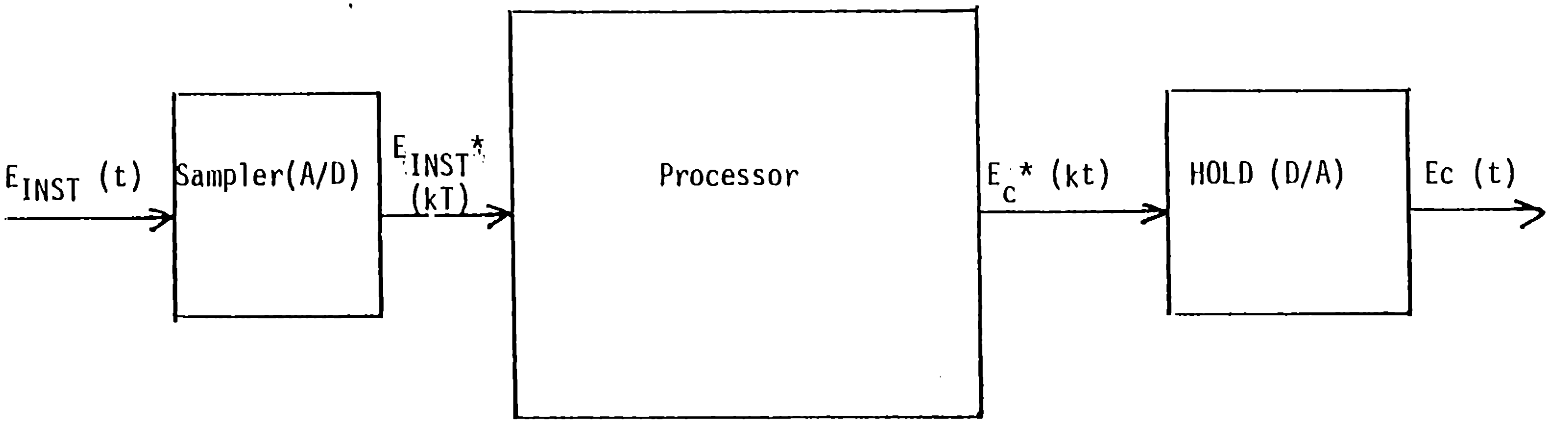


Figure 3.4.3 Analog-digital (A/D), digital-analog (D/A), transfer function model.

between sampler and hold are sampled.

Because a digital computer will be used to simulate the system, the blocks representing sampling and holding functions are easy to implement.

- Sampler: the digital computer processes the simulation at discrete intervals, then the data coming from the pressurizer model is in fact sampled.
- Hold: the digital computer simulating the control system processes the data at discrete intervals of time. Between intervals the last output is held constant. Thus the data coming from the control system model are in fact held.

In other words,

$$E_{inst}(t) = E^*_{inst}(kT) \tag{3.4.9}$$

$$E^*_C\ (kt) = E^*{}_C(t) \tag{3.4.10}$$

3.4.3.5 TRANSFER FUNCTION FOR THE LEVEĹ CONTROLLER

The level controller has two basic jobs

1. To compare the incoming level signal (sampled signal) with the reference level signal (sampled signal). From that comparison the controller decides

$E^*_L(kT)_{inst} > E^*_L(kT)_{ref}$ (Open letdown valve) (Close makeup valve) (3.4.11)

$E^*_L(kT)_{inst} = E^*_L(kT)_{ref}$ (No action) (3.4.12)

$E^*_L(kT)_{inst} < E^*_L(kT)_{ref}$ (Open makeup valve) (Close letdown valve) (3.4.13)

2. To perform the optimal contron action, experience has shown that this optimal control action is obtained by using a proportional-integral differential (PID) controller, tuning up its constant with the controller already connected to the real plant.

   The corresponding PID equations are:

$$E_c^*(kT)_{let} = e_L^*(kT)[K_{11et} + K_{21et} \int dt + K_{31et} \frac{d}{dt}] \qquad (3.4.14)$$

$$E_c^*(kT)_{mak} = e_L^*(kT)[K_{1mak} + K_{2mak} \int dt + K_{3mak} \frac{d}{dt}] \qquad (3.4.15)$$

$$e_L^*(kT) = E_L^*(kT)_{ref} - E_L^*(kT)_{inst} \qquad (3.4.16)$$

·The expression between square brackets is an operator and not a normal equation. The most appropriate values for K_1, K_2 and K_3 will appear later on when the transient analysis of the model will be performed.

3.4.3.6 AMPLIFIERS TRANSFER FUNCTION

The amplifiers, motors, and valves are exactly the same for the letdown and make-up circuits. Thus the analysis will be common for both.

The amplifiers are required because the voltage and the power of the controller output are not enough to drive the motors. The amplifier transfer function in the frequency range of interest is simply a constant.

$$\frac{E_{cA}(t)}{E_c(t)} = K \qquad (3.4.17)$$

K is a parametric constant and its value can be adjusted at the designer's will. The final values for K_{mak} and K_{let} will appear during the transient analysis.

3.4.3.7 TRANSFER FUNCTION FOR THE VALVES MOTORS

The motor chosen to drive the valves is a DC motor, arumature-controlled. Figure 3.4.4 shows this type of motor and its block diagram, both taken from reference 3.9.

By developing the overall transfer function from Figure 3.4.4b, the following equation is derived:

$$\dot{\theta} = \frac{E_a \frac{1}{R_a} K_m I_f - T_L(1 + \tau_a S)}{(1 + \tau_a S)(B_v + J_s) + K_c I_f^2 \frac{1}{R_a} K_m}$$

where:

θ = shaft angle

E_a = controlling voltage signal

R_a = armature resistance

I_a = armature current

K_m = torque constant

J_f = field current (constant)

T_L = load torque

τ_a = armature time constant = L_a/R_a

L_a = armature inductance

B_v = dumping coefficient

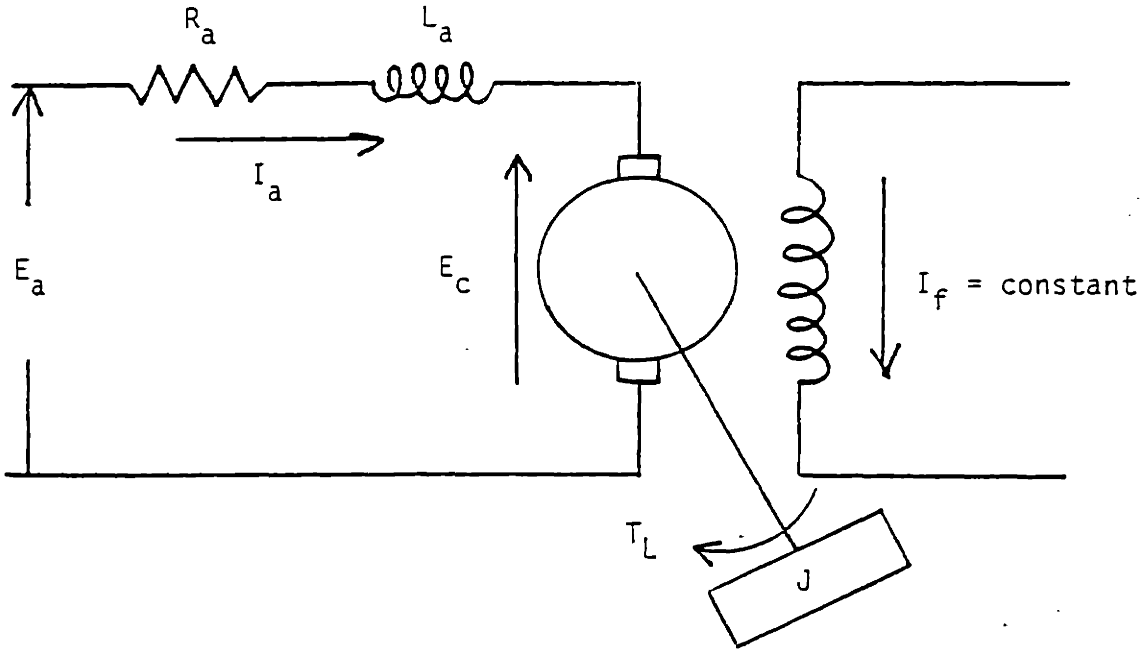


Figure 3.4.4a Armature controlled DC motor.

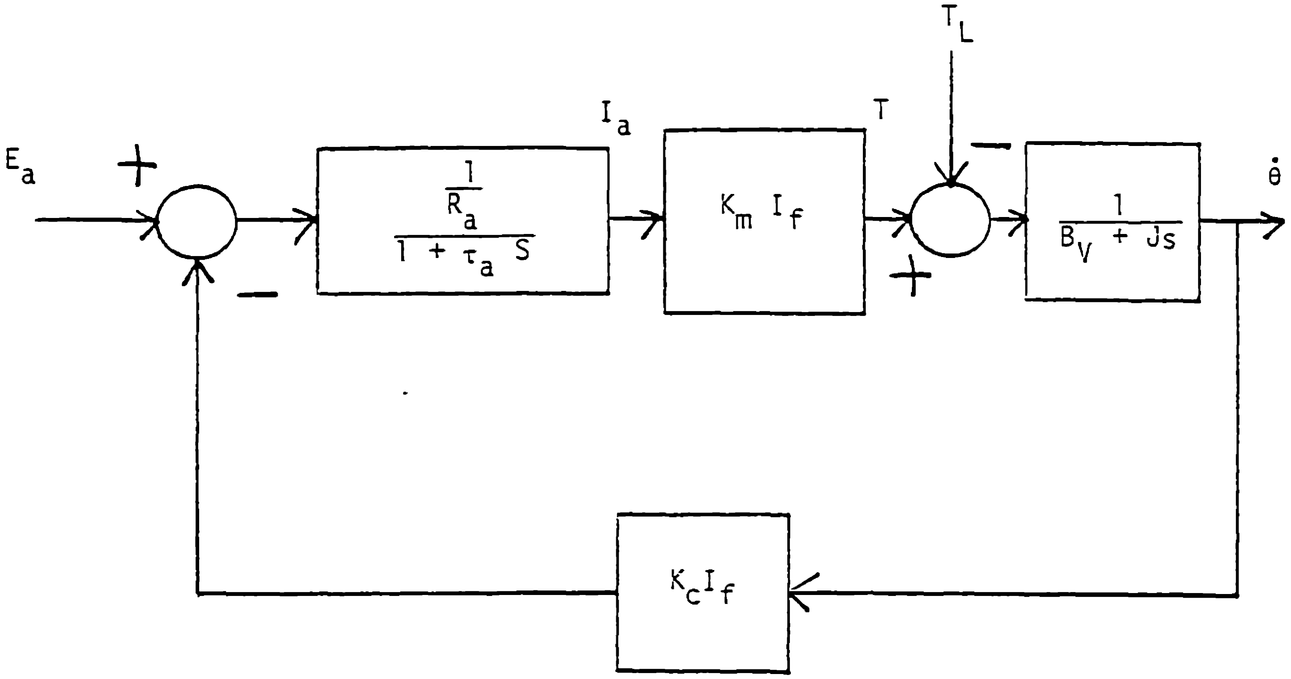


Figure 3.4.4b Armature controlled DC motor, block diagram.

J = moment of the intertie of the armature

K_c = emf constant

Because the motors are relatively small, their τ_a and J can be neglected. Also the load torque can be assumed negligible. With those assumptions, the initial equation is reduced to:

$$\theta = [\frac{\frac{K_m I_f}{R_a}}{B_v + \frac{K_c I_f^2 K_m}{R_a}}] \frac{E_a}{s}$$

Coming back to the time domain

$$\theta (t) = [\frac{\frac{K_m I_f}{R_a}}{B_v + \frac{K_c I_f^2 K_m}{R_a}}] \int_0^t E_{ca}(t)dt \qquad (3.4.18)$$

3.4.3.8 TRANSFER FUNCTIONS FOR THE MAKE-UP VALVE

By definition

$$w_{mak} = \frac{q_{mak}}{V_{mak}}$$

where:

V_{mak} = specific volume of make-up water (m^3/kg)

q_{mak} = make-up flow in m^3/s

w_{mak} = make-up flow in kg/s

The analysis is then divided into q_{mak} and V_{mak}

The make-up flow (q_{mak}) is related with the well-known expression

$$q_{mak} = F(\theta)\sqrt{P_{mak} - P}$$

where

P = primary circuit pressure

P_{mak} = make-up pressure

$F(\theta)$ = valve parameter. This parameter is a function of the shaft angle (θ).

From reference 3.2 it is known that the make-up pressure is kept constant at 0.345 MPa over the primary pressure (the make-up system has an automatic control subsystem to do that). Also from reference 3.2 it is known

$$(q_{mak})_{max} = 3.9 \times 10^{-3} (\frac{m^3}{s})$$

But

$$q_{mak} = 0.5874\ F(\theta)$$

also

$$(q_{mak})_{max} = 0.5874(F(\theta))_{max}$$

Thus, $F(\theta)_{max} = 6.64 \times 10^{-3}\ (m^3 S^{-1} MPa^{-1/2})$

In order to simplify the numerical algorithm, it will be assumed that $F(\theta)$ is a linear function of θ. Finally, it is posulated that $\theta_{max} = 2\pi$.

Under these conditions:

$$F(\theta) = \frac{F(\theta)_{max}}{\theta_{max}} \theta$$

$$F(\theta) = 1.057 \times 10^{-3} \theta \qquad (0 \leq \theta \leq 2\pi)$$

The final equation for q_{mak} is:

$$q_{mak} = \begin{cases} 0 & (\theta \leq 0) \\ 6.207 \times 10^{-4} \theta & (0 \leq \theta \leq 2\pi) \\ 3.9 \times 10^{-3} & (\geq 2\pi) \end{cases} \qquad (3.4.19)$$

With regard to the make-up specific volume, it is known from reference 3.2 that the make-up temeprature is kept constant at 46.67°C. Then,

$$V_{mak} = V_{mak} (46.67, P_{mak})$$

Performing a linearization with the data given in reference 3.6

$$V_{mak} = 1.0116 \times 10^{-2} - 50 \times 10^{-7} (P + 0.345)$$

$$(11 \text{ MPa} \leq P \leq 13 \text{ MPa})$$

Therefore the final equation for w_{mak} is:

$$w_{mak} = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{6.207 \times 10^{-4} \theta}{1.012 \times 10^{-3} - 5.0 \times 10^{-7} P} & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.9 \times 10^{-3}}{1.012 \times 10^{-3} - 5.0 \times 10^{-7} P} & (0 \leq \theta \leq 2\pi) \end{cases} \qquad (3.4.20)$$

P is the primary pressure in MPa.

3.4.3.9 TRANSFER FUNCTIONS FOR THE LETDOWN VALVE

The analytical process is quite similar to the make-up analysis. Because the actual system has no special valve for automatic letdown flow, it is assumed an extra valve system similar to the make-up system is added. Then,

$$(q_{1et})_{max} = 3.9 \times 10^{-3} \quad (\frac{m^3}{s})$$

$V_{1et} = V_p$ (MPa) $\quad$ (V_p = primary specific volume)

$\Delta P = 12.508$ (MPa) $\quad$ ($\Delta P = P - P_{1et}$)

Following the same procedure given in Section 3.4.38, we obtain:

$F(\theta)_{max} = 5.352 \times 10^{-4} \qquad (0 \leq \theta \leq 2\pi)$

$F(\theta) = 3.013 \times 10^{-4}\ \theta \qquad (0 \leq \theta \leq 2\pi)$

then

$$q_{1et}(\theta) = \begin{cases} 0 & (\theta \leq 0) \\ 6.207 \times 10^{-4}\ \theta & (0 \leq \theta \leq 2\pi) \\ 3.9 \times 10^{-3} & (\geq 2\pi) \end{cases} \qquad (3.4.21)$$

and the final equation for the w_{1et} is

$$w_{1et} = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{6.207 \times 10^{-4}\ \theta}{V_p} & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.9 \times 10^{-3}}{V_p} & (\geq 2\pi) \end{cases} \qquad (3.4.22)$$

3.4.3.10 JOINT TRANSFER FUNCTION FOR THE AMPLIFIER, MOTOR AND VALVE

Analyzing first the make-up valve, a joint equation is reached by substitution of (3.3.53) into (3.3.54) and then into (3.3.55). The result follows:

$$w_{mak} = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{6.207 \times 10^{-4}\ \theta}{1.012 \times 10^{-3} - 5.0 \times 10^{-7} P} (K^{m}_{mak})(K_{mak}) \displaystyle\int_{0}^{t} E_c(t)dt & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.9 \times 10^{-3}}{1.012 \times 10^{-3} - 5.0 \times 10^{-7} P} & (0 \leq \theta \leq 2\pi) \end{cases} \tag{3.4.23}$$

K^{m}_{mak} is the motor constant given in (3.3.54) and K_{mak} is the amplifier gain.

By a similar process:

$$w_{let} = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{6.207 \times 10^{-4}}{V_p} (K^{m}_{let})(K_{let}) \displaystyle\int_{0}^{t} E_c(t)dt & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.9 \times 10^{-3}}{V_p} & (0 \geq 2\pi) \end{cases} \tag{3.4.24}$$

K^{m}_{let} is the motor constant and K_{mak} is the amplifier gain.

3.4.3.11 TRANSFER FUNCTION FOR THE PRESSURE SENSOR

The sensor for measuring the pressure are the type called forced balanced transmitter, its theory is very well explained in reference 3.3.

From the instrument handbook the following data are obtained (as was the case of the level sensor)

- hysteresis = 1 percent
- deviation from linearity = 1.5 percent

The hysteresis behavior is only reached when the sensor ranges its maximum value. This case is not likely to occur. The deviation from linearity error will be corrected in the validation process. Thus,

$$P(t)_{inst} = P(t)_{real} \tag{3.4.25}$$

3.4.3.12 TRANSFER FUNCTION FOR THE LEVEL SIGNAL TRANSMITTER

This transmitter is designed to receive the mechanical signal from the pressure sensor, transform it into an electrical signal proportional to the first one, and to send the electrical signal to the processor. The whole process is characterized by

- electrical signal range = $\pm$ 5.12V
- signal delay = 250 (ms)

Thus the transfer function has the following form:

$$E_p(t)_{inst} = \frac{\Delta E_{max}}{\Delta P_{max}} P_{inst}(t - 0.25)$$

From reference 3.2

$$\Delta P_{max} = 13.79 \text{ (MPa)}$$

Then

$$E_p(t)_{inst} = 0.7426P(t - 0.25)_{inst} \tag{3.3.26}$$

where P is in MPa, t is in seconds, E_p is in volts.

3.4.3.13 TRANSFER FUNCTIONS FOR THE PRESSURE CONTROLLER

The main task of this controller is to keep the pressurizer pressure around the reference pressure. The pressure controller has six different actuators to keep the pressure around the set point: one proportional heater, five hysteresis heaters, and one spray valve. Each one of these actuators is analyzed in the following section.

3.4.3.13.1 TRANSFER FUNCTION FOR THE HEATER BANK NUMBER 1 (PROPORTIONAL)

The controller compares the pressure signal with the reference signal. The resultant error is subjected to a PID action. Putting the latter in mathematical terms:

$$E^*_c(kT)_{h1} = [E^*_p(kT)_{ref} - E^*_p(kT)_{inst}][K_1 + K_2 \int dt + K_3 \frac{d}{dt}] \quad (3.4.27)$$

3.4.3.13.2 TRANSFER FUNCTION FOR THE HEATER BANK NUMBER 2

This bank has a typical hysteresis cycle

$$E^*_c(kT)_{h2} = \begin{cases} 0 & E^*_p(kT) > 8.96(V) \\ 0 & 8.89 \leq E^*_p(kT) \leq 8.96 \text{ (once the heater is off)} \\ 10.24(V) & E^*_p(kT) \leq 8.89(V) \\ 10.24(V) & 8.89 \leq E^*_p(kT) \leq 8.96 \text{ (once the heater is on)} \end{cases}$$

(3.4.28)

3.4.3.13.3 TRANSFER FUNCTION FOR THE HEATER BANK NUMBER 3

$$E_c^*(kT)_{h3} = \begin{cases} 0 & E_p^*(kT) > 8.96(V) \\ 0 & 8.86 \leq E_p^*(kT) \leq 8.99 \text{ (once the heater is off)} \\ 10.24(V) & E_p^*(kT) \leq 8.86(V) \\ 10.24(V) & 8.86 \leq E_p^*(kT) \leq 8.96 \text{ (once the heater is on)} \end{cases} \quad (3.4.29)$$

3.4.3.13.4 TRANSFER FUNCTION FOR THE HEATER BANK NUMBER 4

$$E_c^*(kT)_{h4} = \begin{cases} 0 & E_p^*(kT) > 8.96(V) \\ 0 & 8.81 \leq E_p^*(kT) \leq 8.96 \text{ (once the heater is off)} \\ 10.24(V) & E_p^*(kT) \leq 8.81V \\ 10.24(V) & 8.81 \leq E_p^*(kT) \leq 8.96 \text{ (once the heater is on)} \end{cases} \quad (3.4.30)$$

3.4.3.13.5 TRANSFER FUNCTION FOR THE HEATER BANK NUMBER 5

$$E^*_c(kT)_{h5} = \begin{cases} 0 & E^*_p(kT) \geq 8.96(V) \\ 0 & 8.76 \leq E^*_p(kT) \leq 8.96 \text{ (once the heater is off)} \\ 10.24(V) & E^*_p(kT) \leq 8.76V \\ 10.24(V) & 8.76 \leq E^*_p(kT) \leq 8.96 \text{ (once the heater is on)} \end{cases} \quad (3.4.31)$$

The data for the last five equations comes from reference 3.1.

A better understanding of the hysteresis functions is obtained by looking at Figure 3.4.5.

3.4.3.13.6 TRANSFER FUNCTION FOR THE SPRAY

The transfer function implemented at the controller for the spray valve operation is very similar to the proportional heater transfer function. Using the data given in reference 3.1, the function is as follows:

$$E^*_c(kT)_{sp} = [E^*_p(kT)_{ref} - E^*_p(kT)_{inst}][K_1 + K_2\int \quad dt + K_3\frac{d}{dt}] \quad (3.4.32)$$

3.4.3.14 RELAY TRANSFER FUNCTION

Essentially the relays used to close or to open the heater banks 2, 3, 4 and 5 have a similar performance. They open and close their contacts when the processor sends the corresponding signal.

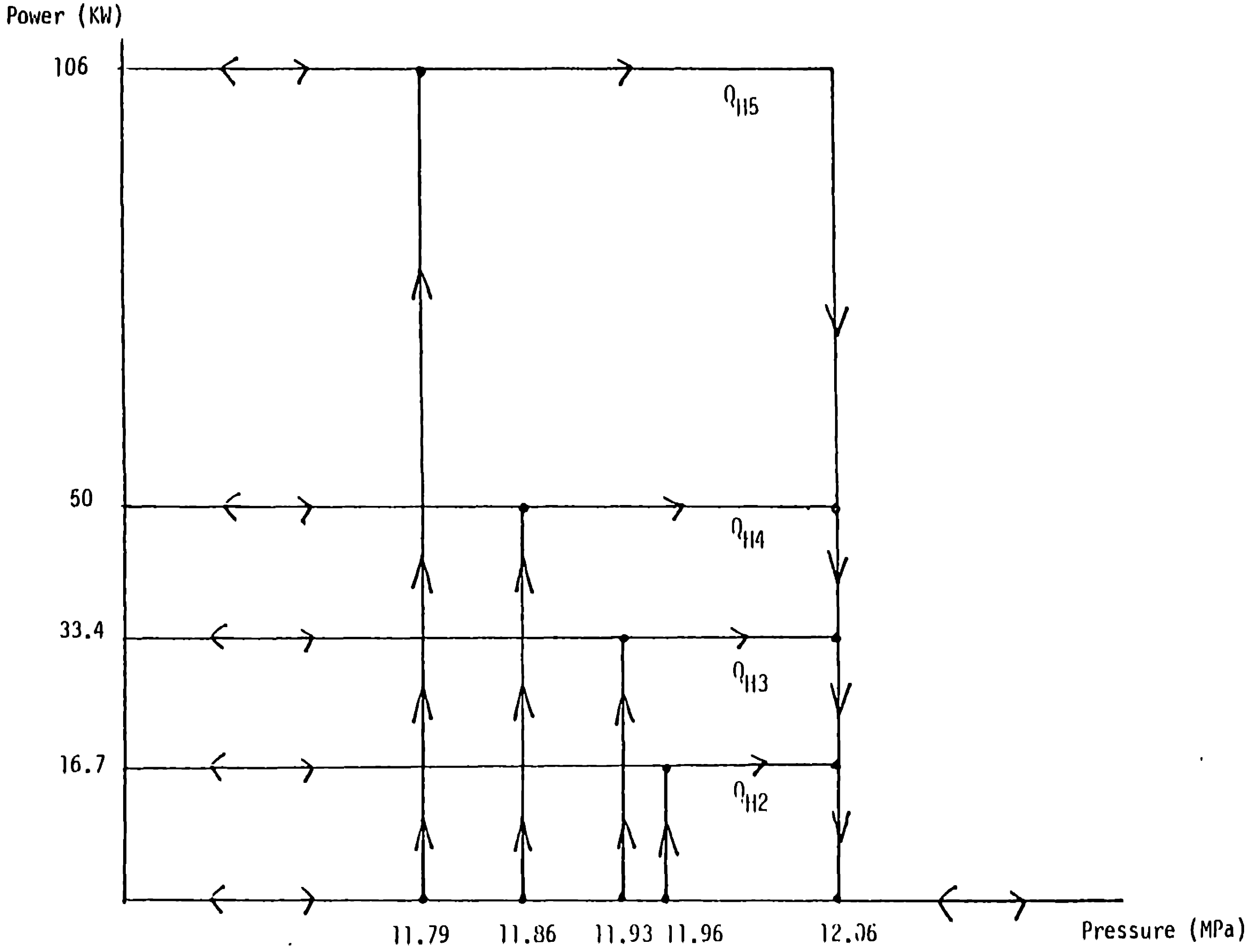


Figure 3.4.5 Hysteresis cycles for the heaters.

The relays close their contacts when they reach the operating current. A close contact means a heater bank is on.

If the mechanical inertias involved are neglected the transfer function in the Laplace domain looks as follows:

$$I(s) = \frac{K\ E_{CH}}{R}\ \frac{1}{S(1 + \tau S)}$$

where

$K\ E_{CH}$ = a constant control signal, often the amplifier

τ = L/R

L = coil inductance

R = coil resistance.

In this case the relays are not very big, that means R >>_ L. Thus τ can be assumed very small. A very small τ leads to the following simplification.

$$I(s) = \frac{E_{CH}}{sR}$$

Returning to the time domain

$$I(t) = \frac{E_{CH}}{R} = \text{constant} \qquad (3.4.33)$$

In other words, for the case at hand it is possible to assume safely that the relays close or open almost instantaneously, upon receiving the control signal from the processor.

3.4.3.15 TRANSFER FUNCTION FOR THE HEATERS

The analysis has been made differentiating the hysteresis heaters from the proportional heater.

3.4.3.15.1 HEATERS WITH A HYSTERESIS CYCLE

A basic assumption is made about the heater power. It will be assumed that as soon as the relay closes its contact, the whole heater power is released into the water. This is not exact, but considering the resistance nature of the heater element, and the high thermal conducutivity of the heater well, the loss in accuracy wil not be significant.

Mathematically the heater transfer functions are expressed as follows:

$$Q_{H2} = \begin{cases} 0 & \text{(relay open)} \\ 16.7 \text{ (KW)} & \text{(relay closed)} \end{cases} \qquad (3.4.34)$$

$$Q_{H3} = \begin{cases} 0 & \text{(relay open)} \\ 33.4 \text{ (KW)} & \text{(relay closed)} \end{cases} \qquad (3.4.35)$$

$$Q_{H4} = \begin{cases} 0 & \text{(relay open)} \\ 50.0 \text{ (KW)} & \text{(relay closed)} \end{cases} \qquad (3.4.36)$$

$$Q_{H5} = \begin{cases} 0 & \text{(relay open)} \\ 106.0 \text{ (KW)} & \text{(relay closed)} \end{cases} \qquad (3.3.37)$$

where Q_{H2}, Q_{H3}, Q_{H4}, Q_{H5} are the powers of the respective heaters.

3.4.3.15.2 PROPORTIONAL HEATER BANK

This heater consists of a variable resistance operated by a DC motor. Assuming the power is delivered linear with the shaft angle, and the maximum power delivered at $\theta = 2\pi$, the transfer function is expressed as follows:

$$Q_{H1} = \begin{cases} 0 & (\theta \leq 0) \\ 2.66 \times \theta & (0 \leq \theta \leq 2\pi) \\ 16.7\ (KW) & (\theta \geq 2\pi) \end{cases} \qquad (3.4.38)$$

Q_{H1} = power delivered by the heater

θ = shaft angle.

3.4.3.16 TRANSFER FUNCTIONS FOR THE SPRAY VALVE

The following data come from reference 3.2:

$(q_{sp})_{max} = 3.28 \times 10^{-3}\ (m^3/s)$

$\Delta P = 0.4826$ MPa

Using a similar treatment as that employed for the make-up valve, we obtain:

$$q_{sp}(\theta) = \begin{cases} 0 & (\theta \leq 0) \\ 5.22 \times 10^{-4}\ \theta & (0 \leq \theta \leq 2\pi) \\ 3.28 \times 10^{-3} & (0 \geq 2\pi) \end{cases}$$

The value for the specific volume is a function of temperature at the cold leg in the primary circuit. Because the analysis of the primary circuit is not included in this thesis, V_{sp} will be introduced as an initial condition, the same as h_{sp}, V_p, h_{su}, etc.

The final equation for the spray flow is as follows:

$$w_{sp}(\theta) = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{5.223 \times 10^{-4}\ \theta}{V_{sp}} & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.28 \times 10^{-3}}{V_{sp}} & (0 \geq 2\pi) \end{cases} \qquad (3.4.39)$$

3.4.3.17 JOINT TRANSFER FUNCTION FOR THE SPRAY VALVE SYSTEM

Combining the functions for the amplifier, motor, and valve, the following equation is obtained:

$$w_{sp}(t) = \begin{cases} 0 & (\theta \leq 0) \\ \dfrac{5.22 \times 10^{-4}}{V_{sp}} (K^{m}_{sp})(K_{sp}) \displaystyle\int_0^t E_c(t)dt & (0 \leq \theta \leq 2\pi) \\ \dfrac{3.28 \times 10^{-3}}{V_{sp}} & (0 \geq 2\pi) \end{cases} \qquad (3.4.40)$$

3.4.3.18 JOINT TRANSFER FUNCTIONS FOR THE HEATER SYSTEM

Again the analysis is repeated into hysteresis heaters and proportional heaters.

3.4.3.18.1 JOINT TRANSFER FUNCTION FOR THE PROPORTIONAL HEATER BANK

Substituting the equations (3.4.38), (3.4.18), and (3.4.17), the joint transfer equation is reached.

$$Q_{H1} = \begin{cases} 0 & (\theta \leq 0) \\ 2.66 \;.\; (K^{m}_{H1})(K_{H1})\int_{0}^{t} E_c(t)dt & (0 \leq \theta \leq 2\pi) \\ 16.7 & (0 \geq 2\pi) \end{cases} \qquad (3.4.41)$$

3.4.3.18.2 JOINT TRANSFER FUNCTION FOR THE HEATER BANK UNDER HYSTERESIS CYCLE

This set of equations comes from subtituting equations (3.4.28), (3.4.29), (3.4.30), (3.4.31) into (3.4.34), (3.4.35), (3.4.36), and (3.4.37) respectively.

$$Q_{H2} = \begin{cases} 0 & \text{if } E^{*}_{c2}(kT) = 0 \text{ (V)} \\ 16.7 & \text{if } E^{*}_{c2}(kT) = 10.24\text{V} \end{cases} \qquad (3.4.42)$$

$$Q_{H3} = \begin{cases} 0 & \text{if } E^{*}_{c2}(kT) = 0 \text{ (V)} \\ 33.4 & \text{if } E^{*}_{c2}(kT) = 10.24\text{V} \end{cases} \qquad (3.4.43)$$

$$Q_{H4} = \begin{cases} 0 & \text{if } E^{*}_{c2}(kT) = 0 \text{ (V)} \\ 50.0 & \text{if } E^{*}_{c2}(kT) = 10.24\text{V} \end{cases} \qquad (3.4.44)$$

$$Q_{H5} = \begin{cases} 0 & \text{if } E^{*}_{c2}(kT) = 0 \text{ (V)} \\ 106.0 & \text{if } E^{*}_{c2}(kT) = 10.24 \text{ (V)} \end{cases} \qquad (3.4.45)$$

The hysteresis cycles are shown in Figure 3.4.5.

3.4.3.19 TRANSFER FUNCTIONS FOR THE VALIDATION PROCESSOR

The specific details of how the validation function will be done is not a subject of this thesis. But it is a fact that the validation processor is intended to keep the instrument signals as close as possible to the true signal inside of the plant. The latter suggests that for the objectives of this work, it is a good approximation to assume a validation transfer function equal to one.

REFERENCES

3.1 Instruction book, Pressurizer, N.S. Savannah Nuclear Power Plant, Babcock and Wilcox Co., New York.

3.2 Nuclear merchant ship reactor final safeguards report. Vol. 1. Description of the N.S. Savannah. BAW-1164 (Vol. 1), June 1980.

3.3 Nuclear reactor (PWR) pressurizer real time modeling for sensor validation. (Master's thesis) by Christopher Geffray, MIT, 1980, Nuclear Engineering Department.

3.4 An improved pressurizer model with bubble rise and condensate drop dynamics, Amir N. Nahavandi, Nuclear Engineering and Design, 12 (1970), pp. 135-147.

3.5 Digital model simulation of a nuclear pressurizer. R.C. Baron. Nuclear Science and Engineering: 52, 283-291 (1973).

3.6 Thermodynamic derivatives for water and steam. Rivkin, Aleksandrov kremenevskaya. V.H. Winston and Sons, 1978, Washington,D.C.

3.7 N.S. Savannah reactor operating manual, Babcock and Wilcox Co., New York, Vol. II, Standard Operating Procedures.

3.8 Bailey product specifications, p. 31-1, f/b line level transmitters.

3.9 Automatic control engineering, Francis H. Raven, McGraw-Hill, 1978.

3.10 Bailey product specifications, E. 41-5, pressure transmitters.

CHAPTER 4

DIGITAL SIMULATION AND TRANSIENT ANALYSIS

4.1 INTRODUCTION

All the fundamentals required to prepare a digital simulation were developed in Chapter 3. Chapter 4 is devoted to describing how the pressurizer model and the control system might interact together. To do so, a code simulating the pressurizer model and its control system were developed. After that, the code was run for several situations checking whenever possible its behavior against the real plant behavior. The final part of the chapter is concerned with tuning up the control system parameters, in order to get the best response possible.

The procedure starts with a general description of the flow diagram appropriate to this problem. After that each main block in the general flow diagram is explained in detail. Finally, the program itself appears. The last section of the chapter describes the calculated cases, their results, and the procedure to tune up the control system.

4.2 GENERAL FLOW DIAGRAM

The equations will be integrated from t to t + T assuming that the system is entirely known at time t. At the beginning, the initial conditions are all that is known, thus the first iteration is made by using those conditions as the starting point. The integrations are performed by using the simplest approach.

$$F(t + T) = F(t) + T \times \dot{F}(t) \qquad (4.2.1)$$

$F(t)$ is a function of time t

$\dot{F}(t)$ is the derivative of $F(t)$ at time t

T is the iteration interval

$F(t + T)$ is the function at time $t + T$.

Before making the integrations, several computations must be performed. Following the order given in Figure 4.2.1, these computations are (the nomenclature is given in Chapter 3):

- w_{1et} and w_{mak}
- w_{su}
- Q_H and w_{sp}
- h_f and $1/h_{fg}$
- w_c
- w_{f1}
- v_f

At this point $L(t)$ is calculated.

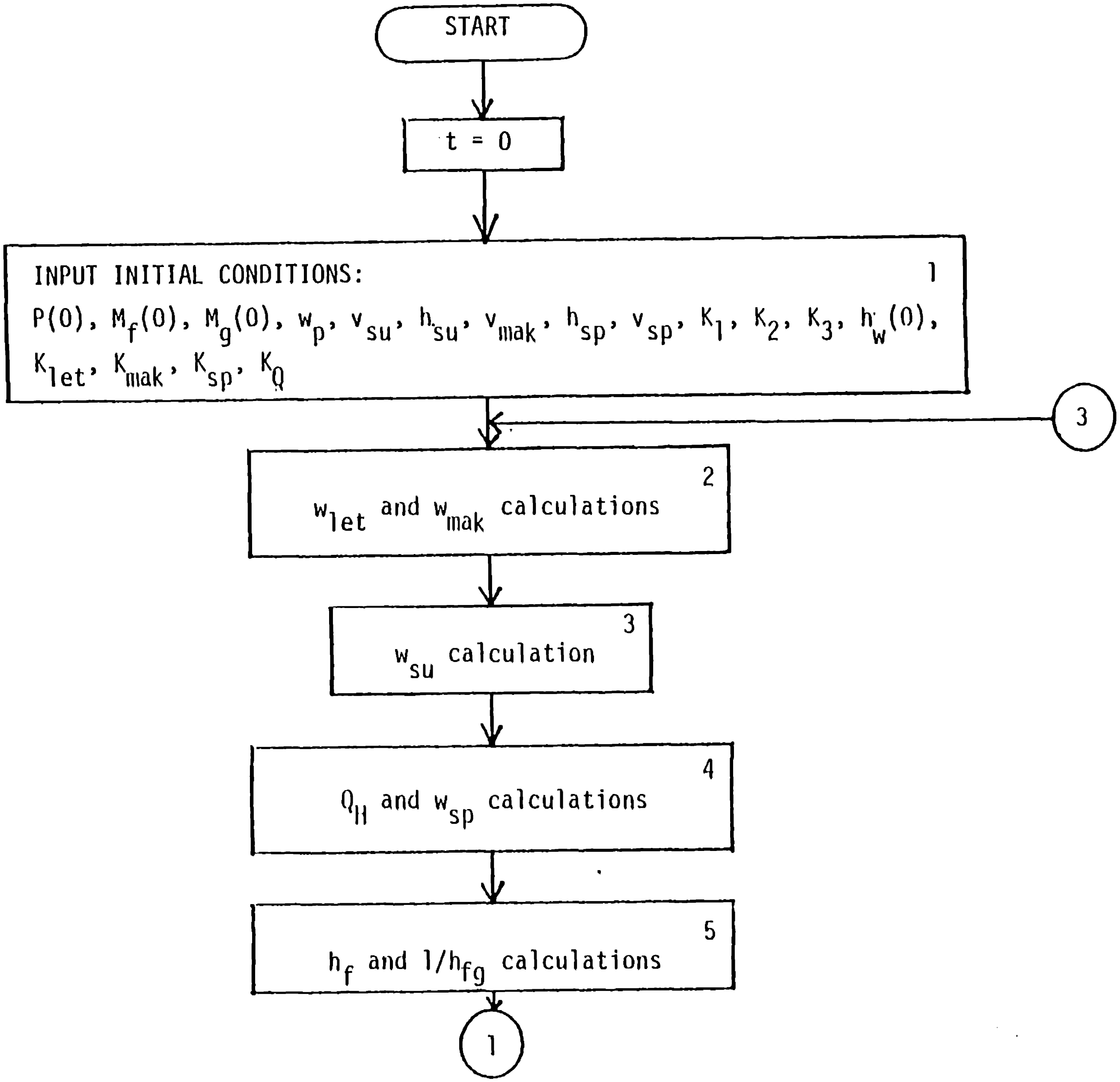
- $w_{su}(h_{su} - h_f)$

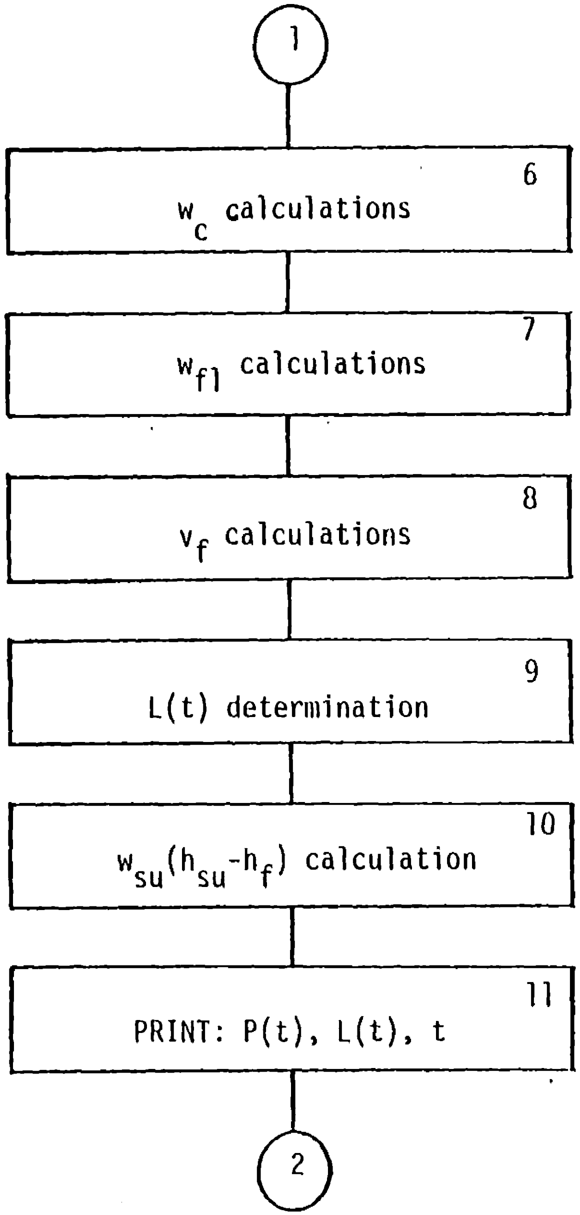
Next $P(t)$, $L(t)$, and t are printed.

Then $\dot{P}(t)$ and $P(t + T)$ are calculated.

- $\dot{h}_w(t)$ and $h_w(t + T)$ are calculated,
- $\dot{M}_g(t)$ and $M_g(t + T)$ are calculated,
- $\dot{M}_f(t)$ and $M_f(t + T)$ are calculated,

and finally the cycle is repeated by making $t = t + T$ or another alternative is to stop the iteration process. A few comments are required up to this point:


START
$t = 0$
INPUT INITIAL CONDITIONS: 1
$P(0)$, $M_f(0)$, $M_g(0)$, w_p, v_{su}, h_{su}, v_{mak}, h_{sp}, v_{sp}, K_1, K_2, K_3, $h_w(0)$, K_{let}, K_{mak}, K_{sp}, K_Q
3
2
w_{let} and w_{mak} calculations
3
w_{su} calculation
4
Q_H and w_{sp} calculations
5
h_f and $1/h_{fg}$ calculations
1


1
6
w_c calculations
7
w_{fl} calculations
8
v_f calculations
9
L(t) determination
10
$w_{su}(h_{su}-h_f)$ calculation
11
PRINT: P(t), L(t), t
2

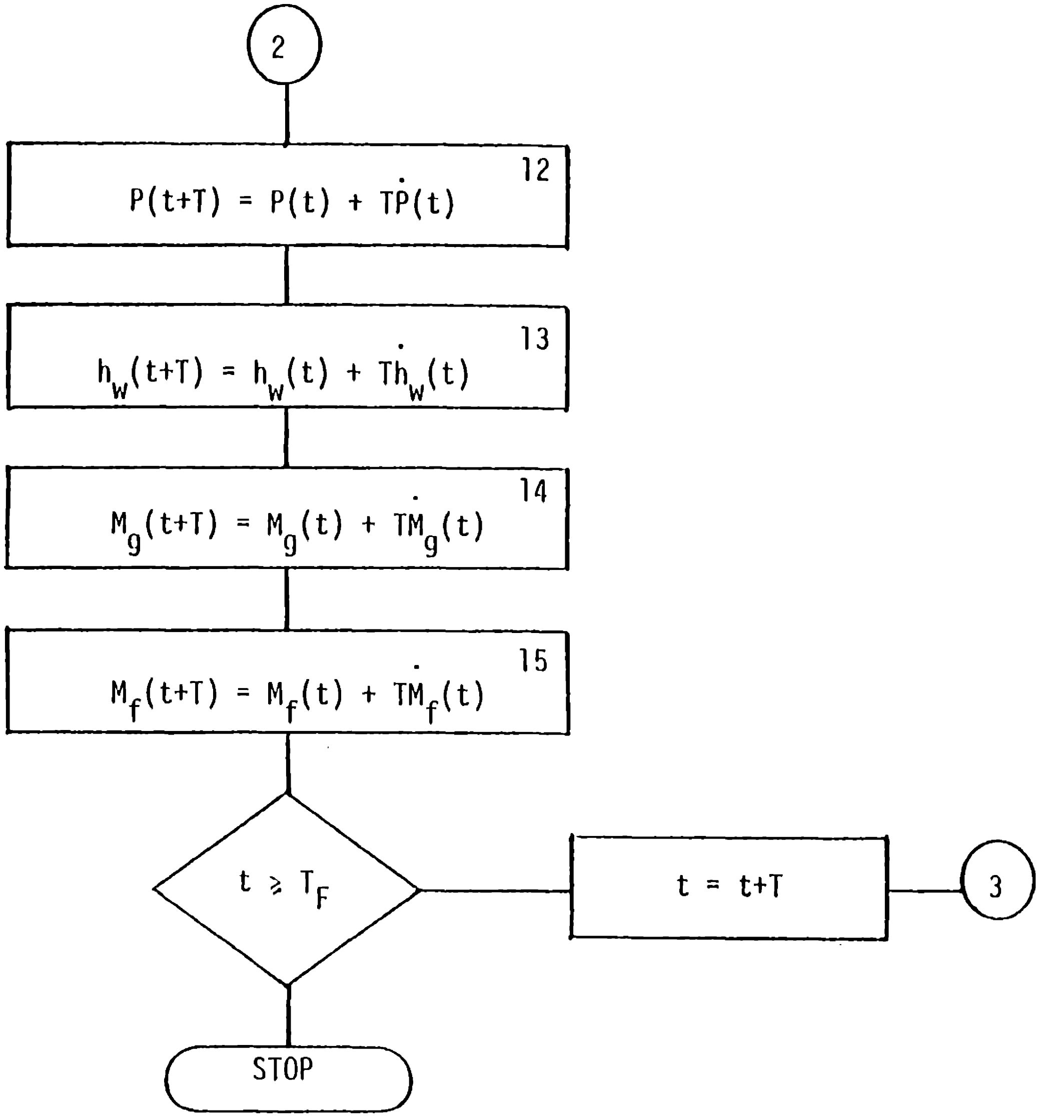

2
12
$P(t+T) = P(t) + T\dot{P}(t)$
13
$h_w(t+T) = h_w(t) + T\dot{h}_w(t)$
14
$M_g(t+T) = M_g(t) + T\dot{M}_g(t)$
15
$M_f(t+T) = M_f(t) + T\dot{M}_f(t)$
$t \geq T_F$
$t = t+T$
3
STOP

Figure 4.2.1 General flow chart.

1. Each one of the blocks shown in Figure 4.2.1 is explained in detail in the following section.
2. The control actions are included in the flow diagrams under the names of w_{let}, w_{mak}, Q_H, and w_{sp}.

4.3 DETAILED ANALYSIS OF THE GENERAL FLOW CHART

4.3.1 INITIAL CONDITIONS

Because the code is programmed in a computer of low memory capacity, several inputs are directly set into the program. The others go in the numerical registers. The following inputs go in registers: $P(0)$, $M_f(0)$, $M_g(0)$, $h_w(0)$. The others are directly coded. They are: w_p, v_{su}, h_{su}, v_{mak}, h_{sp}, v_{sp}, K_1, K_2, K_3, K_{let}, K_{mak}, K_{sp}, K_Q. More information is given in the code users manual in Appendix H.

4.3.2 LET-DOWN AND MAKE-UP FLOWS CALCULATIONS

As previously noted, the w_{let} or w_{mak} computations implicitly describe the action of the PID controller. Therefore, a first step in obtaining these values is to develop a simulation model for the PID controller. At the same time, noting from equations (3.4.23) and (3.4.24) that an integration is made over the PID output $E_c(t)$, a complete subroutine will be designed. This subroutine will perform the following function:

$$\gamma(k) = \frac{1}{D}\left(K_1 + \frac{K_2}{D} + K_3 D\right) e(t) \tag{4.3.1}$$

$\gamma(k)$ represents an integration made over a PID operation previously performed upon the error e(t).

First we have the classical numerical approach for the PID function (Ref. 4.4):

$$E_c(h) = K_1 e(k) + K_2 T \sum_{n=1}^{k} e(n) + E_c(0) + \frac{K_3}{T}[e(k) - (e(k - 1)] \tag{4.3.2}$$

where

$E_c(k)$	PID signal instant k
e(k)	error signal instant k
e(k - 1)	error signal instant (k - 1)
K_1	proportional constant
K_2	integral constant
K_3	derivative constant
T	iteration interval
E(0)	initial PID signal

But this equation is too cumbersome to implement. A more convenient way is to use the following:

$$E_c(k - 1) = K_1 e(k - 1) + K_2 T \sum_{n=1}^{k-1} e(n) + E_c(0) + \frac{K_3}{T}[e(k - 1) - e(k - 2)]$$

Defining

$$\Delta E_c(k) = E_c(k) - E_c(k - 1)$$

$$\Delta E_c(k) = K_1[e(k) - e(k - 1)] + K_2 T e(k) + \frac{K_3}{T}[e(k) - 2e(k - 1) + e(k - 2))$$

and $E_c(k) = E_c(k - 1) + \Delta E_c(k)$ (4.3.3)

Following a similar reasoning for the extra integration over the PID function

$$\gamma(k) = T \sum_{n=1}^{k} E_c(n)$$

$$\gamma(k - 1) = T \sum_{n=1}^{k-1} E_c(n)$$

$$\Delta\gamma(k) = \gamma(k) - \gamma(k - 1)$$

$$\Delta\gamma(k) = T\, E_c(k)$$

and finally

$$\gamma(k) = \gamma(k - 1) + TE_c(k) \tag{4.3.4}$$

By combining equations (4.3.3) and (4.3.4), the general expression for the subroutine is obtained.

$$\gamma(k) = \gamma(k - 1) + \quad E_c(k - 1) + K_1[e(k) - e(k - 1)] + K_2Te(k) + \frac{K_3}{T} [e(k) - 2e(k - 1) + e(k - 2)] \tag{4.3.5}$$

The next step is to perform the computation of w_{mak} and w_{let}. Figure 4.3.1 shows the detailed flow diagram which simulates the computations. What the flow diagram says, step-by-step, is the following:

1. The error in level is obtained
2. A PID function is operated over the error.
3. A test is made to see if the error is positive or negative. The sign will point what actuator should be operated. Both branches have the integration over the PID function, also a consistency

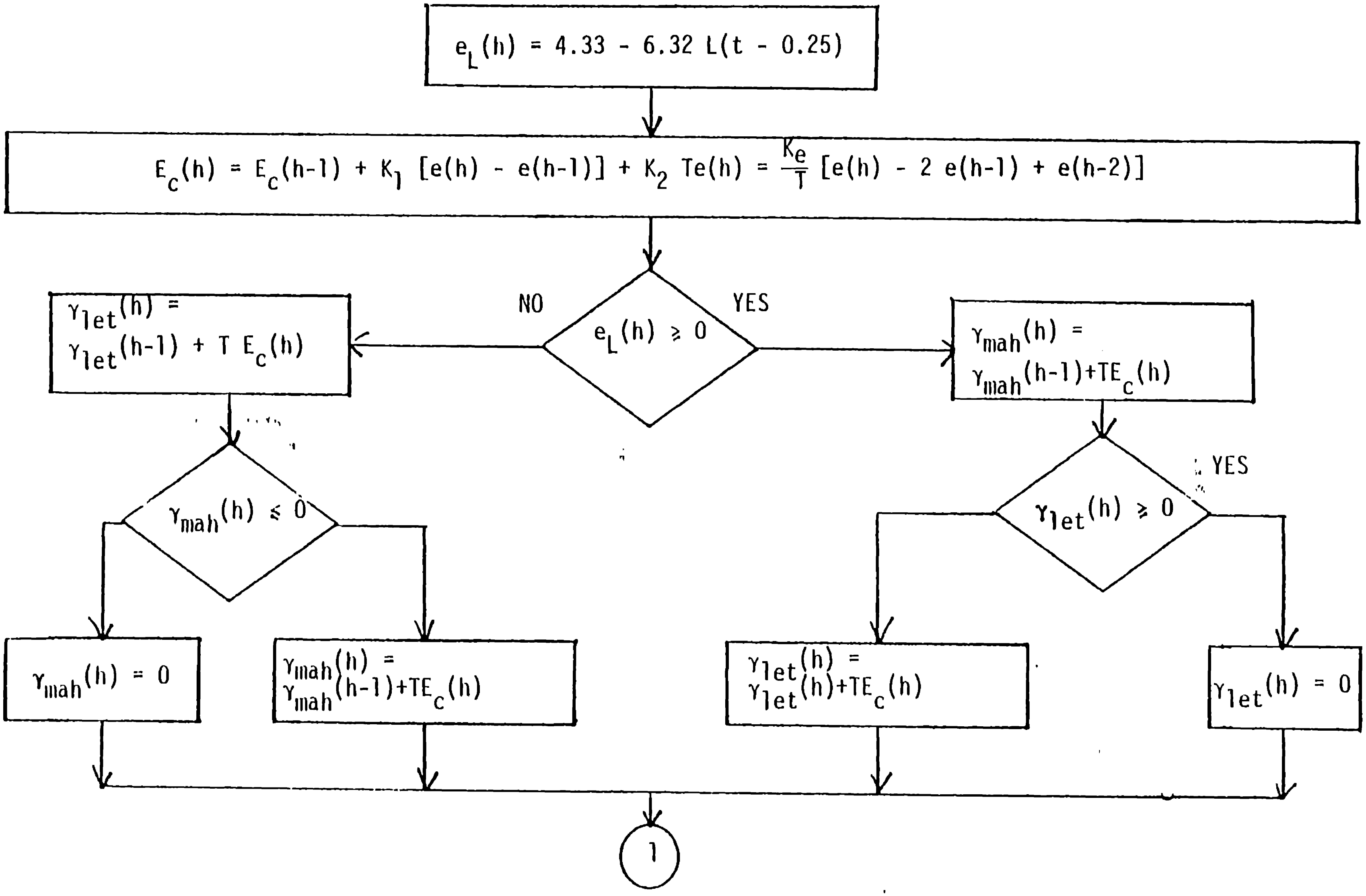
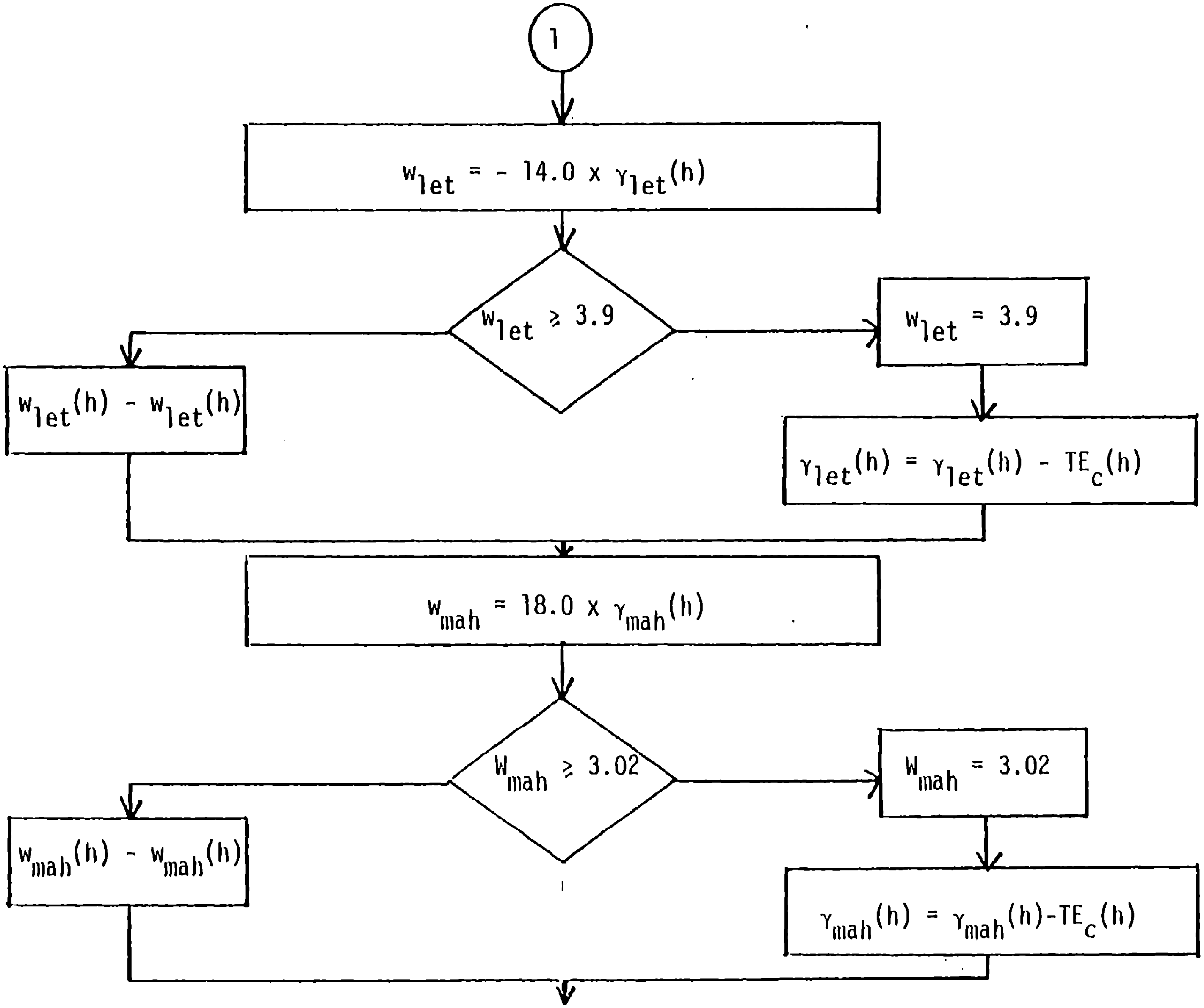

$e_L(h) = 4.33 - 6.32\ L(t - 0.25)$
$E_c(h) = E_c(h-1) + K_1\ [e(h) - e(h-1)] + K_2\ Te(h) = \frac{K_e}{T}\ [e(h) - 2\ e(h-1) + e(h-2)]$
NO
$e_L(h) \geq 0$
YES
$\gamma_{let}(h) =$ $\gamma_{let}(h-1) + T\ E_c(h)$
$\gamma_{mah}(h) =$ $\gamma_{mah}(h-1)+TE_c(h)$
$\gamma_{mah}(h) \leq 0$
YES
$\gamma_{let}(h) \geq 0$
$\gamma_{mah}(h) = 0$
$\gamma_{mah}(h) =$ $\gamma_{mah}(h-1)+TE_c(h)$
$\gamma_{let}(h) =$ $\gamma_{let}(h)+TE_c(h)$
$\gamma_{let}(h) = 0$
1

Figure 4.3.1 w_{let} and w_{mak} computations.


1
$w_{let} = - 14.0 \times \gamma_{let}(h)$
$w_{let} \geq 3.9$
$w_{let}(h) - w_{let}(h)$
$w_{let} = 3.9$
$\gamma_{let}(h) = \gamma_{let}(h) - TE_c(h)$
$w_{mah} = 18.0 \times \gamma_{mah}(h)$
$W_{mah} \geq 3.02$
$w_{mah}(h) - w_{mah}(h)$
$W_{mah} = 3.02$
$\gamma_{mah}(h) = \gamma_{mah}(h)-TE_c(h)$

check to avoid negative values for θ is made.

4. w_{1et} is calculated from equation (3.4.24). A check is made to avoid w_{1et} gains over its maximum value, and also if the maximum condition is reached, an expression for $\gamma_{1et}(k)$ is implemented, keeping $\gamma_{1et}(k)$ constant.
5. w_{mak} is calculated from equation (3.4.23), and the same comments for w_{mak} apply here.

4.3.3 TOTAL SURGE FLOW COMPUTATIONS

Under the assumptions made in Chapter 3 w_{su} is simply

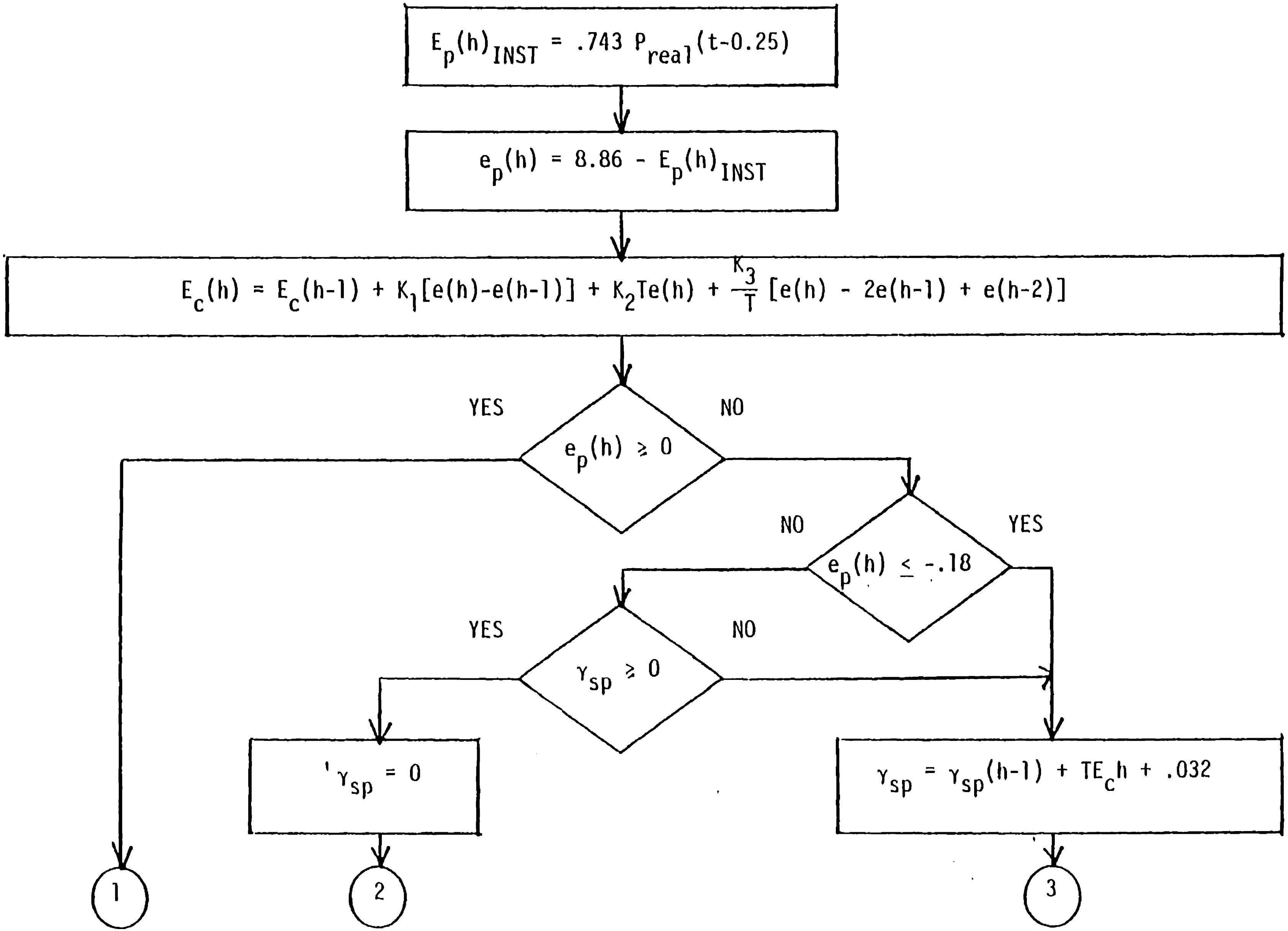
$$w_{su} = w_{mak} + w_p - w_{1et}$$

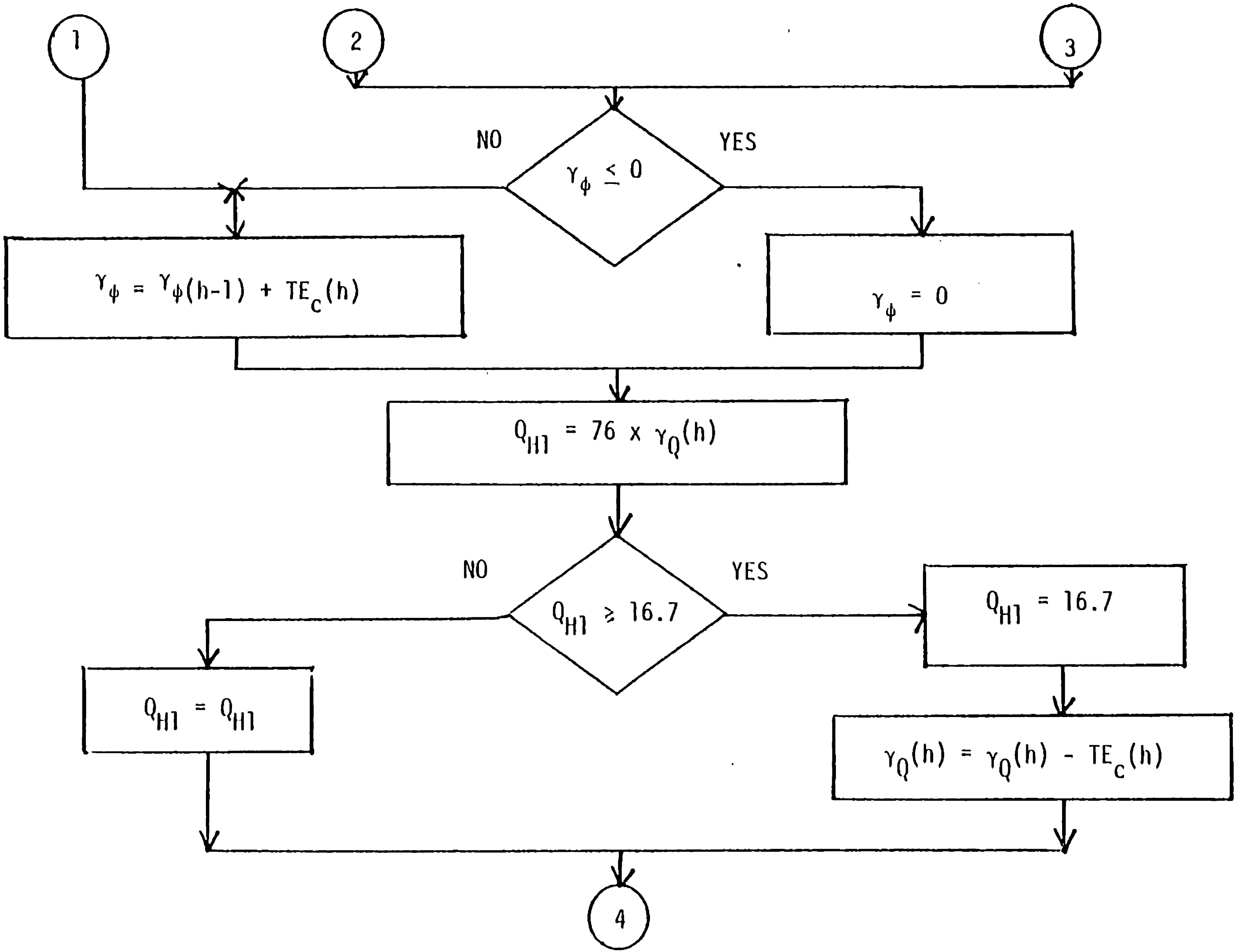
where w_p is the primary water surge.

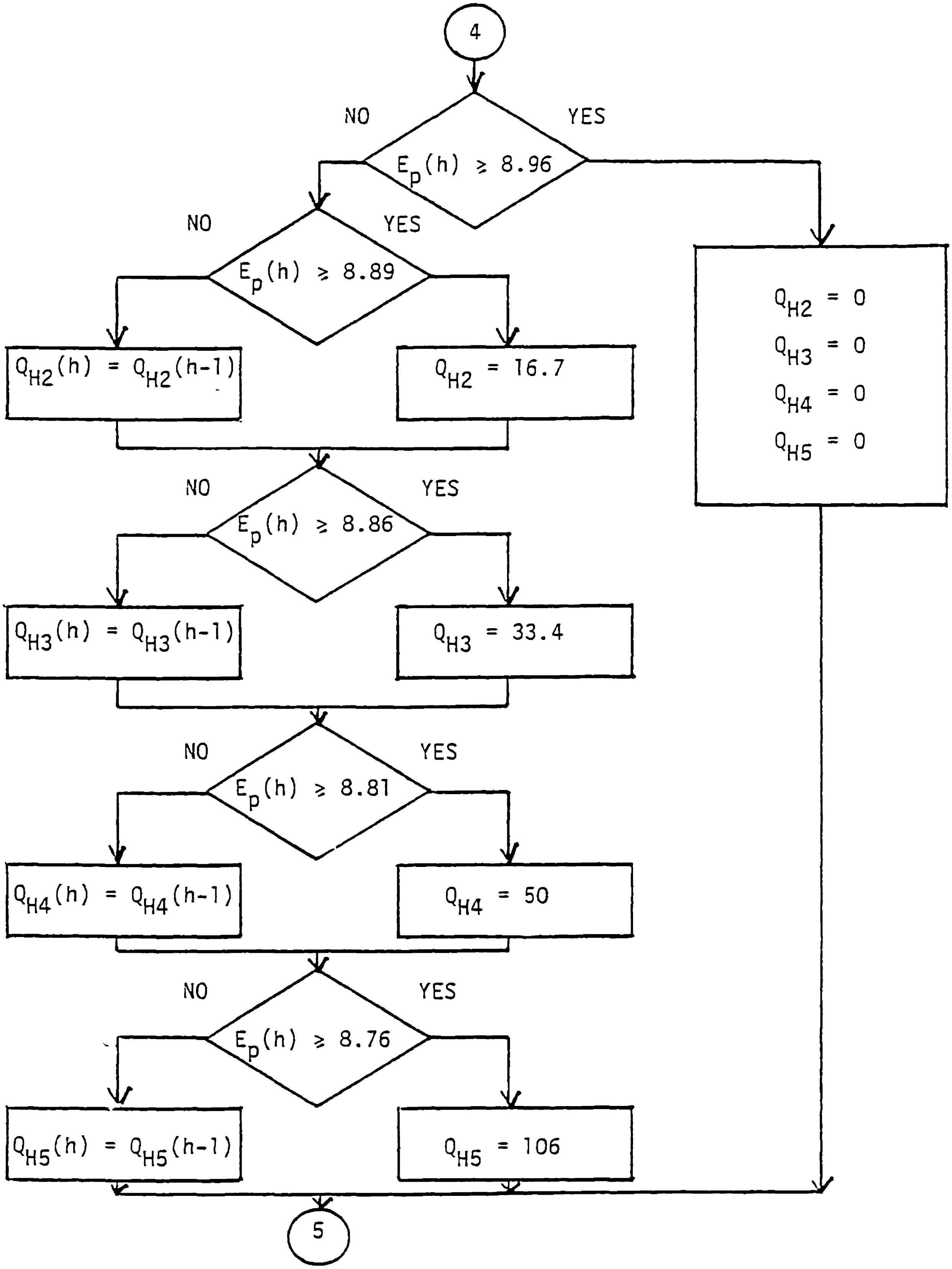
4.3.4 TOTAL HEAT AND SPRAY FLOW COMPUTATIONS

Because w_{sp} is only a PID controlled variable its flow diagram is fairly similar to those of w_{mak} and w_{1et}. Q_H have the PID variable plus the back-up heaters which work under a hysteresis control cycle. Figure 4.3.2 shows the complete flow diagram to get Q_H and w_{sp}. The explanation of Figure 4.3.2 step by step follows.

1. The electrical equivalent to the pressure signal is obtained.
2. The error signal is calculated.
3. A PID function is operated upon the error functions.
4. Depending on the error sign, the controller decides to actuate the spray valve or the proportional heaters. This block has the


$E_p(h)_{INST} = .743\ P_{real}(t-0.25)$
$e_p(h) = 8.86 - E_p(h)_{INST}$
$E_c(h) = E_c(h-1) + K_1[e(h)-e(h-1)] + K_2Te(h) + \frac{K_3}{T}[e(h) - 2e(h-1) + e(h-2)]$
YES
NO
$e_p(h) \geq 0$
NO
YES
$e_p(h) \leq -.18$
YES
NO
$\gamma_{sp} \geq 0$
$\gamma_{sp} = 0$
$\gamma_{sp} = \gamma_{sp}(h-1) + TE_ch + .032$
1
2
3


1
2
3
NO
$\gamma_\phi \leq 0$
YES
$\gamma_\phi = \gamma_\phi(h-1) + TE_c(h)$
$\gamma_\phi = 0$
$Q_{H1} = 76 \times \gamma_Q(h)$
NO
$Q_{H1} \geq 16.7$
YES
$Q_{H1} = 16.7$
$Q_{H1} = Q_{H1}$
$\gamma_Q(h) = \gamma_Q(h) - TE_c(h)$
4


4
NO
YES
$E_p(h) \geq 8.96$
NO
YES
$E_p(h) \geq 8.89$
$Q_{H2}(h) = Q_{H2}(h-1)$
$Q_{H2} = 16.7$
$Q_{H2} = 0$
$Q_{H3} = 0$
$Q_{H4} = 0$
$Q_{H5} = 0$
NO
YES
$E_p(h) \geq 8.86$
$Q_{H3}(h) = Q_{H3}(h-1)$
$Q_{H3} = 33.4$
NO
YES
$E_p(h) \geq 8.81$
$Q_{H4}(h) = Q_{H4}(h-1)$
$Q_{H4} = 50$
NO
YES
$E_p(h) \geq 8.76$
$Q_{H5}(h) = Q_{H5}(h-1)$
$Q_{H5} = 106$
5

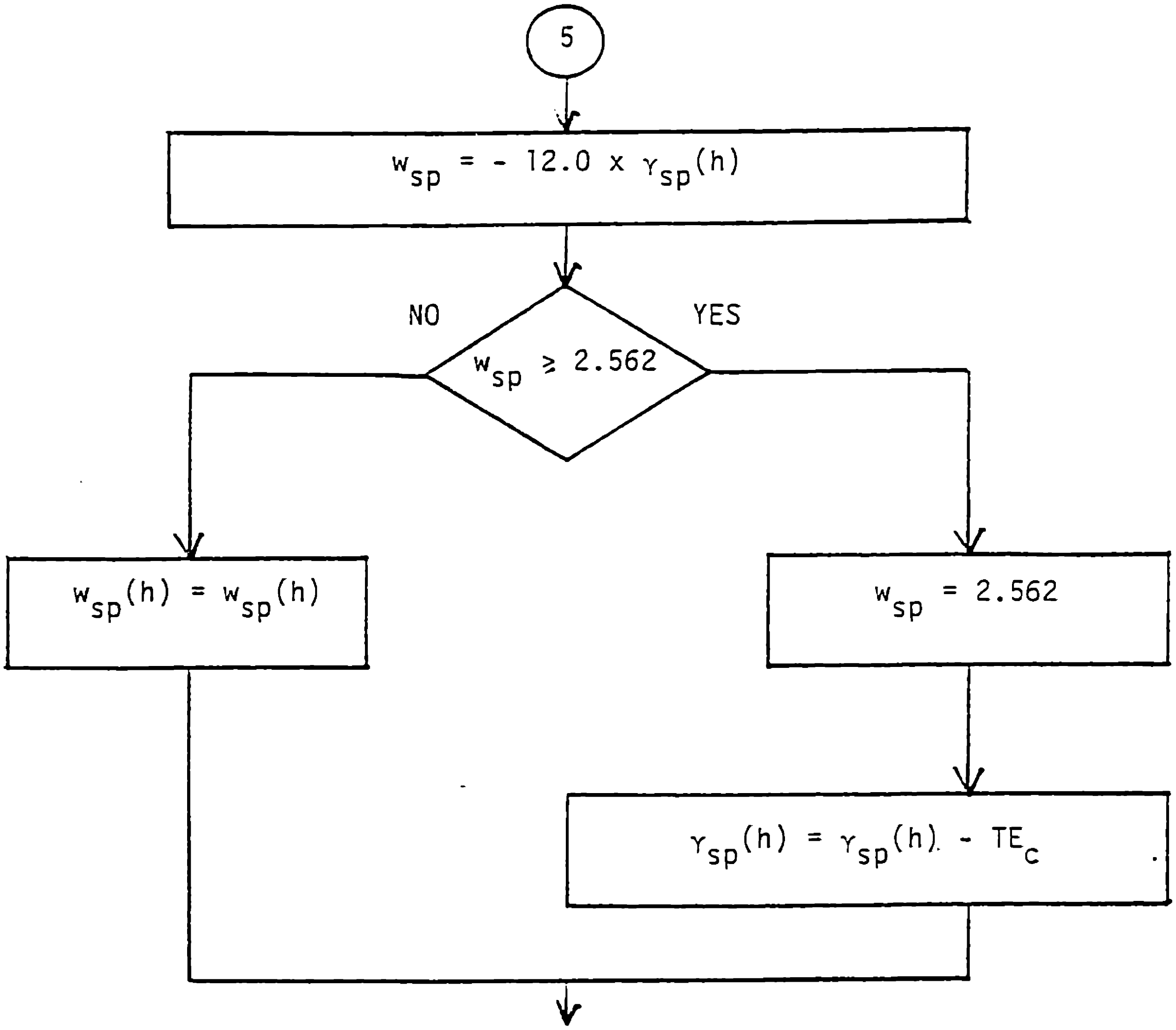

5
$w_{sp} = - 12.0 \times \gamma_{sp}(h)$
NO
YES
$w_{sp} \geq 2.562$
$w_{sp}(h) = w_{sp}(h)$
$w_{sp} = 2.562$
$\gamma_{sp}(h) = \gamma_{sp}(h) - TE_c$

Figure 4.3.2 Q_H and w_{sp} computations.

characteristics of the similar one in w_{let} and w_{mak} calculations.

5. Q_{H1} (the proportional heat) is calculated.
6. The hysteresis cycle for the back-up heaters is computed.
7. w_{sp} is computed.

4.3.5 SATURATION LINE ENTHALPIES CALCULATIONS

These are two linearized functions of the pressure and they are computed by equations (3.3.30) and (3.3.31).

4.3.6 CONDENSED WATER FLOW CALCULATIONS

Equation (3.3.35) is implemented in the algorithm to calculate w_c.

4.3.7 FLASHING FLOW CALCULATION

This block is implemented with the following characteristics:

1. When $h_w - h_f \leq 2\ w_{fl}$ is considered as a quasi steady state flashing, thus w_{fl} is given by equation (3.3.22).
2. If it is an outsurge and $h_w - h_f \geq 2$, the flashing is taken into acount as a natural flashing, then w_{fl} is given by equation (3.3.36).
3. If $h_f > h_w$ w_{fl} is equal to zero.
4. At insurge conditions natural flashing is zero, and the quasi steady state flashing is negligible.

All these conditions are shown in Figure 4.3.3.

4.3.8 SPECIFIC VOLUME COMPUTATION

v_f is computed by the linearized equation (3.3.33).

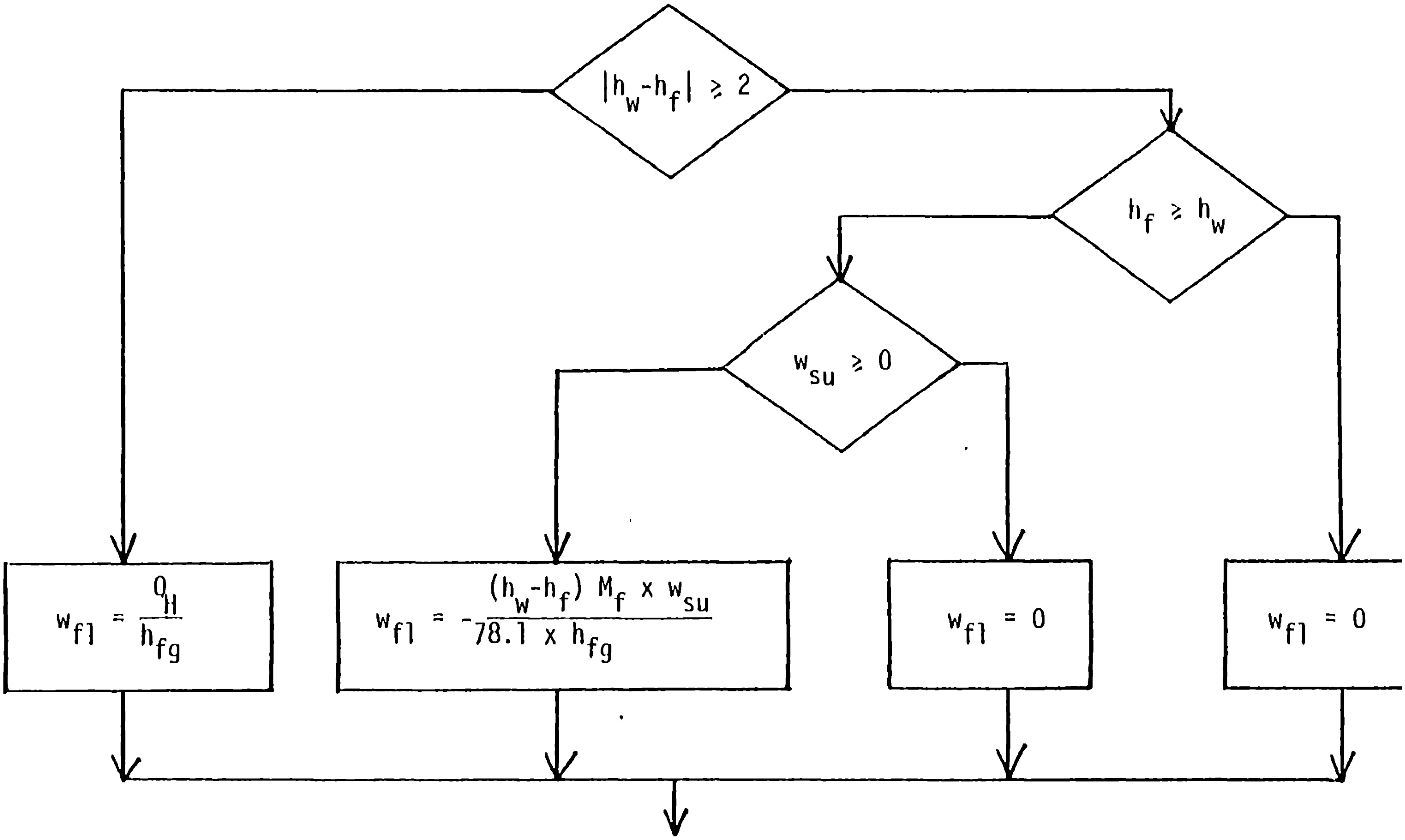

$|h_w - h_f| \geq 2$
$h_f \geq h_w$
$w_{su} \geq 0$
$w_{fl} = \frac{Q_H}{h_{fg}}$
$w_{fl} = -\frac{(h_w - h_f)\, M_f \times w_{su}}{78.1 \times h_{fg}}$
$w_{fl} = 0$
$w_{fl} = 0$

Figure 4.3.3 w_{fl} computation

4.3.9 LEVEL (L(t)) DETERMINATION

The inputs required to calculate the level are now known. The level is next computed by using equations (3.4.6) where $V_f = M_f \times v_f$.

4.3.10 SURGE ENTHALPY CALCULATION

Although the expression to be calculated is w_{su} $(h_{su} - h_f)$, the new term is only h_{su}. h_{su} has the following characteristics:

1. If $w_{su} > 0$, $h_{su} = h_{su}$.
2. If $w_{su} < 0$, $h_{su} = h_f$.

This behavior is shown in Figure 4.3.4.

4.3.11 PRINT SEQUENCE

The pressure P(t), the level (t), and the time t are printed.

4.3.12 PRESSURE INTEGRATION

The $\dot{P}(t)$ is computed by using equation (3.4.1). After that P(t + T) is obtained by numerical integration (equation 4.2.1).

4.3.13 WATER ENTHALPY INTEGRATION

The $\dot{h}_w(t)$ is computed by using equation (3.4.4). After that $h_w(t + T)$ is obtained by numerical integration.

4.3.14 STEAM MASS INTEGRATION

The $\dot{M}_g(t)$ is computed by using equation (3.3.11), under the assumption that $M_s \simeq M_g$. After that $M_g(t + T)$ is obtained by numerical

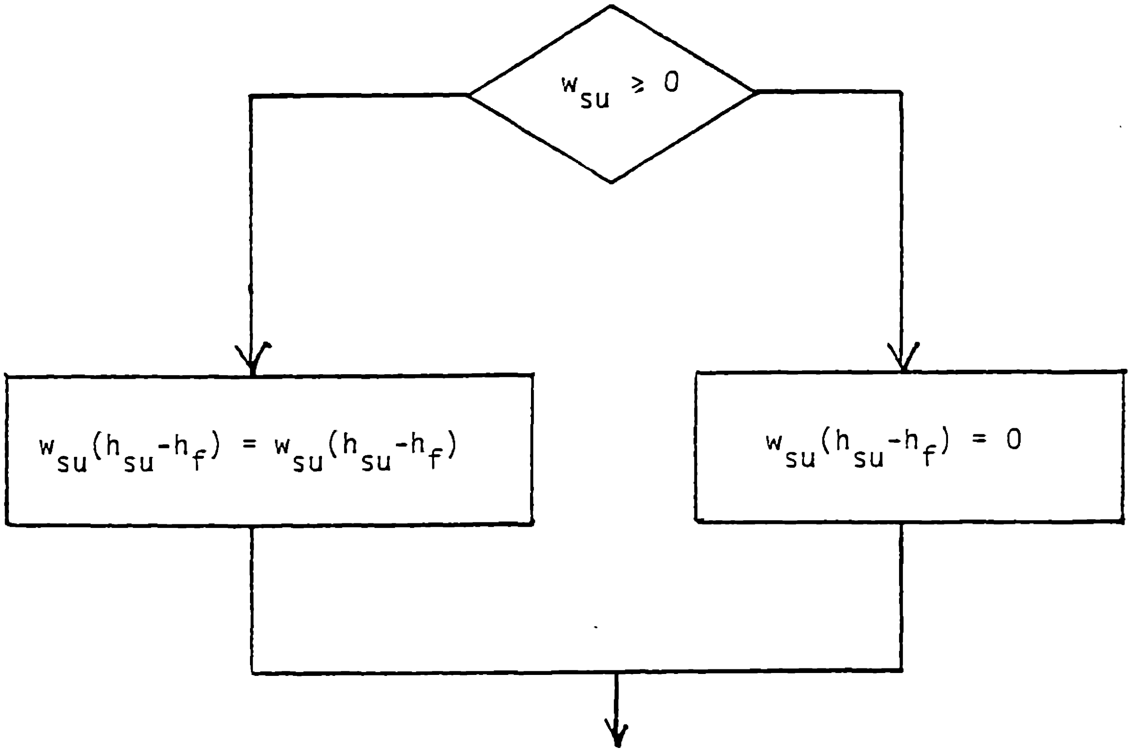


Figure 4.3.4 $w_{su}(h_{su}-h_f)$ computation.

integration.

4.3.15 WATER MASS COMPUTATIONS

The $\dot{M}_f(t)$ is computed by using equation (3.3.12), under the assumption that $M_w \simeq M_f$. After that $M_f(t + T)$ is obtained by numerical integration.

4.3.16 ITERATION

If the simulation is not stopped, the process is recycled to the beginning making the shift to calculate the next time step, so $F(t + T) = F(t)$ now.

4.4 THE PROGRAM

A code performing the functions explained by the flow diagrams has been written and run on a TI-59 calculator.

The code is written in A.O.S. language and it has features that allow us to introduce several values as a function of time for the w_p input. Also all the points for the pressure and level can be changed at any instant of the calculations. The code is composed of a main body and two subroutines. Subroutine X^2 calculates the PID function, meanwhile subroutine $\sqrt{X}$ makes the consistency checks on w_{let}, w_{mak}, w_{sp}, and Q_H.

In general, the code takes a fairly long time to perform its work, because of the low capacity of the calculator (one iteration takes about 46 s). That means the simulation is far from being in real time.

The code listing and the users manual are in Appendix H.

4.5 CONTROL SYSTEM TUNING

The final section of this chapter is devoted to explaining how the control system is tuned, and which particular constants are used in the design. The final part of the section has the results of the study cases and an analysis of the data obtained.

4.5.1 SIMULATION INPUT DATA

Most of the specific characteristics of the plant and the control system have been stated in previous chapters, but one very important parameters which has not yet been explained is the constant for the DC motor simulation.

Because in this work an actual implementation will not be performed, it will use generic values for small DC motors. If an actual implementation were made, the transient calculations would have to worked out again with the specific constants. From Reference 4.1, a generic value for the motor constants is given to be:

$K^m I_f$ = 10 newton-m/amp

R_a = 5 x (Ω)

B_x = 0.5 newton-m/rad/sec.

Substituting these values in equation (3.4.18), the motor constant (K^m) becomes

K^m = 2.857.

This K^m value will be used in the four motors involved in the design because they are assumed to be similar.

The list of initial conditions for the simulation follows:

$P(o) = 11.93$ (MPa)

$L(o) = 0.69$ (m)

$V_g(o) = 2.605$ (m^3)

$V_f(o) = 5.76$ (m^3)

The above data were obtained from Reference 4.2.

Because the behavior of the model will be compared with real outputs obtained from the ship's sea trials, more specific data related to the sea trials are added (Reference 4.3):

T_{HL}	=	270°C	(hot leg temperature)
T_{CL}	=	260°C	(cold leg temperature)
P_{CL}	=	12.41 (MPa)	(cold leg pressure)
T_{mak}	=	37.2°C	(buffer seals temperature)
P_{mak}	=	12.75 (MPa)	(buffer seals pressure)

Assuming the cold leg conditions is that of the sprays, and the hot leg conditions is that of an in-surge

v_{sp}	=	$1.26\text{x}10^{3}$	(m^3/kg)
h_{sp}	=	1134.16	(joules/kg)
v_{su}	=	$1.29\text{x}10^{-3}$	(m^3/kg)
h_{su}	=	1183.52	(joules/kg)
v_{mak}	=	$1.0\text{x}10^{-3}$	(m^3/kg)

By combining the above data, a value for $M_f(o)$ and $M_g(o)$ is obtained:

$M_f(o) = 1153$ (kg)

$M_g(o) = 180.75$ (kg)

The water enthalpy $h_w(o)$ comes from the linearized expression (Eq. 3.3.30) at P = 11.93 (MPa).

$h_w(o) = 1499.13$ (joules/kg)

Finally the set point for the starting of spray action is 12.10 (MPa) (Ref. 4.2).

4.5.2 CONTROL SYSTEM TUNING

The procedure to tune up a PID controller is as follows:

1. Remove all integral and derivative action, and tune the proportional mode to give the desired response characteristics, ignoring any offset.
2. Increase the proportional gain, and attempt to restore the response characteristics by adjusting the derivative time.
3. Adjust the integral constant to remove the offset.

The gain of the motor amplifier was standardized to a value of 10, then the model was subjected to a positive step function of w_p of +2.47 (kg/s). Under this input the controller constants were changed until the response was satisfactory. The results for the tuning process are shown in Figure 4.5.1. The final setting was found to be:

K_1	=	1.0	(proportional gain)
K_2	=	0.0	(inverse of integral time)
K_3	=	10.0	(derviative time)

Two comments follow:

1. What we are looking for is to reduce the overshoot and to speed up

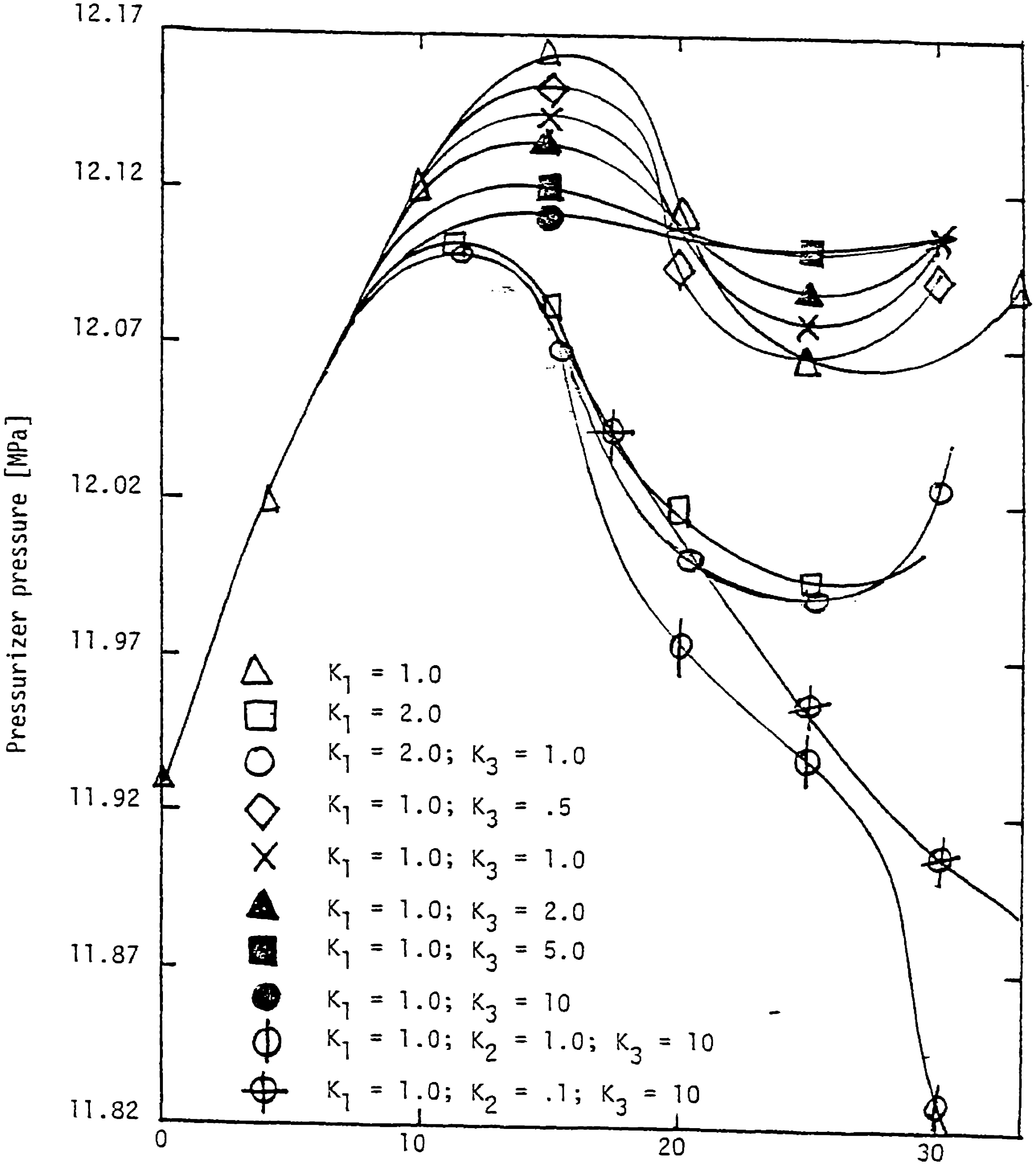


Figure 4.5.1 PID controller tuning.

the response without introducing instabilities.

2. The final result of $K_2 = 0.0$ indicates that for practical purposes the controller is a PD controller. This conclusion is similar to that reached by the designers of the actual control system--18 years ago when they installed a PD controller (Reference 4.2).

4.5.3 STUDY CASES

After tuning the system, one may want to compare the behavior of the model to the behavior of the real plant. It turns out to be very difficult to do this because the N.S. Savannah propulsion plant was decommissioned several years ago, therefore data about its performance are scarce and difficult to find.

Nevertheless, records of the initial sea trials of the ship are available, and they contain some pressurizer trainsient records. The problem with this type of information is that it does not contain any reference to the shape and size of the surge to or from the pressurizer.

The alternative solution is to test several shapes and sizes of surges until the pressurizer water level curves (the sea trial level curve and the simulated level curve) take a similar shape. The fact that the levels follow a similar pattern does not ensure that the surges are similar because the surge flow is a function of the time derivative of the pressure and this derivative is different in the simulated model than in the seal trial results.

A correction, taking this effect into account, can be added:

$$w_{su} = w_{su}^{*} + \frac{V}{v^2}\frac{\partial v}{\partial P}\left(\frac{\partial P^{*}}{\partial t} - \frac{\partial P}{\partial t}\right) \tag{4.5.1}$$

where V = primary water volume

* = values from similar level behavior test

$$\frac{V}{v^2} \frac{\partial v}{\partial P} \simeq - 4.892 \times 10^{-5}$$

Because of the way the sea trial data are presented, this kind of comparison was only possible with insurge cases.

It should be kept in mind that the behavior of the simulated plant has not been forced to be similar to the old plant. Rather, the results of the simulation show how the behavior of the new system will differ from that of the old system. Although the model has several approximations and the computer code also has a few approximations to fit it inside the small calculator, also the controller constants are different, and the inputs to the model are only approximated to the plant, the behavior of the model resembles fairly well the behavior of the actual plant. (No quantification of the resemblance is added because of the approximations made, which makes that number of little value.)

What is apparent from the simulation is that the new control system handles the overshoots of the response better than the old system.

The study cases were:

1. Transient from 40 percent load to base load.
2. Transient from base load to 40 percent load.
3. Transient from 60 percent load to base load.
4. Transient from 40 percent load to base load without any controlling action.
5. Transient from base load to 40 percent load without any controlling

action.

6. Transient from 40 percent load to base load adding an automatic letdown valve.
7. Transient from base load to 40 percent load adding an automatic letdown valve.

By base load is meant the low power at which all normal ship requirements other than propulsion power are met.

The shapes of the insurges and outsurges applying to the model are shown in Figures 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, and 4.5.7.

To change from a system without an automatic letdown valve to one with automatic letdown valve, the letdown valve amplifier constant in the code was simply changed from 0 to 10.

Figures 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, and 4.5.7 also show the results of all the tests, and, in the case of insurges, the corresponding sea trial results.

Most of the discussion that follows is related to the insurge pressure curves because these curves show the action of the PID controller on the spray valve. The outsurge curves are strongly influenced by the hysteresis heaters and their behavior should not change very much from the original controller to the new one. (The proportional heater gets saturated very soon with the kinds of transients under consideration.) On the other hand, the PID action is evident in the outsurge level curves, where the makeup valve acts upon a PID control signal. The special case when makeup valve and letdown valve are considered together shows the effect of the PID action in both cases.

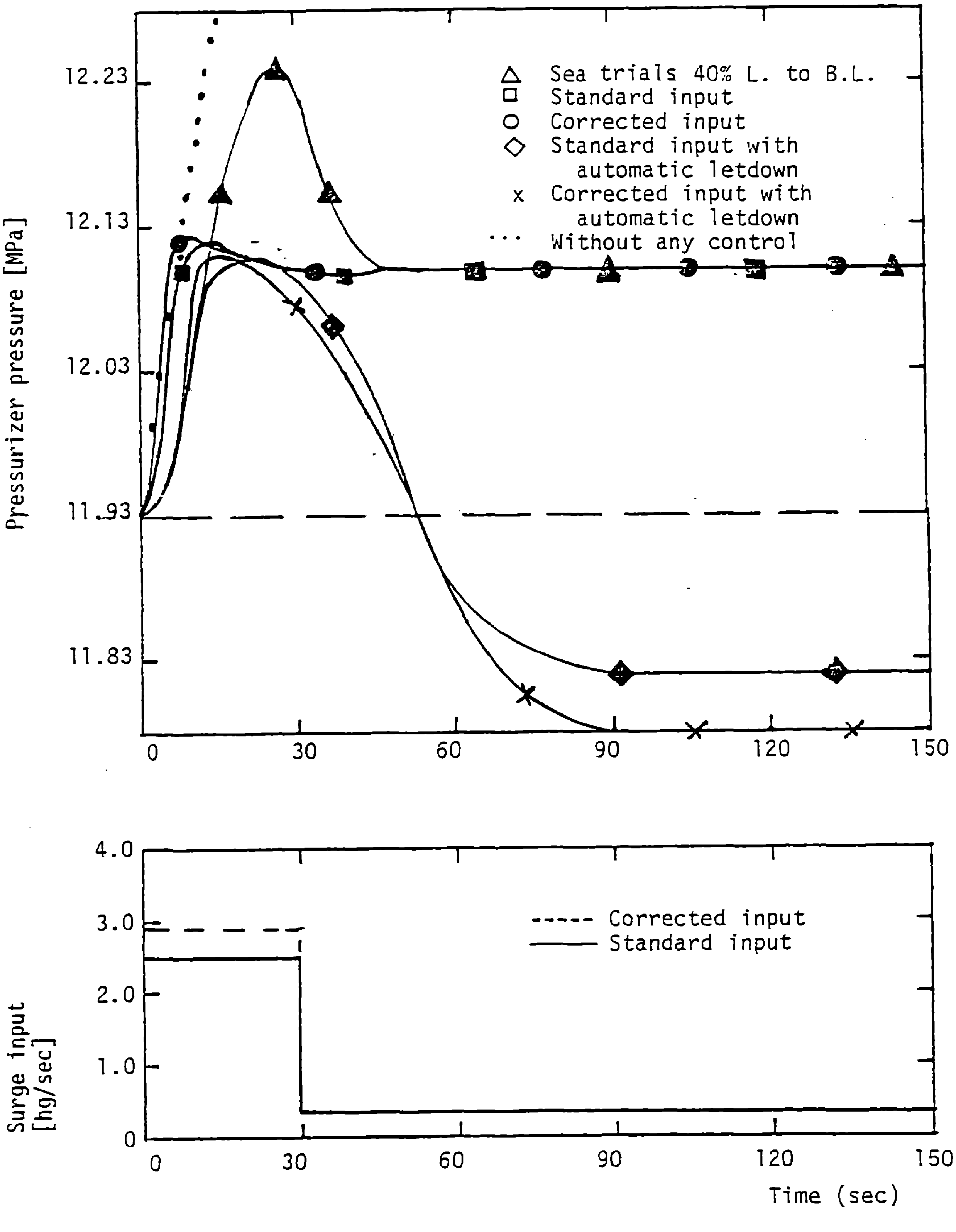


Figure 4.5.2 Pressurizer pressure behavior under transient conditions.

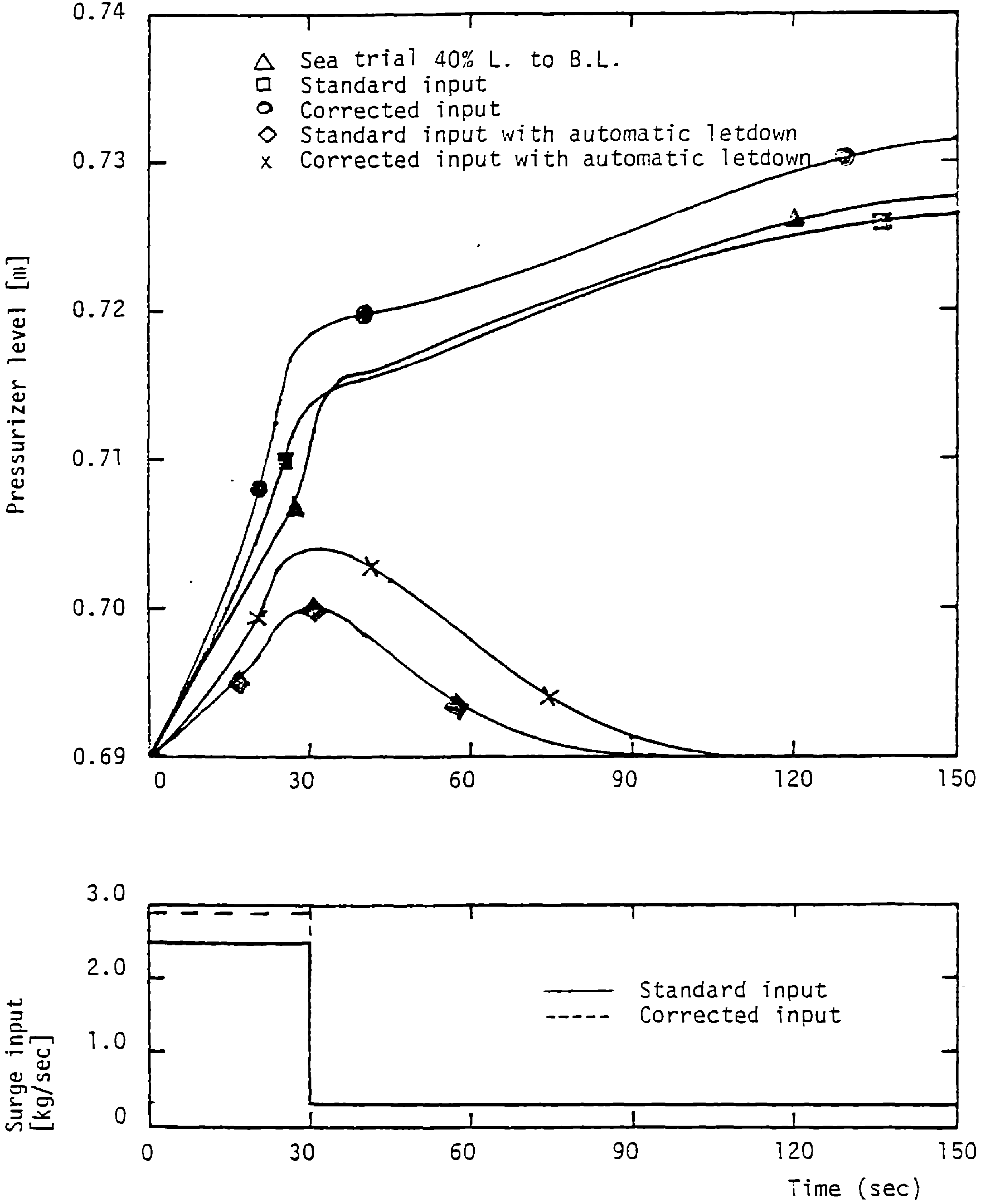


Figure 4.5.3 Pressurizer level behavior under transient conditions.

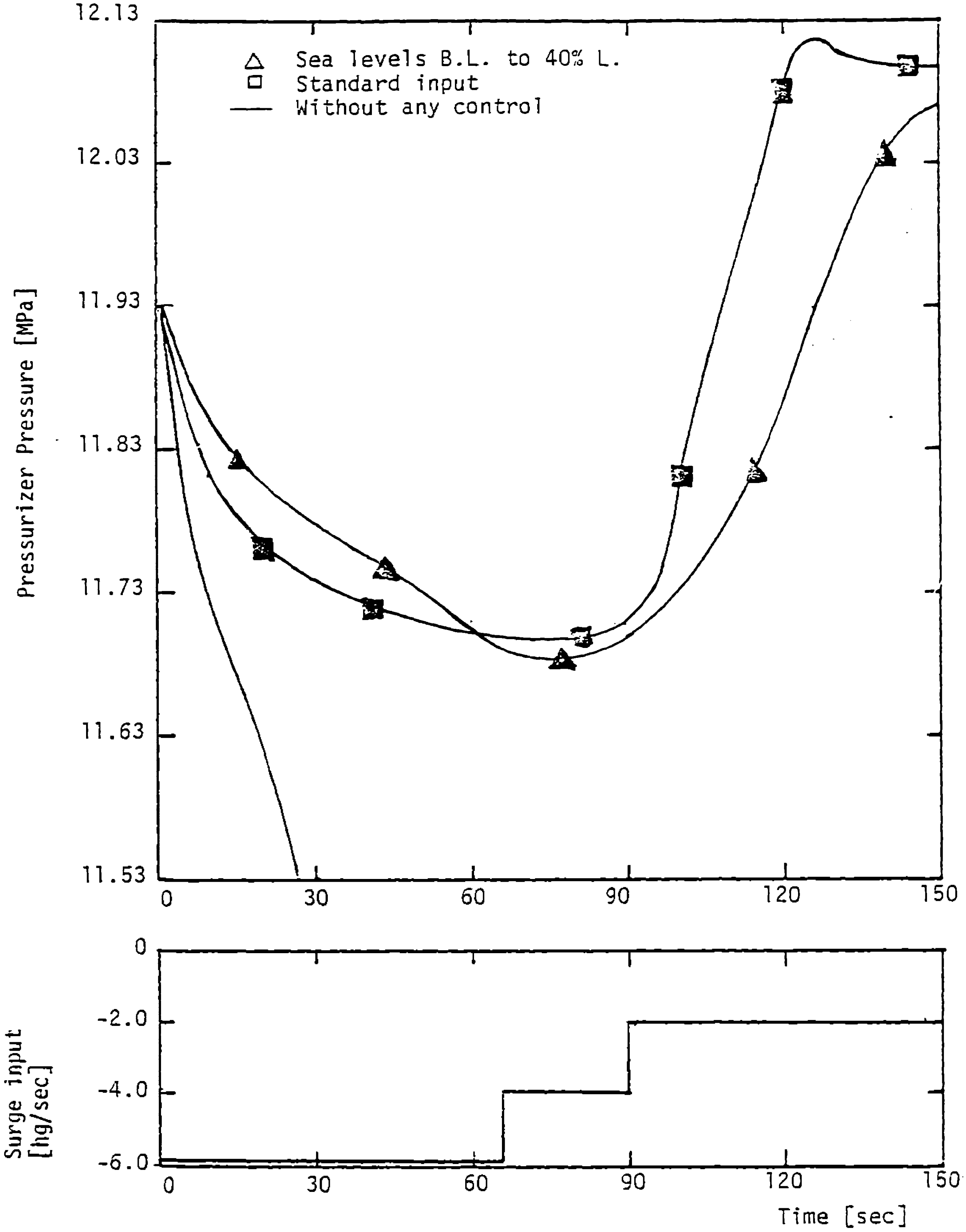


Figure 4.5.4 Pressurize pressure behavior under transient conditions.

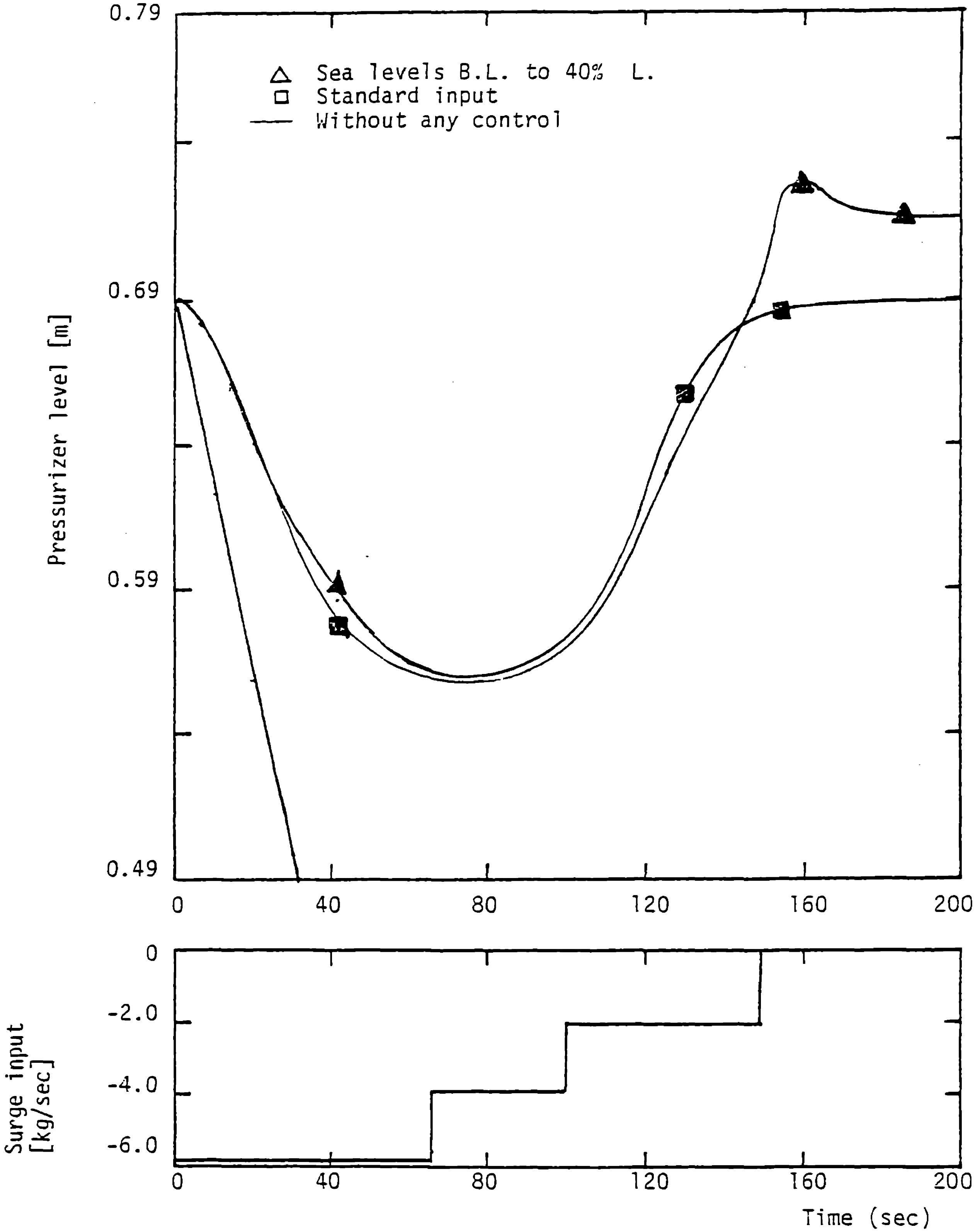


Figure 4.5.5 Pressurizer level behavior under transient conditions.

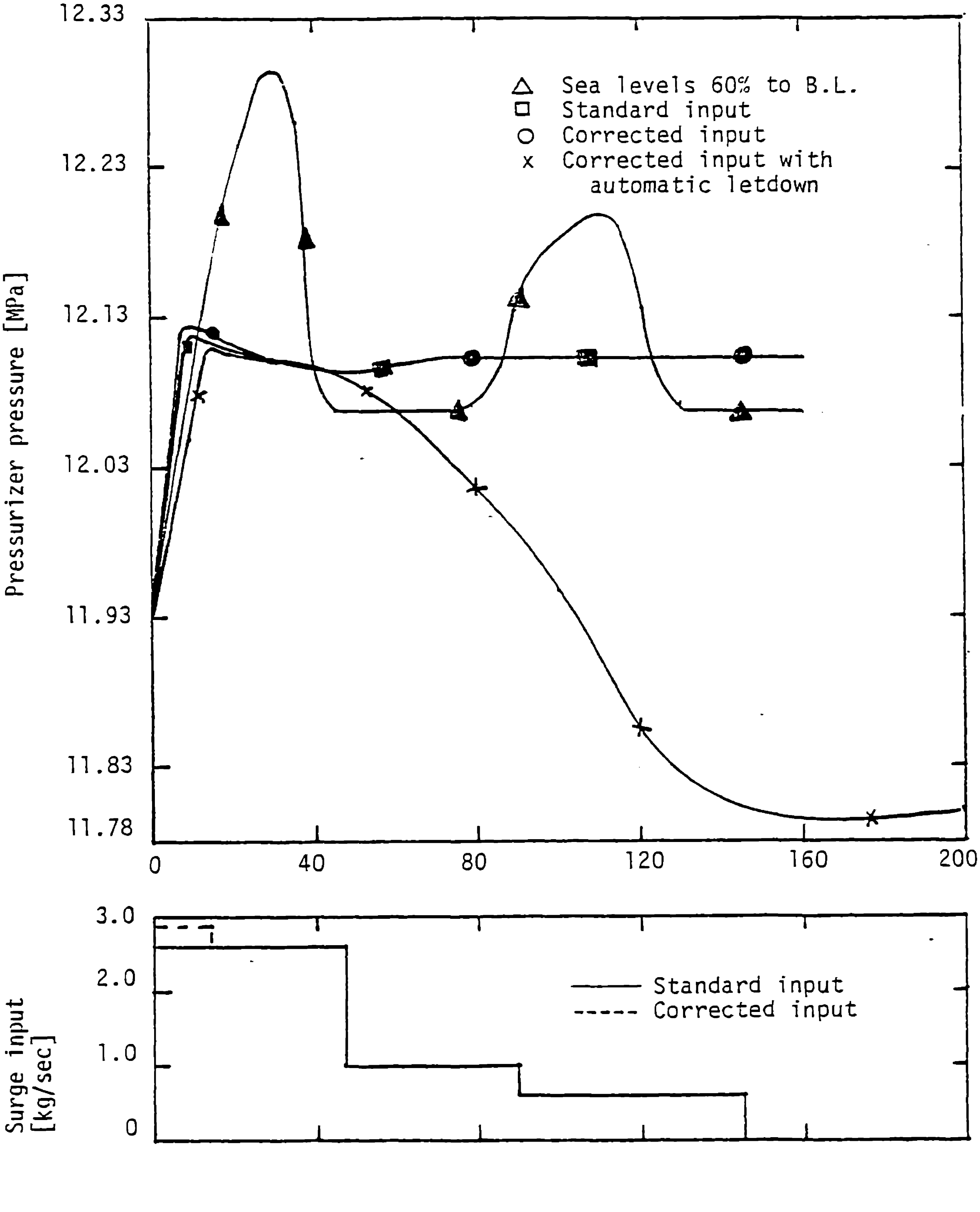


Figure 4.5.6 Pressurizer pressure behavior under transient conditions.

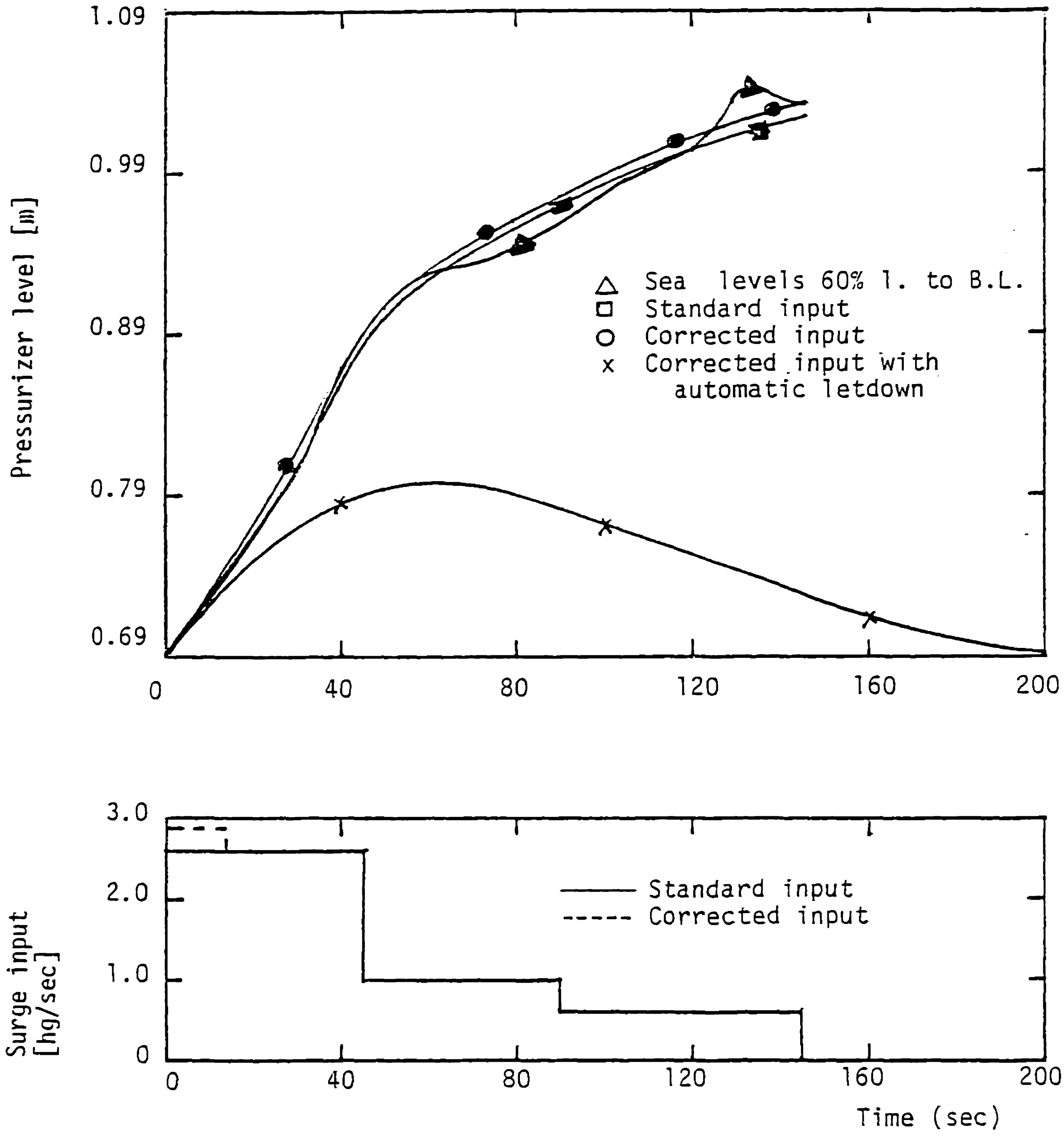


Figure 4.5.7 Pressurizer level behavior under transient conditions.

From Figure 4.5.2 we can see that the pressure overshoot with the new control system reaches 0.13 percent and the rise time is approximately 7 sec. Both numbers indicate the transient is rapidly controlled and kept inside a safe envelope of limits. This characteristic of the pressure response appears in all the study cases.

The level behavior during an outsurge transient is shown in Figure 4.5.3 here the strong derivative actions, required by the controller, damps the level behavior in such a way that no overshoot appears and the pressurizer level reaches the stead state smoothly. Because the levels do not cross the reference line, this behavior is exactly the same for an outsurge case with or without automatic letdown valve.

Figures 4.5.2 and 4.5.3 show the pressure and level behavior of the system when it is subjected to an insurge, and the control system does have an automatic letdown valve. Both parameters show sharp differences from the case without automatic letdown valve.

First, the level reaches the steady state at its reference value although the insurge has not yet finished, and it reaches the steady state without showing an overshoot behavior. Second, the automatic letdown flow produces a net outsurge to recover the original level; this net outsurge reduces the pressure to a point below its reference value. The pressure approaches the set point before the backup heaters are required to go into action, and the proportional heater alone is trying to recover the pressure; the pressure will be fairly constant at 11.83 (MPa) value until the proportional heater raises the water enthalpy to a flashing region, then the pressure will return smoothly to its reference value.

Figure 4.5.6 and 4.5.7 also show an insurge transient due to a greater input. Although the input is higher than the previous one, the control system does handle the transient by obtaining an overshoot of 0.14 percent and a rise time of approximately 7 sec in the pressure.

Finally, all the figures related with transients also show what the behavior of the pressure and the level if there is no control at all. These curves clearly show the positive controlling action of the designed control system.

Recall that the model of the pressurizer is an isolated model from the primary system, where the inputs w_{su} and h_{su} are set arbitrarily by the designer in order to test the control system. The fact is that the input to the pressurizer (the surge flow) does depend on the output of the control system because the surge flow is a function of the time derivative of the pressure. A comprehensive way of considering this is to model the pressurizer together with the primary system, but that is beyond the scope of this thesis. Another way to verify this effect is by the correction implied in equation 4.5.1. Figures 4.5.2, 4.5.3, 4.5.6 and 4.5.7 show the pressure behavior for the standard insurge and the pressure behavior for an insurge approximated by equation 4.5.1. The overshoot is higher and the rising time is smaller that the test case, but the fact is the control system does handle the transient without difficulty.

REFERENCES

4.1 Automatic control engineering. Francis H. Raven. McGraw-Hill. 1978.

4.2 N.S. Savannah training manual, ship and system descriptions, Vols. I and II. N.S. Savannah technical staff, Babcock and Wilcox, and Wilcox-Todd Shipyard, Galveston, Texas.

4.3 Savannah nuclear power. N.S. Savannah power operation to 100 percent. New York Shipbuilding Corporation, Camden, N.J.

4.4 New algorithms for control. Donald R. Coughanower. Chemical Engineering, June 2, 1969.

CHAPTER 5

SUMMARY AND CONCLUSIONS

The study has been performed up to the point when the preliminary design stage has been completed. Also a new pressure and volume control system has been designed and tested with a simple pressurizer model, in a simulation code.

The steps followed to complete the preliminary design stage were:

1. Organization of surveillance, data validation, and control tasks in functional blocks.
2. Study of the input-output parameters corresponding to the specific case of the N.S. Savannah nuclear propulsion plant.
3. Preselection of eight feasible digital architectures by using a weighting factor method.
4. Hardware design of the eight preselected alternatives.
5. Development of a more accurate figure of merit (EMV) to choose the best alternative.
6. Selection of the optimal architecture for surveillance, data validation and control functions

The steps followed to complete the design of the pressure and volume control system were:

1. Selection of the stability and transient analysis method (time domain analysis).
2. Development of the state equations for the pressurizer.
3. Selection of the controller (PID).
4. Development of the transfer functions for the plant and the control

system.

5. Development of a simulation code.
6. Tuning up of the controller by running study cases with the simulation code.

The remainder of the chapter is concerned with specific conclusions related to the preliminary design, specific conclusions related to the pressure and volume control system design, and general recommendations.

5.1 PRELIMINARY DESIGN CONCLUSIONS

1. A robust methodology to design the optimal surveillance, data validation, and control system for a nuclear propulsion plant has been developed. The method is general enough to be used in nuclear power plants and even in any complex process that has to be monitored and controlled.
2. If the digital architecture is wanted for only process controlling purposes, the design that should be chosen is the dual star serial transmission architecture (Figures 2.4.7 and 2.5.6).
3. If the digital architecture is wanted only for data validation and surveillance functions in the marine envionment, the global data bus architecture should be chosen (Figures 2.4.3 and 2.5.7).
4. For a combined task of controlling the process and performing data validation and plant surveillance, the dual star serial transmission architecture will be favored by a risk-averse decision maker (Figures 2.4.7 and 2.5.6).
5. If the dual star serial alternative architecture is chosen, the

software package should be debugged up to a a probability of software failure = 5 x 10^{-3}.

6. The final conclusions favor the use of distributed systems over the centralized ones. The conclusions were reached in an environment of assumptions unfavorable to the distributed alternative. This fact strengthens even more the decision to opt for distributed systems. Moreover, several other attributes favoring distributed architectures were not included in the figure of merit, e.g.: expandability of the system (SCDS grows as the plant grows), external disruption resistance (the distributed physical location of the processes gives protection against external disruptive effects), degraded mode operation (the system can survive failures internally or externally caused up to a certain degree of damage.

5.2 PRESSURE AND VOLUME CONTROL SYSTEM DESIGN CONCLUSIONS

1. The pressure and volume control algorithm can be fit in a very small microprocessor. The limitation is the processing speed of the microprocessor to keep pace in real time.
2. A digital controller does control the pressure and volume in the pressurizer as well as the original pneumatic controller. From the study cases, the digital controller shows a greater flexibility to obtain transient responses from the plant with low overshoots (0.13 percent) and fast-rising times (approximately 7 sec).
3. From an strict control viewpoint the introduction of an automatic letdown valve is advisable as it reduces even more the peak in

pressure and controls the level during insurges. This conclusion can be modified for other reasons (see Section 5.3).

4. To control the pressure and the volume requires a PID controller with the proportional gain set to 1 and the derivative time set to 10, and the inverse of the integral time set to 0.

5.3 GENERAL RECOMMENDATIONS

1. If the procedure developed to design and select a digital architecture is used to design a surveillance, data validation and control system (SDCS) for a land-based commercial nuclear power plant, the following suggestions are made:
   - The environmental factor used to calculate the failure rate should be adapted to the expected environment.
   - By studying in detail the inputs and outputs of the plant, a new division of the tasks has to be made.
   - After calculating the memory requirements and the data transmission requirements, the new alternatives can be designed.
   - Because of the larger size of the plant, the distributed alternatives should be studied loop by loop (and not using an average case as in this work).
2. The figure of merit used in this thesis--expected monetary value (EMV) does not consider the personal attitudes of the decision maker. The preference structure of the decision maker should be added to the figure of merit to make the final decision as close as

possible to the real world.

3. For future work, a more detailed analysis of the quantification of the payoffs is recommended. In this work, this task was complicated by the lack of updated information related to those quantities.
4. This thesis was developed under the assumption that a SDCS has only two states, operating or failed. A more realistic approach is to consider a third state of degraded mode operation. This topic by itself requires a separate study.
5. This thesis used a figure of merit under one attribute domain (economic payoffs), but if the study were expanded to large nuclear power plants, the analysis can be made under a multiattribute domain (economic payoffs, general plant safety, availability, etc.)
6. Another field of improvement is to assess how the environmental factor (π_E) used to calculate the failure rates, could be affected by exposing the digital device to nuclear radiation; this case is especially interesting in the case of distributed digital systems because some of the processors will be located closer to radiation sources than a central computer would be.
7. This work has considered eight basic architectures. The basic architecture can be extended by adding redundancies in critical points of the design. For further work in the field, it is recommended that sensitivity analysis be performed on the figure of merit by introducing such redundancies in the design. The analysis should start from the engineering design viewpoint, then the fault

tree and equations should be restructured correspondingly, the costs should be adjusted, and then the sensitivity study can be performed.

8. Although the cost of producing the special software can be reduced by using common algorithms in every processing block, the cost of producing the software needed for the SDCS always will be the dominant factor in the cost figure. That leads to the recommendation for future work to choose a hardware package with the maximum available software possible, decreasing in that way the cost of developing unique software.

9. The inclusion of protected memory devices (ROM) should be considered in future designs.

The following set of recommendations concerns the design of a pressure and volume control system.

10. Although it is not part of the scope of this thesis, it has been noted that the model used to simulate the pressurizer behavior behaves consistently faster than the actual plant. This observations is in keeping with the results obtained by Geffray in his thesis (Ref. 3.3). For the purposes of this work, this behavior however does not make much difference from the actual behavior, and will not affect the conclusions, but for the data validation task, some of the assumptions should be relaxed in order to get a response closer to the real one.

11. From a strict control viewpoint, the use of an automatic letdown valve appears to be desirable, but safety considerations, or the

possibility of a loss of coolant accident (LOCA) due to a failure in the control system could preclude implementation of such a device. To have a LOCA due to a failure in the automatic letdown valve is a real possibility because the total inventory of water of this nuclear system is small (approximately 20 m^3).

13. As a conclusion of this work, and from past experience, control of pressure and volume in a nuclear system is readily achieved using a PD controller. The constants for the controller come from the tuning-up of the PD controller attached to the specific plant.

APPENDIX A

N.S. SAVANNAH REACTOR FEATURES

This appendix is included only for illustrative purposes. More details about the N.S. Savannah nuclear plants are given in Reference A.1.

The description of the N.S. Savannah nuclear propulsion plant has been divided into four parts: (1) the basic working cycle; (2) the pressurizing system; (3) the purification system; and (4) the secondary system. Figure A.1 is a block diagram with all the main components of the ship's nuclear propulsion plant.

A.1 BASIC WORKING CYCLE

The basic working material--and neutron moderator--for the Savannah reactor is demineralized and purified water. This "primary water" is circulated between the reactor and two heat exchangers (steam generators). The water is force-circulated at the rate of 16,000 gallons per minute, at a mean temperature of 508°F. The water is pressurized to 1750 psia.

The maximum total heat generated by the reactor is 70 MW or about 240 million Btu/hr

The primary water enters the lower portion of the reactor, and leaves near the top. The circulation takes place in two independent loops. Each coolant loop consists of a heat exchanger and two pumps. This two-loop arrangement provides ample flexibility to maintain reduced-power cooling of the reactor with one heat exchanger and one pump. Such cooling would be necessary after reactor shutdown or setback, to remove

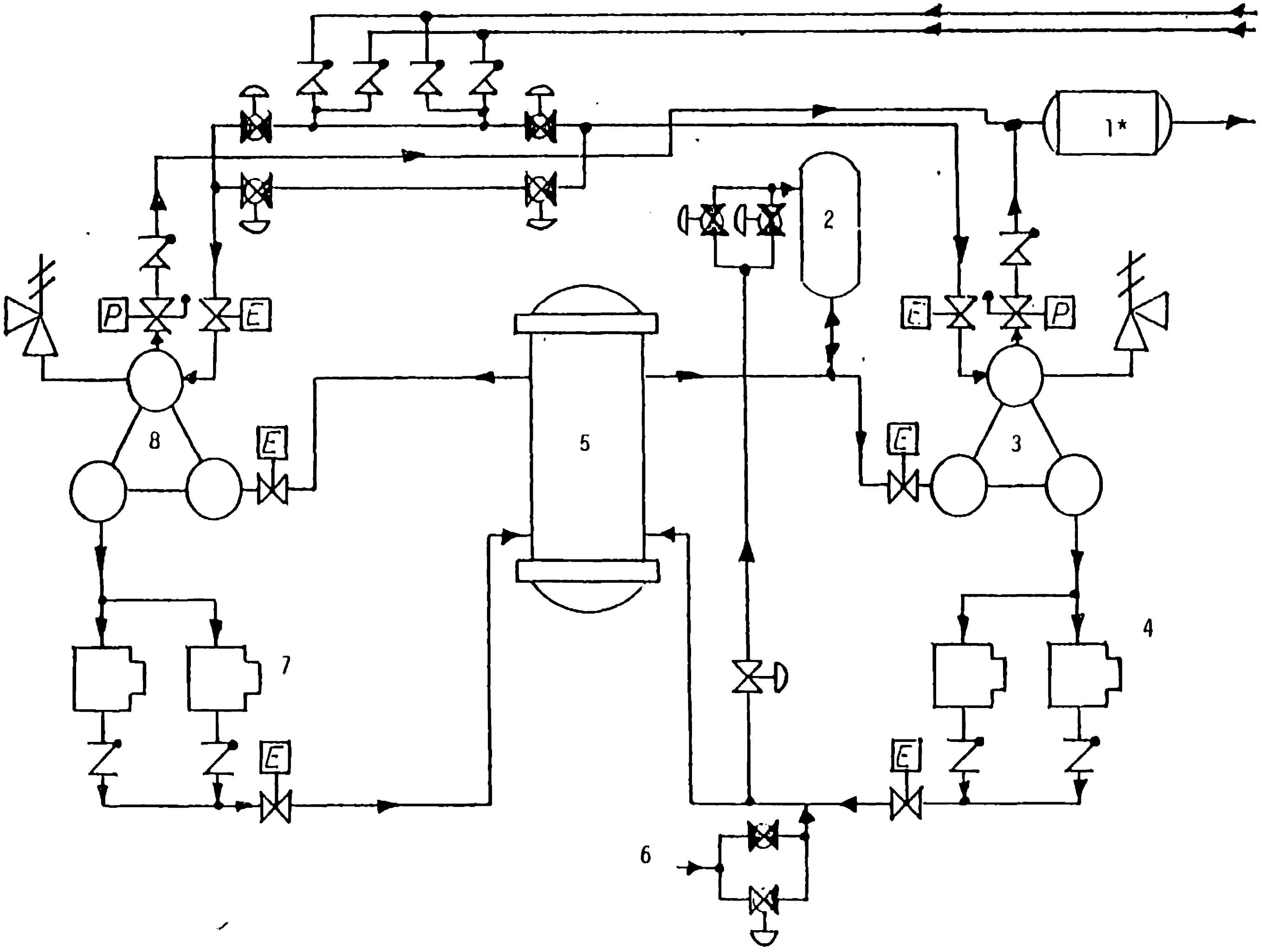


Figure A.1 N.S. Savannah Nuclear Propulsion Plant.
*See legend on next pages.

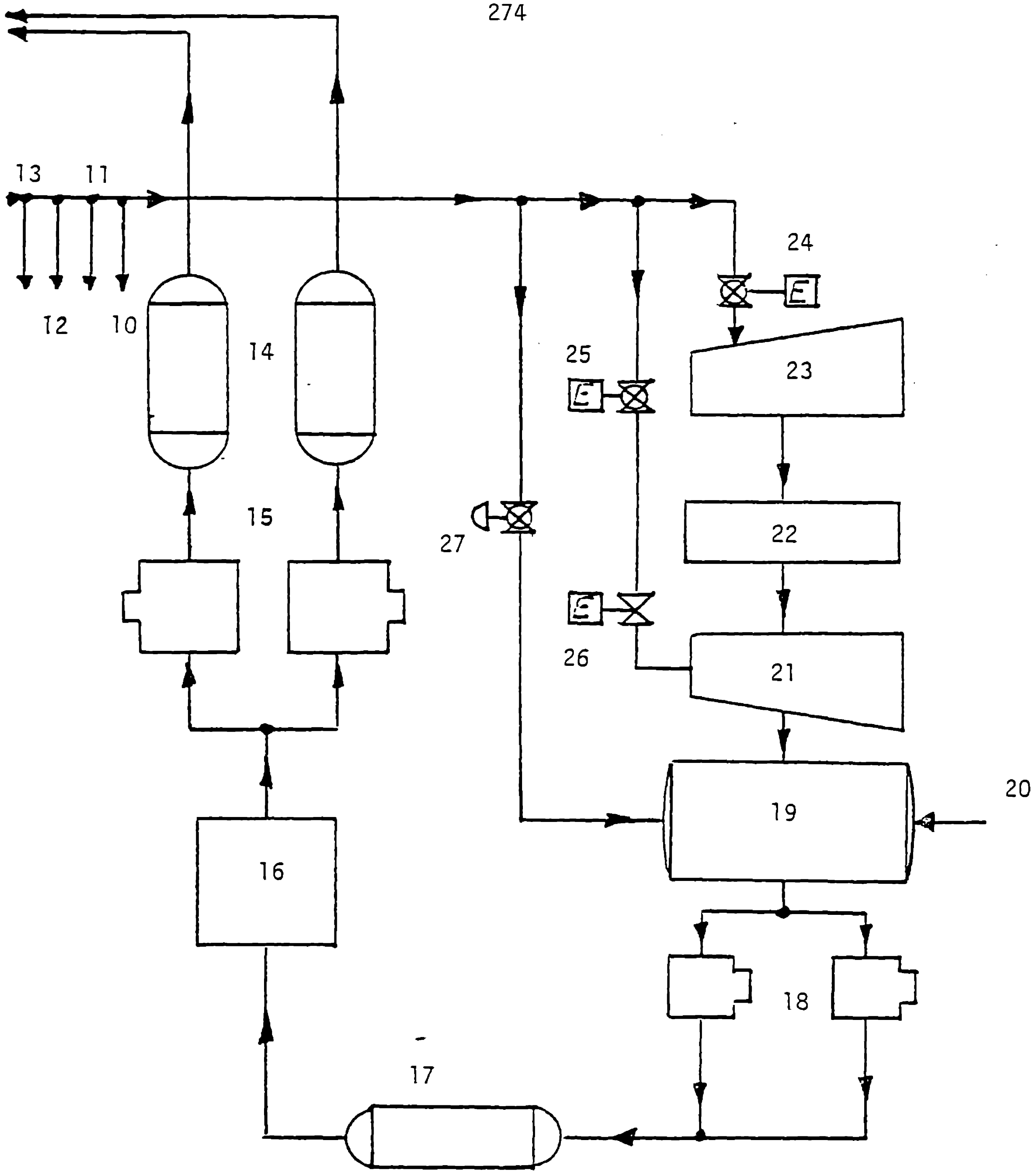
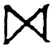
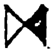
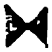
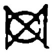
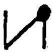
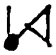
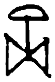
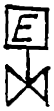
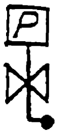
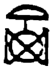
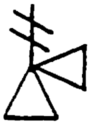


Figure A.1 (continued).

	Valve normally open
	Valve normally half open
	Valve normally closed
	Globe valve
	Check swing valve
	Check stop valve
	Diaphragm operated valve
	Electrical motor operated valve
	Quick closing valve piston operated
	Globe valve diaphragm operated
	Relief valve

1. Steam separator
2. Pressurizer
3. Starboard steam generator
4. Starboard primary pumps
5. Reactor vessel
6. Makeup flow
7. Port primary pumps
8. Port steam generator

10. Steam to main ejectors
11. Steam to low pressure steam generator
12. Steam to main feed pumps

13. Steam to main turbo generators
14. High pressure heaters
15. Main turbo feed pumps
16. Deaerator tank
17. Low pressure heater
18. Condensate pumps
19. Main condenser
20. Seawater injection
21. Low pressure turbine
22. Steam separator
23. High pressure turbine
24. Ahead throttle valve
25. Astern throttle valve
26. Guardian valve
27. Steam bypass to condenser

the decay heat from fission residues.

Each loop contains two electrically operated gate valves that can be closed to isolate the reactor. Appropriate interlocks are provided so that all four gate valves cannot be closed simultaneously once the reactor has started up in normal operation. Position indicators show the amount of gate valve openings at all times. The inlet gate valves (two) are positioned adjacent to the reactor, whereas the outlet gate valves (two) are adjacent to, and ahead of, the heat exchangers. The greater length of outlet piping thus provided acts as an overflow reservoir in the case of power surges with one loop isolated.

The circulating pumps (total of four) are of the canned rotor type. The rotor is mounted vertically above the impeller, and has windings for two speeds, namely: half and full. At full speed, each pump will move 5000 gpm against a head of 70 psi. The pumps are located on the downstream side of the heat exchangers, to minimize problems of radioactivity and corrosivity from the primary water. A check valve is placed on the discharge side of each pump to protect it against back-pressure surges in the primary piping. The pumps are separately cooled by water. The total pumping power required is about one MW (i.e., 250 KW per pump) ... or 1.5 percent of the total reactor power.

The steam generators (total of two) consist of a U-shell, U-tube heat exchanger section, with a steam drum on top. The heat exchanger section contains about 800 stainless steel 3/4-inch O.D. tubes. It is connected to the U-shell heat exchanger by risers and downcomers. The steam drum is equipped with cyclone separators and scrubbers which provide dry saturated steam at the main outlet. The total amount of steam generated is approximately 260,000 pounds per hour at 460 psia, 475°F. Separate feedwater pumps supply make-up water to the steam generators. The heat exchanger water-to-steam cycle is called the "secondary loop" of the reactor plant.

All primary piping carrying water between the reactor and heat exchangers is of type 304 stainless steel, 12-1/2 inch I.D. The design pressure of this piping is 2000 psi. The secondary piping carrying steam from the generating drums to the turbines is 8-1/2 inch I.D., designed for 800 psi. Appropriate steam safety valves and stop-check valves are provided.

A.2 THE PRESSURIZING SYSTEM

A fundamental design feature of the Savannah reactor is that no boiling of the primary water is allowed. As an initial safeguard against boiling, the maximum temperature of the reactor water is de-rated about 100°F below its saturation value at the equilibrium pressure of 1750° psia. But the steam turbines don't know about this de-rating; their demands for steam rise and recede with the ship's operational requirements. Because of these load changes, the primary water pressure will be altered.

The demand for increased steam in the secondary loop means that more heat has to be taken out of the primary loop, thereby disturbing equilibrium conditions. As a result, the reactor pressure is reduced. At lowered primary pressure, some of the water inside the reactor could flash into steam and local or general boiling could occur. Depending on the frequency and severity of load changes, the neutron moderation could upset fission criticality conditions with the ultimate possibility of fuel element burnout.

To prevent this possibility, a pressurizing and relief valve system is provided. The "pressurizer" is an electrically heated pressure vessel in which an auxiliary steam space is maintained in pressure equilibrium with the primary water. The equilibrium pressure (1750 psia) is maintained by the alternate use of electrical heaters or spray-cooling as the transients of the primary system demand.

The electrical heaters are housed in heater wells which heat the primary water (in the pressurizer only) to the saturation temperature, thereby forming a vapor chamber above the water. Spray-coolers are located in the vapor region to reduce the vapor pressure when necessary. In the center of the tank, a standpipe provides the reference leg for water-level control. To meet heavy transients, appropriate steam relief valves and water surge lines are provided.

Due to the reactor stability provided by the Savannah's pressurizer, steam can be delivered to the turbines varying in pressure from 450 psia (at maximum power) to 730 psia (at zero power).

A.3 THE PURIFICATION SYSTEM

Under equilibrium pressure conditions, the primary water will become radioactivated by the neutrons in the reactor core. Also, because of the temperatures involved, corrosion products will accumulate. And, furthermore, there is always the possibility that some fission products may find their way into the primary water. To remove the radioactive and corrosive matter from the primary water, a purification system is provided.

A fraction of the primary water is by-passed through the purifier at the normal rate of 20 gpm. To permit a higher rate of purification, a by-pass rate of 60 gpm can be handled. The driving force through the purifier is the 1750 psia pressure head of the primary water. The 520°F primary water is "let down" through a combination of flash coolers and block orifices to about 65 psia, 110°F.

After letdown, the primary water passes through a demineralizer consisting of a bank of three ion exchangers. The resins in these ion exchangers chemically purify the water by removing the dissolved radio-contaminants and corrosive products. The undissolved radioactive and corrosive particulates are removed by effluent filters. Each ion exchanger and filter has a useful life of at least 50 days, after which it has to be removed and replaced. Appropriate valving permits sequential operation of the ion exchangers and filters for at least 150 days of continuous purification.

The purified water is returned to the primary loop, via a surge tank and charge pump. Ahead of the surge tank, primary make-up water is added. In the surge tank, any radioactive and corrosive gases trapped in the primary water will separate automatically, whereupon these gases are vented off. Beyond the surge tank, a hydrogen addition system maintains a minimum concentration of 20 cc/liter of dissolved hydrogen in the primary water. This excess hydrogen scavenges the free oxygen liberated by dissociation of the water when in the active region of the reactor core. The overall result is minimum corrosion in the primary loops.

A.4 SECONDARY SYSTEM

The propulsion machinery on Savannah is essentially the same as that on a conventional steam-powered ship: a two-element steam turbine driving a single propeller through mechanical reduction gears. The propulsion system contributes 1,265 short tons to the total 4,348 short tons power plant weight; the remainder is made up of reactor system (1,665 short tons) and shielding (2,418 short tons). The only unique feature of the engine room resulting from use of a reactor plant for steam generation is the consolidated control room. Emergency propulsion power is supplied by a 750 hp electric motor which engages one of the high-speed pinions in the reduction gear via a quick-connect coupling. An oil-fired boiler is provided for generation of air ejector motive steam to maintain a main condenser vacuum during emergency propulsion operation, thereby reducing blade windage losses in the main turbine.

Normal electric power is supplied by two, geared, steam-turbine generator units; standby electric power is furnished by two diesel generators, and emergency power by another diesel generator located on the navigation bridge deck. The secondary system is also shown schematically in Figure A-1. Two 16,000 gallon per day distillers of the multiple-effect type provide ample fresh water for plant make-up (via ion exchangers), drinking, washing, and culinary needs.

The main propulsion unit is a cross-compound turbine with high- and low-pressure sections coupled to a double-helical, double-reduction gear of conventional design, this unit delivers 22,000 maximum SHP at 110 rpm with saturated steam at a pressure of 472 psia and a condenser vacuum of 28.45 in. Hg; astern power is 8,000 SHP at 53.5 rpm, in compliance with standard practice of 80 percent of normal ahead torque at half rpm with 100 percent normal ahead steam flow. The propeller is five-bladed, made of nickel-manganese-bronze. The 4,500 rpm, high-pressure turbine has 9, single-row stages of impulse type blading. The 3,000 rpm, low-pressure turbine has 7, single-row ahead stages of impulse type blading; this turbine also as 1 double-row and 1 single row stage of impulse type blading for astern operation. Both turbine casings are split on a horizontal plane. High-pressure turbine exhaust steam, with 11 percent moisture content, passes through a 2-stage, baffle/cyclone, moisture separator before admission to the low-pressure turbine; inter-stage moisture collecting provisions are also included in both turbines. Steam flow is regulated by an electric motor-operated throttle valve controlled by an electrical servo system mounted on a maneuvering handwheel on the main control console.

Hung from the low-pressure turbine, the main condenser is a single pass, non-divided design with scoop sea water injection for normal operation and a 150 hp, 20,000 gpm sea water circulating pump for standby and maneuvering. The 3/4 in. copper-nickel tubes are welded to single, copper-nickel tube sheets for tightness and then lightly rolled for vibration resistance. The 2 turbine-generator condensers are two-pass design, also with welded tubes, and are cooled to maintain 29 in. Hg vacuum by continuous duty sea water circulating pumps. Feedwater is drawn from condenser hotwells by two 40 hp condensate pumps, heated and deaerated and returned to the steam generators at 347°F by the 650 gpm (maximum) steam-turbine driven feed pump.

APPENDIX B

SOFTWARE PARAMETERS FORECASTING

Maurice H. Halstead holds in his book, Elements of Software Science (Ref. B.1) that even relative intangible objects such as computer programs are governed by natural laws. His work starts with the assumption that the human brain obeys a more rigid set of rules than it has been aware of; he later proves the point.

The Halstead theory allows us to forecast with reasonable confidence several software parameters. Those concerning here are:

- program volume
- time to write and debug the algorithm
- number of errors non-detected, buried in the final program.

The fundamentals and theory development are given in reference B.1. For the purposes of this thesis the equations related to those three parameters are stated:

$$\eta^* = 2 + \eta_2^* \tag{B.1}$$

$$\eta_2 = \eta_2^* \left[\frac{\log(\eta^*/2)(\eta_1 - 2)}{\eta^* \log 2} + 1\right] \tag{B.2}$$

$$\left(\frac{\eta^* \log \eta^*}{\log 2}\right)^2 = \lambda\left(\eta_1 \frac{\log \eta_1}{\log 2} + \frac{\eta_2 \log \eta_2}{\log 2}\right)\left(\frac{\log (\eta_1 + \eta_2)}{\log 2}\right) \tag{B.3}$$

$$N = \frac{\eta_1 \log \eta_1}{\log 2} + \frac{\eta_2 \log \eta_2}{\log 2} \tag{B.4}$$

$$V = \frac{N \log (\eta_1 + \eta_2)}{\log 2} \tag{B.5}$$

$$V^{*} = (2 + \eta_2^{*}) \frac{\log (2 + \eta_2^{*})}{\log 2} \tag{B.6}$$

$$E = \frac{V^2}{V^{*}} \tag{B.7}$$

$$\hat{T} = \frac{E}{3600\ S} \tag{B.8}$$

$$\hat{B} = \frac{V}{3600} \tag{B.9}$$

LEGEND:

η_1 = number of unique or distinct operators appearing in that implementation

η_2 = number of unique or distinct operands appearing in that implementation

N_1 = total usage of all of the operators appearing in that implementation

N_2 = total usage of all of the operands appearing in that implementation

η = $\eta_1 + \eta_2$

N = $N_1 + N_2$

η_1^{*} = minimum possible number of operators for a known algorithm (2)

η_2^{*} = minimum possible number of operators for a known algorithm

η^{*} = $\eta_1^{*} + \eta_2^{*} = 2 + \eta_2^{*}$

V = program volume (bits)

V^{*} = minimum possible volume for a known algorithm, also called potential volume

E = total number of elementary mental discriminations required to generate a given program, also called effort

$\hat{T}$ = estimated value of programming time (hours)

S = Stroud number ($5 \leq S \leq 20$ sec^{-1}), lower limit corresponds to an inexperienced programmer, and the higher to an experienced one ($S = 15$ will be used in the code)

$\hat{B}$ = estimated number of bugs remaining in the program.

λ = language constant (FORTRAN case $\lambda = 1.14$)

These equations have no close form and the only way to solve them for V, $\hat{T}$, and $\hat{B}$ is by numerical approximation.

A complete computer code solving the equation has been written, the listing of the code, its inputs and outputs and its user's manual is given at the end of this appendix.

To obtain the data required by the code, the following assumptions are made:

1. η_2^* is equal to the total number of significant input parameters plus output parameters of the system.
2. In order to calculate the input and output parameters of the system, only the significant parameters are included. By significant it is meant those parameters which interrelate with others in the algorithm code, for example, status signals are not included.
3. The input data come from Section 2.3
4. To calculate the input and output parameters for the advanced control function the following assumptions are made:

a) One parameter per peripheral (1 magnetic tape, 1 disk drive, 3 consoles, 1 printer, 1 card reader). Total = 7.

b) The total number of communication parameters is approximately equal to the number of peripherals plus the number of validation and control algorithms (49).

c) The number of polling parameters is the same as the communication parameters (49).

d) The safety state vector has 30 parameters

5. The input parameters to the control algorithm are the validated parameters from the validation algorithm.

6. Any kind of signal which does not undergo a transformation through the code is not included.

7. The significant output parameters for the advanced control algorithm are the summation of peripheral parameters, communication parameters, polling parameters, and the safety state vector.

8. The significant input parameter for the advanced control parameter is the summation of all significant output parameters coming from the validation blocks.

The data about channels and significant parameters comes from the analysis in Section 2.3 and the results are shown in Table B.1.

The η_2^* values calculated in Table B.1 are the inputs to the code. The results coming from the code are in Table B.2. The results given in Table B.2 are the basis for making the hardware design in Section 2.5.

Table B.1

INPUT-OUTPUT PARAMETERS

FUNCTION	SYMBOL	SIGN. INPUT PARAMETERS	INPUT CHANNELS	SIGN. OUTPUT PARAMETERS	OUTPUT CHANNELS	n_2^*
Level control both steam gen.	C_1	7	7	3	3	10
Pressure, volume control pressurizer	C_2	12	12	13	17	25
Temperature control and load following	C_3	34	34	30	31	64
Pressure control sec. system	C_4	5	5	4	4	9
Propeller shaft speed control	C_5	8	8	9	10	17
Flow, temperature control in purification sys.	C_6	28	28	26	28	54
Pressure and temp. control buffer seals	C_7	15	15	15	17	30
SUBTOTAL					110	
Steam generators validation	D_1	24	24	16	16	40
Pressurizer validation	D_2	12	39	10	19	22
Nuclear parameters validation	D_3	12	12	4	4	16
Feed water system validation	D_4	9	15	10	12	19
Turbines validation	D_5	36	51	17	22	53

Table B.1 (continued)

INPUT-OUTPUT PARAMETERS

FUNCTION	SYMBOL	SIGN. INPUT PARAMETERS	INPUT CHANNELS	SIGN. OUTPUT PARAMETERS	OUTPUT CHANNELS	n_2^*
Primary purification validation	D_6	21	87	12	34	33
Buffer seals validation	D_7	33	78	18	33	51
Buffer seal flow validation	D_8	69	69	26	26	95
1-10 control rods validation	D_9	69	138	24	47	93
11-21 control rods validation	D_{10}	72	144	25	49	97
Electrical system validation	D_{11}	78	177	27	60	105
Primary pumps validation	D_{12}	48	60	21	25	69
Primary circuit validation	D_{13}	45	93	29	41	74
Feedwater system validation	D_{14}	51	102	15	36	66
SUBTOTAL			1089	254		
Advanced control	AC	254	254	128	128	382

Table B.2

RESULTS FROM SOFTWARE SCIENCE CODE

BLOCK SYMBOL	MEMORY REQUIREMENTS (kby)	PROGRAMMING TIME (hours) T_p	REMAINING ERRORS ($\hat{B}$)
C_1	0.214	1.33	0.58
C_2	1.77	30.18	4.82
C_3	17.10	911.2	46.7
C_4	0.165	0.89	0.45
C_5	0.712	7.82	1.95
C_6	11.37	493.66	31.04
C_7	2.74	58.5	7.49
D_1	5.53	168.06	15.11
D_2	1.32	19.75	3.61
D_3	0.63	6.5	1.71
D_4	0.93	11.69	2.54
D_5	10.38	430.80	28.34
D_6	3.48	84.04	9.51
D_7	9.89	400.98	27.03
D_8	43.95	3748.8	120
D_9	41.79	3477.15	114.11
D_{10}	46.13	4030.12	125.98
D_{11}	55.73	5351.85	152.19
D_{12}	20.44	1189.66	55.83
D_{13}	24.18	1530.42	66.03
D_{14}	18.36	1011.84	50.13
SUBTOTAL	316.811	22965.24	864.15
Adv. Cont.	1163.73	510538.87	3177.77
TOTAL	1480.54	533498.11	4041.92

SOFTWARE SCIENCE CODE USER'S MANUAL

A list with the parameters and their register locations follows:

REGISTER	VARIABLE
01	η_1
11	η_2^*
12	η^*
13	η_2
14	$(\frac{\eta^* \log \eta^*}{\log 2})^2$
15	λ
16	N
17	V
18	V*
19	auxiliary
20	E
21	S
22	$\hat{T}$
23	$\grave{B}$

The procedure for use of the code follows:

1. Load the code
2. Input λ (reg. 15)
3. Input S (reg. 21)
4. Input η_2^* (reg. 11)
5. input a guess of η_1 (reg. 01); the guess must be lower than the real η_1
6. Start by pressing key A

7. When code stops, recall reg. 17, which gives the estimated program volume in bits

8. Recall reg. 22, which gives the estimated programming time in hours.

9. Recall reg. 23, which gives the estimated number of remaining errors buried inside the program.

Finally Table B.3 has the code listing in AOS language.

REFERENCE

B.1 Elements of Software Science. Maurice H. Halstead. Elsevier North Holland, Inc., 1977.

Table B.3

Software Science Code Listing

```
000  76  LBL
001  11   A
002  02   2
003  42  STO
004  12   12
005  43  RCL
006  11   11
007  44  SUM
008  12   12
009  76  LBL
010  13   C
011  43  RCL
012  12   12
013  55   ÷
014  02   2
015  95   =
016  28  LOG
017  65   ×
018  53   (
019  43  RCL
020  01   01
021  75   -
022  02   2
023  54   )
024  95   =
025  55   ÷
026  43  RCL
027  12   12
028  95   =
029  55   ÷
030  02   2
031  28  LOG
032  95   =
033  85   +
034  01   1
035  95   =
036  65   ×
037  43  RCL
038  11   11
039  95   =
040  42  STO
041  13   13
042  43  RCL
043  12   12
044  28  LOG
045  65   ×
046  43  RCL
047  12   12
048  95   =
049  55   ÷
050  02   2
051  28  LOG
052  95   =
053  33  X²
054  42  STO
055  14   14
056  32  X:T
057  43  RCL
058  01   01
059  65   ×
060  43  RCL
061  01   01
062  28  LOG
063  55   ÷
064  02   2
065  28  LOG
066  95   =
067  85   +
068  43  RCL
069  13   13
070  65   ×
071  43  RCL
072  13   13
073  28  LOG
074  55   ÷
075  02   2
076  28  LOG
077  95   =
078  42  STO
079  16   16
080  65   ×
081  53   (
082  53   (
083  43  RCL
084  01   01
085  85   +
086  43  RCL
087  13   13
088  54   )
089  28  LOG
090  55   ÷
091  02   2
092  28  LOG
093  54   )
094  65   ×
095  43  RCL
096  15   15
097  95   =
098  77   GE
099  12   B
100  69  OP
101  21   21
102  13   C
103  76  LBL
104  12   B
105  43  RCL
106  01   01
107  85   +
108  43  RCL
109  13   13
110  95   =
111  28  LOG
112  55   ÷
113  02   2
114  28  LOG
115  95   =
116  65   ×
117  43  RCL
118  16   16
119  95   =
120  42  STO
121  17   17
122  99  PRT
123  43  RCL
124  11   11
125  85   +
126  02   2
127  95   =
128  42  STO
129  19   19
130  28  LOG
131  65   ×
132  43  RCL
133  19   19
134  95   =
135  55   ÷
136  02   2
137  28  LOG
```

Table B.3 (continued)

```
138  95   =
139  42  STO
140  18   18
141  43  RCL
142  17   17
143  33  X²
144  55   ÷
145  43  RCL
146  18   18
147  95   =
148  42  STO
149  20   20
150  55   ÷
151  43  RCL
152  21   21
153  95   =
154  55   ÷
155  03   3
156  06   6
157  00   0
158  00   0
159  95   =
160  42  STO
161  22   22
162  99  PRT
163  43  RCL
164  17   17
165  55   ÷
166  03   3
167  00   0
168  00   0
169  00   0
170  95   =
171  42  STO
172  23   23
173  99  PRT
174  91  R/S
```

APPENDIX C

CONFIGURING SHEET FOR ARCHITECTURES

The design sheets shown in this appendix are standard configuration worksheets. They are intended as a means of calculating the power requirements, unibus extensions, and cabinet requirements for each architecture. Also the final hardware prices are obtained.

The first set of worksheets (C.1) corresponds to the central and dual central architectures. The interfacing devices and others are the recommended in DEC manuals (references C.1, C.2, C.3, C.4). The prices are the ones for 1980. Worksheets C.2 is the configuration for the star architecture parallel transmission. Because the CPU, memory, and peripherals are exactly the same for every distributed architecture; these elements are calculated only once on Worksheet C.2. The results are used as a starting point in the following sheets. Also worksheet C.2 has the configuration sheets for the corresponding control and diagnosis microprocessors.

Worksheet C.3 is for the star architecture serial transmission. Worksheet C.4 has the dual star parallel transmission architecture. Worksheet C.5 has the dual star serial transmission architecture; this architecture has exactly the same design as the star architecture for the central minicomputer unit. Worksheet C.6 covers the global bus architecture; C.7 has the dual global architecture. This configuration has the same minicomputer unit as global bus.

The microprocessor hardware has been designed based on LSI-11 devices. For light loaded control microprocessors the LSI-11/02 CPU has been chosen; the heavier loaded diagnostics microprocessors use LSI-11/23 machines.

After verifying each design can hold the heaviest loads in its category, the configuration sheets have been written for a microprocessor holding an average load. The reason for doing that is to avoid taxing in cost and probability of failure the distributed alternatives. After all, only a few microprocessors will hold the heavier load; most of them will not be so loaded. Finally the most loaded LSI-11/02 microprocessor will average 719 instructions per signal, and the most loaded LSII-11/23 microprocessor will have an average of 88 instructions per signal. Both numbers are calculated on the basis of a 2-second updating time.

C.1 CENTRAL PROCESSOR AND DUAL ARCHITECTURES
CONFIGURING WORKSHEET

SM-70TAA-LA

PAGE: 1 OF 7

DATE: ______________

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-5 BOX CPU					SUs 6 BOX CPU					SUs 1-2 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
							Enter space, power, and loads required or supplied by options																Add all prices	
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	11/70 NK																				81750	81750	
		BALANCE				D	D	D	D														81750	
	1	RL11-AK																				5500	5500	
		BALANCE				D	D	D	D														87250	
	1	TS03-MA																				4100	4100	
		BALANCE				D	D	D	D														91350	
	1	LP11-VA				D	D	D	D													5300	5300	
		BALANCE				10	←				→	2	1	1.7									96650	
	1	CR-11				1							1	1.5								7500	7500	
		BALANCE				9						2	-	.2									104150	
	1	11960				-						-	-	-			-	-	-			1800	1800	
		BALANCE				9						2	-	.2					→ .2				105950	
	1	BA11-KE (1)			5	-													50			3200	3200	
		BALANCE			5	9						2	-	-					50.2				109150	
	1	DD11-D			2	-											7	2	-			860	860	
		BALANCE			3	9						2	-	-			7	2	50.2				110010	
	3	YS11-AP			-	-						2					5	2	13.5			14300	42900	
		BALANCE			3	9						-	-	-			2	-	36.7				152910	
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 2 OF 7

DATE: ____________

				EXPANSION SPACE																				
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 3-4 BOX 1					SUs 5 BOX 1					SUs 1-2 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
					3	9											2	-	36.7				152910	
				Enter space, power, and loads required or supplied by options																		Add all prices		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	DD11-D			2	-	7	2														860	860	
		BALANCE			1	9						2	2										153770	
	1	DD11-C			1	-																430	530	
		BALANCE			-	9	7	2	29.7			2	2				2	-	36.7				154200	
	9	LPA11-KE				9	7	-	35.0								2		7			5300	47700	
		BALANCE			-	-	-	2	-5.3			2	2				-	-	29.7				201900	
	1	DB11-A				18						2	2	2.2								1850	1850	
		BALANCE			-	18	-	2	-5.3			-	-	-2.2			-	-	-				203750	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
TOTAL EXPANSION SPACE LEFT																								
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 3 OF 7

DATE: ____________________

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SU's 3-4 BOX 1					SU's 1-2 BOX 2					SU's 3-4 BOX 2					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
					-	18	-	2	-7.5														203750	
							Enter space, power, and loads required or supplied by options															*Add all prices*		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	11960				-	-	-				-	-				-	-				1800	1800	
		BALANCE				18																205550		
	1	BA11-VE (2)			5	-			50													3200	3200	
		BALANCE			5	18			12.5													208750		
	2	DD11-D			4	-			-			7	2				7	2				860	1720	
		BALANCE			1	18		2	12.5			7	2	40.5			7	2	31.5			210470		
	18	AD11-K				18		2	2			7	2	9			5	2	7			2000	36000	
		BALANCE			1	-		-	40.5			-	-	31.5			2	-	24.5			246470		
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 4 OF 7

DATE: ____________

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	EXPANSION SPACE																				UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
				PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 5 BOX 2					SUs 3-4 BOX 2					SUs 1-2 BOX 3							
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
									24.9			2											246470	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	1	DD11-C					2	2	24.5			-	-	-								430	430	
		BALANCE					2	2	24.9			2	-	-									246900	
	1	DB11-A				18	-	-	2.2			-	-	-								1850	1850	
		BALANCE				18	-	-	22.3			2	-	-									248750	
	1	11960				-	-	-	-			-	-	-								1800	1800	
		BALANCE				18	-	-	22.3			2	-	-									250550	
	1	BA11-KE (3)			5	-	-	-	50			-	-	-								3200	3200	
		BALANCE			5	18	-	-	72.3			2	-	-									253750	
	1	DD11-D			2	-	-	-	-			-	-	-			7	2				860	860	
		BALANCE			3	18	-	-	72.3			2	-	-			7	2					254610	
	18	AM11-K			-	-			-			-					-	-				1250	22500	
		BALANCE			3	18			72.3			2		72.3			7	2	62.3				277110	
	9	LPA11-KE			-	9						2	-	10			7	-	35			5300	47700	
		BALANCE			3	9	←	—	—	—	→	-	-	62.3			-	2	27.3				324810	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																						TOTALS		

CONFIGURING WORKSHEET

PAGE: 5 OF 7

DATE: ____________

				EXPANSION SPACE																					
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SU's 1-2 BOX 3					SU's 3-4 BOX 3					SU's 5 BOX 3					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
					3	9	-	2	24.5														324810	
				Enter space, power, and loads required or supplied by options																		Add all prices		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	DD11-D			2	-		-				7	2									860	860	
		BALANCE			1	9		2				7	2										325670	
	1	DD11-C			1	-		-				-	-				2	2				430	430	
		BALANCE			-	9		2				7	2	24.5			2	2					326100	
	7	LPA11-KE			-	7		-				7	-	35			-	-				5300	37100	
		BALANCE			-	2		2				-	2	-10.5			2	2					363200	
	8	AA11-K			-	8		2	5.0				2	5.0			2	2	5.0			1250	10000	
		BALANCE				-6		-	-5.0				-	-15.5			-	-	-5.0				373200	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																				TOTALS				

CONFIGURING WORKSHEET

PAGE: 6 OF 7

DATE: ____________

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2 BOX 4					SUs 3-4 BOX 4					SUs 5 BOX 4					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
				-	-	-6			25,5														373200	
				Enter space, power, and loads required or supplied by options																		*Add all prices*		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	11960				-			-													1800	1800	
		BALANCE				-6			-25,5														375000	
	1	BA11-K (4)			5	-			50													3200	3200	
		BALANCE			5	-6			24,5														378200	
	2	DD11-D			4		7	2				7	2									860	1720	
		BALANCE			1	-6	7	2	24,5			7	2										379920	
	1	DD11-C			1	-											2	2				430	430	
		BALANCE			-	-6	7	2				7	2				2	2	24,5				380350	
	1	DB11-A			-	18	-	-				-	-				2	2	2,2			1850	1850	
		BALANCE			-	12	7	2	22,3			7	2	-12,7			-	-	22,3				382200	
	9	LPA11-KE			-	9	7	-	35,0			2	-	10								5300	47700	
		BALANCE			-	3	-	2	-12,7			5	2	22,7			-	-	-				429900	
	9	AA11-K			-	9		2	5,0			5	2	17,5								1250	11250	
		BALANCE			-	-6		-	-			-	-	-44,0			-	-	-				441150	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 7 OF 7

DATE: ____________

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	EXPANSION SPACE																		UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
				PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2 BOX 5					SUs 3-4 BOX 5					SUs 5 BOX 5							
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
					-	-6		-	14.9														441150	
				Enter space, power, and loads required or supplied by options																		Add all prices		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	H960				-	-	-	-													1800	1800	
BALANCE						-6	-	-	-44.9														442950	
	1	BA11-KE (5)			5	-	-	-	50													3200	3200	
BALANCE					5	-6	-	-	+5.1														446150	
	2	DD11-D			4	-	7	2				7	2									860	1720	
BALANCE					1	-6	7	2	5.1			7	2										447870	
	1	DD11-C			1	-	-	-	-			-	-				2	2	5.1			430	430	
BALANCE					-	-6	7	2	5.1			7	2				2	2	2.2				448300	
	1	DB11-A				18	-	-				-	-				2	2	2.9			1850	1850	
BALANCE						12	7	2	2.9			7	2				-	-	2.9				450150	
	10	AA11-K				10	7	2	22.5				1	2.5								1250	12500	
BALANCE						2	-	-	-19.6			7	1	2.5									462650	
	1	H960				-	-	-	-			-	-	-								1800	1800	
BALANCE						2	-	-	-19.6			7	1	-2.5									464450	
	1	BA11-KE			5	-	-	-	50			-	-	-								3200	3200	
BALANCE					5	2	-	-	-27.9			7	1	-			-	-	-				467650	
	1452	BC05M-25			-	-	-	-	-			-	-	-			-	-	-			63	91476	
BALANCE																							559126	
	144	BC05M-25			-	-	-	-	-			-	-	-			-	-	-			63	9072	
BALANCE																							568198	
	106	MPCBS(duel architect)																				1350	1431	
TOTAL EXPANSION SPACE LEFT																								
																					TOTALS			

C.2 STAR ARCHITECTURE (Parallel Transmission)

CONFIGURING WORKSHEET

SM-60LLA-CA

PAGE: 1 OF 4

DATE: ________________

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2-3 BOX CPU					SUs 4-5 BOX CPU					SUs 6 BOX CPU					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
				Enter space, power, and loads required or supplied by options																			Add all prices	
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	11/60 EA				D	D	D	D													30200	30200	
		BALANCE																					30200	
	1	RL-11 AK				D	D	D	D													5500	5500	
		BALANCE				14	1	1	6,5			-	-	-			1	2	9,7				35700	
	1	MS11-KE (extra)				-																4800	4800	
		DALANCE				14	1	1	6,5			-	-	-			1	2	9,7				40500	
	1	TS02-MA				1	1		1.5								-	-				4100	4100	
		DALANCE				13	-	1	60								1	2	9,7				44600	
	1	CP11-VA				1		1	1.5								-	-	-			5300	5300	
		DALANCE				12	-	-	3,5								1	2	9,7				49900	
	1	CR-11				1												1	1.5			7500	7500	
		DALANCE				11	-	-	3,5								1	1	8,2				57400	
		DALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

Note: Up to * the numbers are common to all distributed architectures.

DATE: ______________

PAGE: 2 OF 4

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2 BOX 1					SUs 3-4 BOX 1					SUs 5-6 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						11																	57400	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15"	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	1	BA11-P (1)			6	-			25					25					15				-	
		BALANCE			6	11			25					25					15				57400	
	3	DD11-D			6	-	7	2				7	2				7	2					-	
		BALANCE			-	11	7	2	25			7	2	25			7	2	15				57400	
	3	VS11-AP				-											7	2	13.5			14300	42900	
		BALANCE				11	7	2	25			7	2	25			-	-	1.5				100300	
																							100300	*
		BALANCE																						
	2	DR11-B				2	7	2	3.3			7	2	3.3								1750	3500	
		BALANCE				9	-	-	21.7			-	-	21.7			-	-	1.5				103800	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 3 OF 4

DATE: ______________________

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 7-10 BOX 1					SUs 11-14 BOX 1					SUs 15-18 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						9			21.7					21.7					1.5				03800	
				Enter space, power, and loads required or supplied by options																		Add all prices		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	2	H960			12																	1800	3600	
		BALANCE			12														17				107400	
	6	DD11-DF			12		28	8	21.7			28	8	21.7			28	8	1.5			860	1720	
		BALANCE				9	28	8	21.7			28	8	21.7			28	8	18.5				109120	
	12	DR11-B				12	28	8	13.7			28	8	13.2			28	8	13.2			1750	21000	
		BALANCE				-3	-	-	8.5			-	-	8.5			-	-	5.3				130120	
	1	H960																				1800	1800	
		BALANCE																					131920	
	1	BA11-P (2)																				4150	4150	
		BALANCE																					136070	
	3	DD11-DF																				860	2580	
		BALANCE																					138650	
	1	DB11-A																				1850	1850	
		BALANCE																					140500	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 4 OF 4

DATE: ______

EXPANSION SPACE

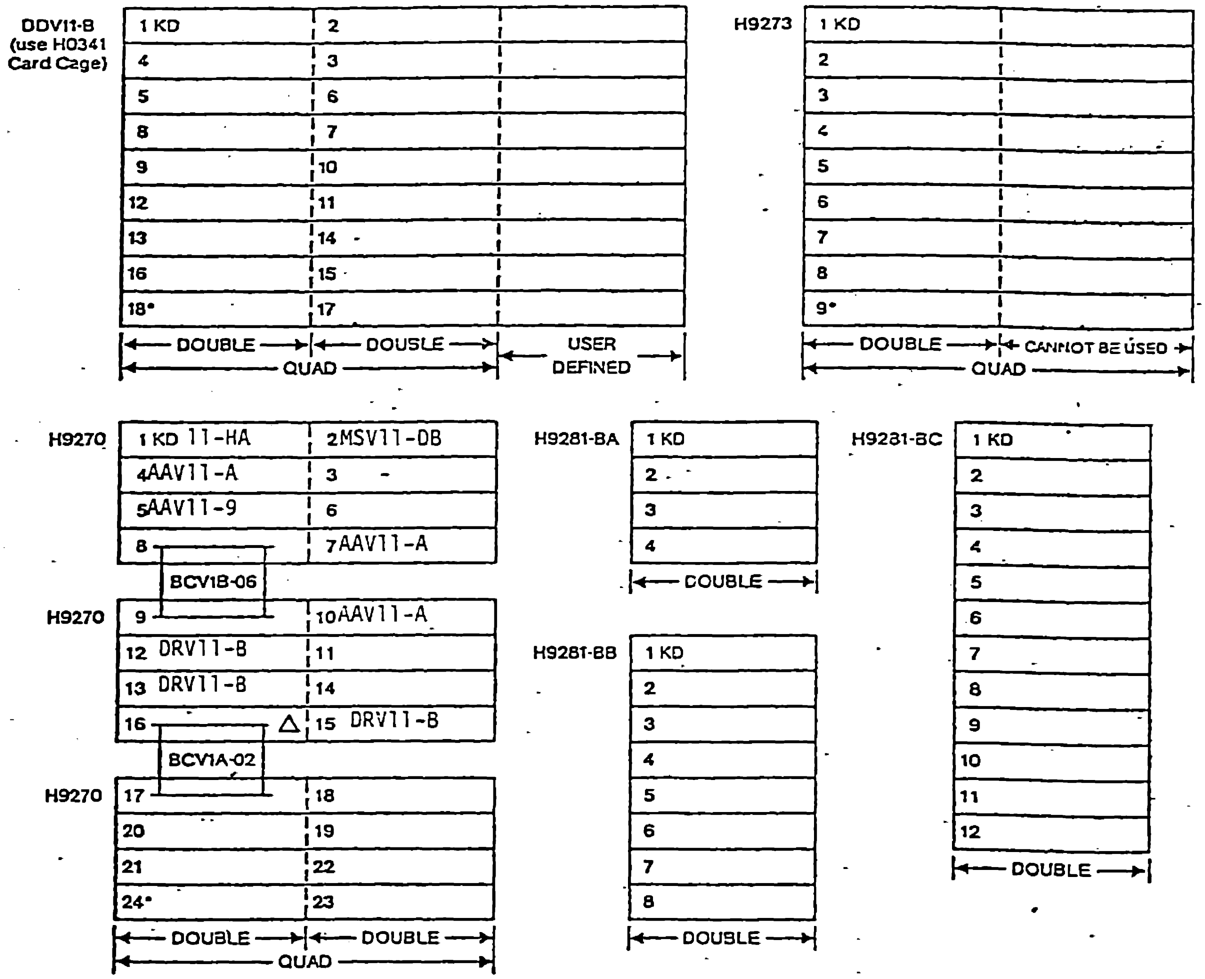
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 19-28 BOX 2 3					SUs 29-38 BOX 2 3					SUs 39-48 BOX 2 3					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
					-	3	-	-															140500	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	5	H960			30																	1800	9000	
		BALANCE																					149500	
	2	BA11-P							50					50					30			4150	8300	
		BALANCE							50					50					30				151800	
	15	DD11-DF			30		70	20				70	20				70	20				860	12900	
		BALANCE			0		70	20	50			70	20	50			70	20	30				170700	
	2	DB11-A (2) (3)				36																1850	3700	
		BALANCE				33	70	20	50			70	20	50			70	20	30				174400	
	28	DR11-B				28	70	20	33			70	20	33			56	16	26.4			1750	49000	
		BALANCE				5	-	-	17			-	-	17			14	4	3.6				223400	
	168	BC07D (cables)				-	-	-	-			-	-	-			-	-	-			116	19488	
		BALANCE																					242088	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
TOTAL EXPANSION SPACE LEFT																								
																					TOTALS			

CONTROL MICROPROCESSOR (STAR ARCHITECTURE) Parallel Transmission

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KD11-HB	1	2D	3.7	2	2.7	.51	1400
Processor Option											
RAM Memory				MSV11-DB							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In	16	DRV11-B	3	3Q	9.9	3	5.7	-	1860
		Bits Out	16								
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs										
	Outputs			AAV11-A	4	4Q	13.2	4	8	1.8	6000
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	2				26	5.0	1400
Cables											
Switch				MPC8S	8						108
							2D				
				TOTALS		7Q	37	9	16.4	2.37	11168

BACKPLANE SELECTOR



DDV11-B (use H0341 Card Cage)

1 KD	2	
4	3	
5	6	
8	7	
9	10	
12	11	
13	14	
16	15	
18*	17	
DOUBLE	DOUBLE	USER DEFINED
QUAD		

H9273

1 KD	
2	
3	
4	
5	
6	
7	
8	
9*	
DOUBLE	CANNOT BE USED
QUAD	

H9270

1 KD 11-HA	2MSV11-DB
4AAV11-A	3 -
5AAV11-9	6
8	7AAV11-A

BCV1B-06

H9270

9	10AAV11-A
12 DRV11-B	11
13 DRV11-B	14
16 △	15 DRV11-B

BCV1A-02

H9270

17	18
20	19
21	22
24*	23
DOUBLE	DOUBLE
QUAD	

H9281-BA

1 KD
2
3
4
DOUBLE

H9281-BB

1 KD
2
3
4
5
6
7
8
DOUBLE

H9281-BC

1 KD
2
3
4
5
6
7
8
9
10
11
12
DOUBLE

△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	-	-

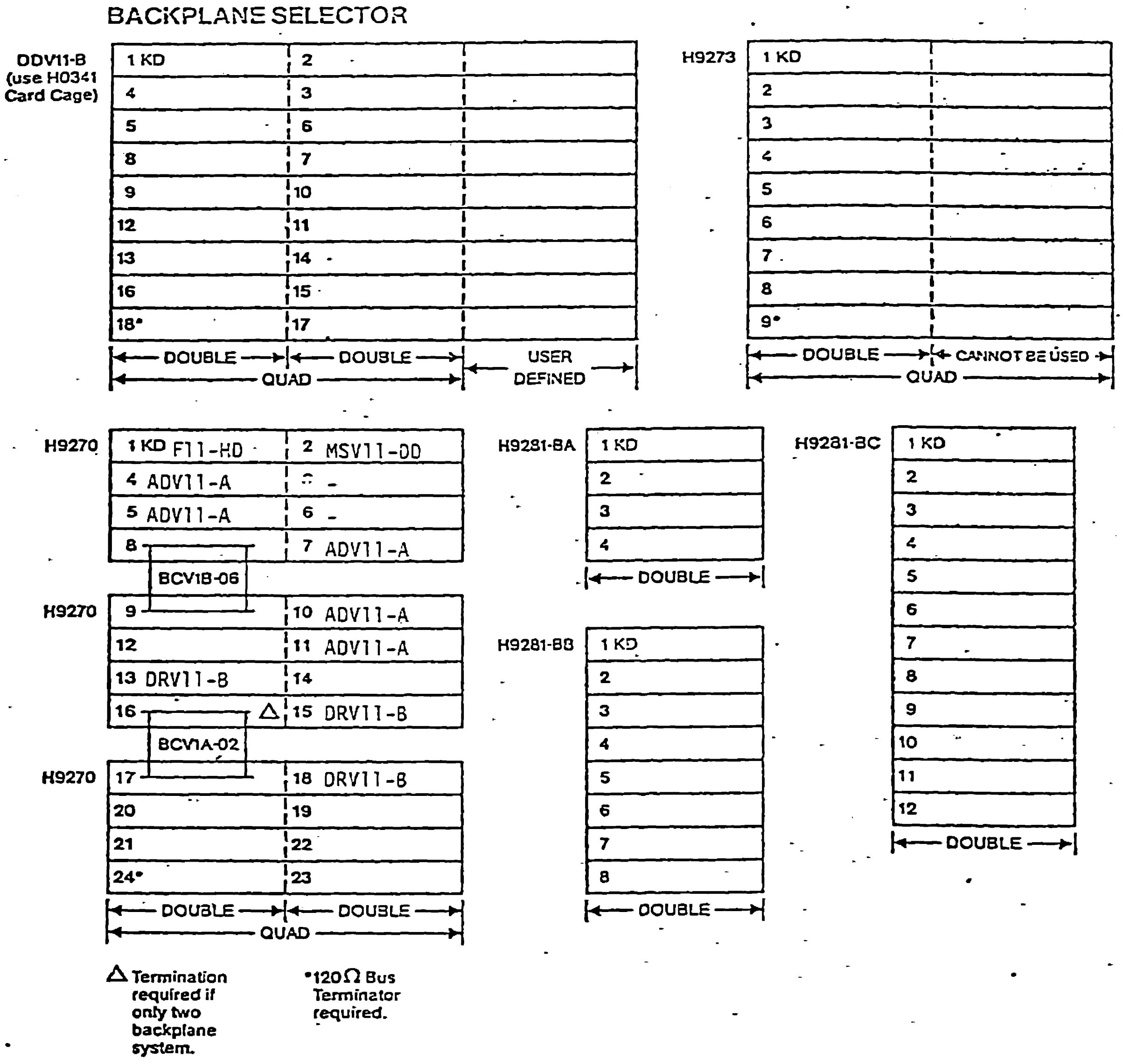
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

DIAGNOSIS MICROPROCESSOR (STAR ARCHITECTURE) Parallel Transmission

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In		DRV11-B	3	3Q	9.9	3	5.7	-	1860
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	5Q	9.5	5	7.5	2	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	3		15.3				600
Power Supplies				H780-H	2				26	5.0	1400
Cables											
						2D					
				TOTALS		8Q	38.7	10	16.9	.57	14860

BACKPLANE SELECTOR



DDV11-B (use H0341 Card Cage)

DOUBLE	DOUBLE	USER DEFINED
1 KD	2	
4	3	
5	6	
8	7	
9	10	
12	11	
13	14	
16	15	
18*	17	

←— DOUBLE —→|←— DOUBLE —→ ← QUAD → | ← USER DEFINED →

H9273

DOUBLE	CANNOT BE USED
1 KD	
2	
3	
4	
5	
6	
7	
8	
9*	

←— DOUBLE —→|← CANNOT BE USED → ←— QUAD —→

	DOUBLE	DOUBLE
H9270	1 KD F11-HD	2 MSV11-DD
	4 ADV11-A	3 -
	5 ADV11-A	6 -
	8	7 ADV11-A
	BCV1B-06	
H9270	9	10 ADV11-A
	12	11 ADV11-A
	13 DRV11-B	14
	16 △	15 DRV11-B
	BCV1A-02	
H9270	17	18 DRV11-B
	20	19
	21	22
	24*	23

←— DOUBLE —→|←— DOUBLE —→ ←— QUAD —→

H9281-BA

DOUBLE
1 KD
2
3
4

H9281-BB

DOUBLE
1 KD
2
3
4
5
6
7
8

H9281-BC

DOUBLE
1 KD
2
3
4
5
6
7
8
9
10
11
12

△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

C.3 STAR ARCHITECTURE (SERIAL TRANSIMISSION) (The central minicomputer is given at parallel transmission)

CONFIGURING WORKSHEET

PAGE: 1 OF 1

DATE: ____________

EXPANSION SPACE

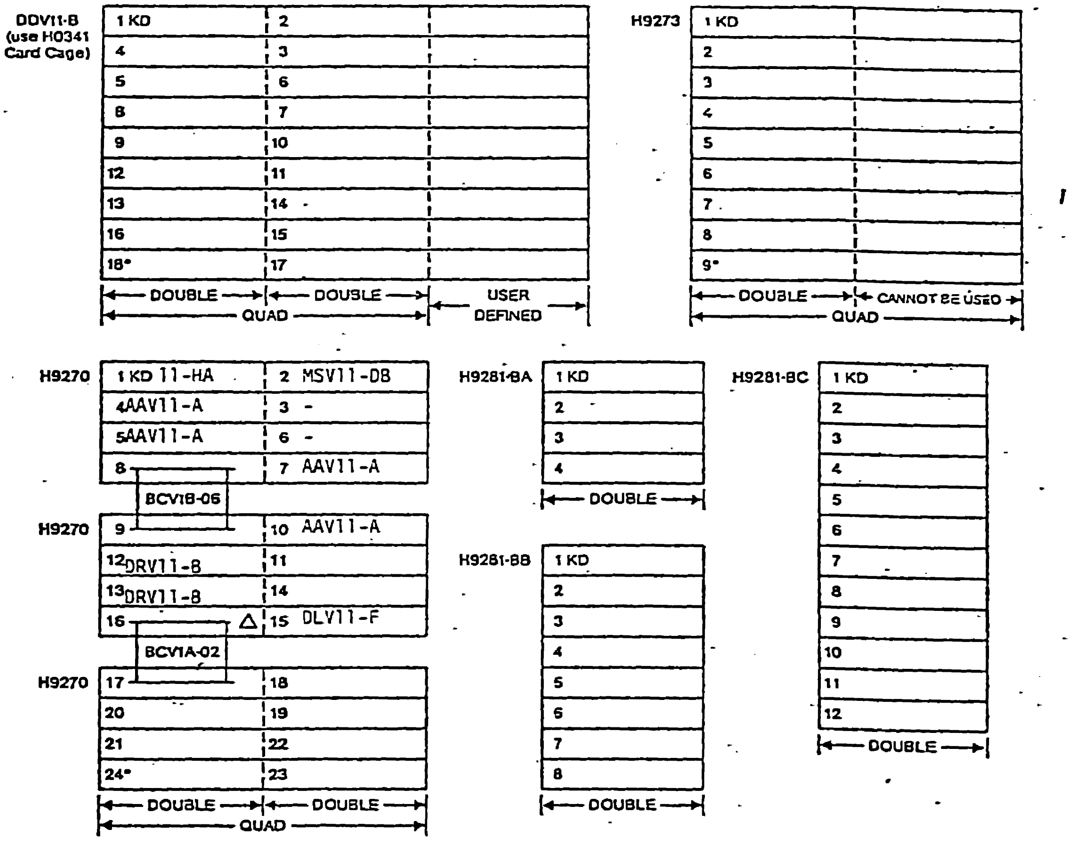
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2 BOX 1					SUs 3-4 BOX 1					SUs 5-6 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						11	7	2	25			7	2	25			-	-	15				100300	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	*Add all prices*		
	6	DZ11-C				6	5		23.5			1		4,7								2550	15300	
		BALANCE				5	2		1.5			6	2	20.3			-	-	15				115600	
	84	BC05C-50 (cable)																				153	12852	
		BALANCE																					128452	
		DALANCE																						
		BALANCE																						
		DALANCE																						
		DALANCE																						
		DALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																				TOTALS				

STAR ARCHITECTURE, SERIAL TRANSMISSION, CONTROL MICROPROCESSOR

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price S
				Type	#		AC	DC	+5	+12	
Processor				KD11-H8	1	2D	3.7	2	2.7	.57	1400
Processor Option											
RAM Memory				MSV11-D8							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC			DLV-11F	1	1D	2.2	1	1.0	.18	310
	EIA Non-Moderᵐ Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In	16	DRV11-B	2	2Q	6.6	2	3.8	-	1240
		Bits Out	16								
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs										
	Outputs			AAV11-A	4	4R	13.2	4	8	1.8	6000
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-11	2				26	5.0	1400
Cables											
Switch			MPC8S	8							108
				TOTALS		6Q 3D	35.9	9	15.5	2.55	10858

BACKPLANE SELECTOR



△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

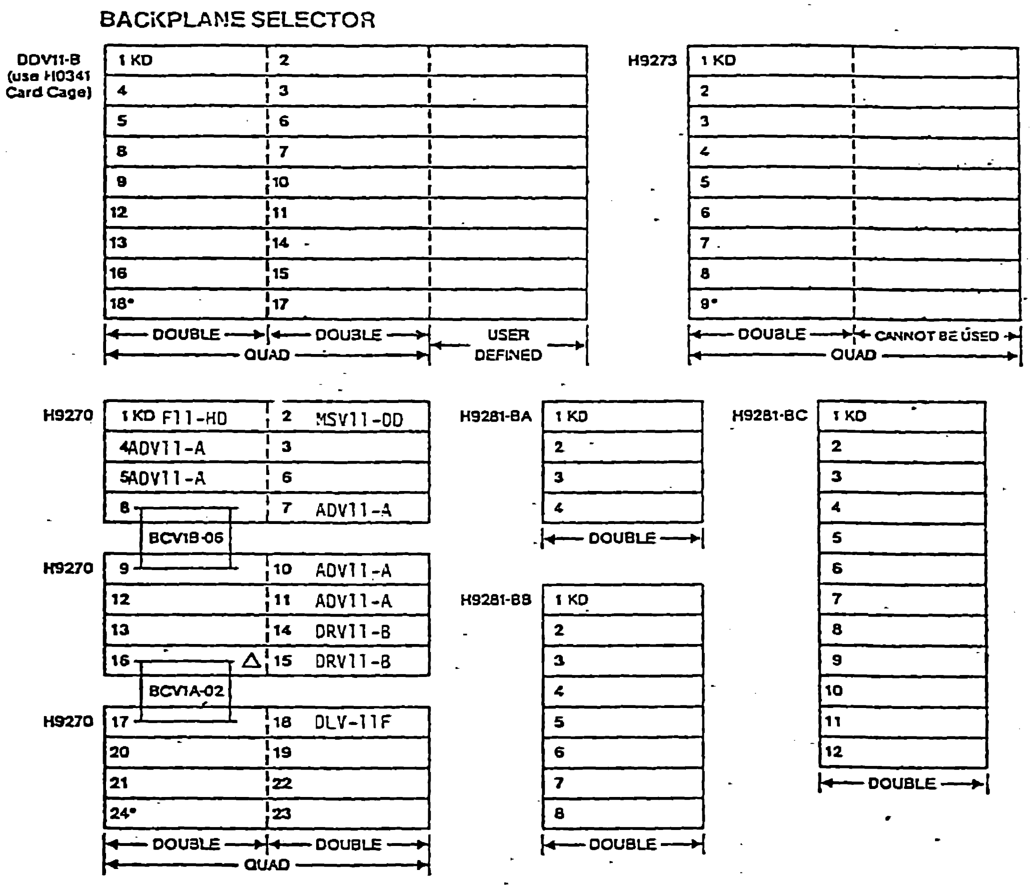
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

STAR ARCHITECTURE, SERIAL TRANSMISSION (Diagnosis Microprocessor)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price S
				Type	#		AC	DC	+5	÷12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC			DLV-11F	1	1D	2.2	1	1.0	.18	310
	EIA Non-Modem Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In	16	DRV11-8	2	2Q	6.6	2	3.8	-	1240
		Bits Out	16								
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	5Q	9.5	5	7.5	2.	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	3		15.3				600
Power Supplies				H780-H	2				26	50	1400
Cables											
				TOTALS		30 70	37.5	10	16	2.75	14550

BACKPLANE SELECTOR



△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A..
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A..
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

C.4 DUAL STAR ARCHITECTURE (Parallel Transmission)

CONFIGURING WORKSHEET

SM-60LLA-CA

PAGE: 1 OF 3

DATE: ____________

				EXPANSION SPACE																				
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 1-2 BOX 1					SUs 3-4 BOX 1					SUs 5-6 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						11	7	2	25			7	2	25			-	-	1.5				100300	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	2	DR11-B				2	7	2	3.3			7	2	3.3								1750	3500	
		BALANCE				9	-	-	21.7			-	-	21.7			-	-	1.5				103800	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

Note: Up to * is the control unit.
Up to ** is the switch.

DATE: ____________

PAGE: 2 OF 3

EXPANSION SPACE

LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs 7-16 BOX 1 2					SUs 17-26 BOX 1 2					SUs 27-36 BOX 1 2					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						9	-	-	21.7			-	-	21.7			-	-	1.5				103800	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	5	H960			30																	1800	9000	
		BALANCE			30																		112800	
	15	DD11-DF			30		35	10				35	10				35	10				860	12900	
		BALANCE			-	9																	125700	
	1	DB11-A				18																1850	1850	
		BALANCE				27	35	10	21.7			35	10	21.7			35	10	1.5				127550	
	1	BA11-P (2)							25					25					15			4150	4150	
		BALANCE				27	35	10	46.7			35	10	46.7			35	10	30.2				131700	
	26	DB11-B				26	35	10	33			35	10	33			35	10	19.8			1750	45500	
		BALANCE				1	-	-	13.7			-	-	13.7			-	-	10.4				177200	*
	1	DT07				18													6.0			6400	6400	
		BALANCE				18	-	-	13.7			-	-	13.7			-	-	4.4				6400	**
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																					TOTALS			

CONFIGURING WORKSHEET

PAGE: 3 OF 3

DATE: ____________

EXPANSION SPACE

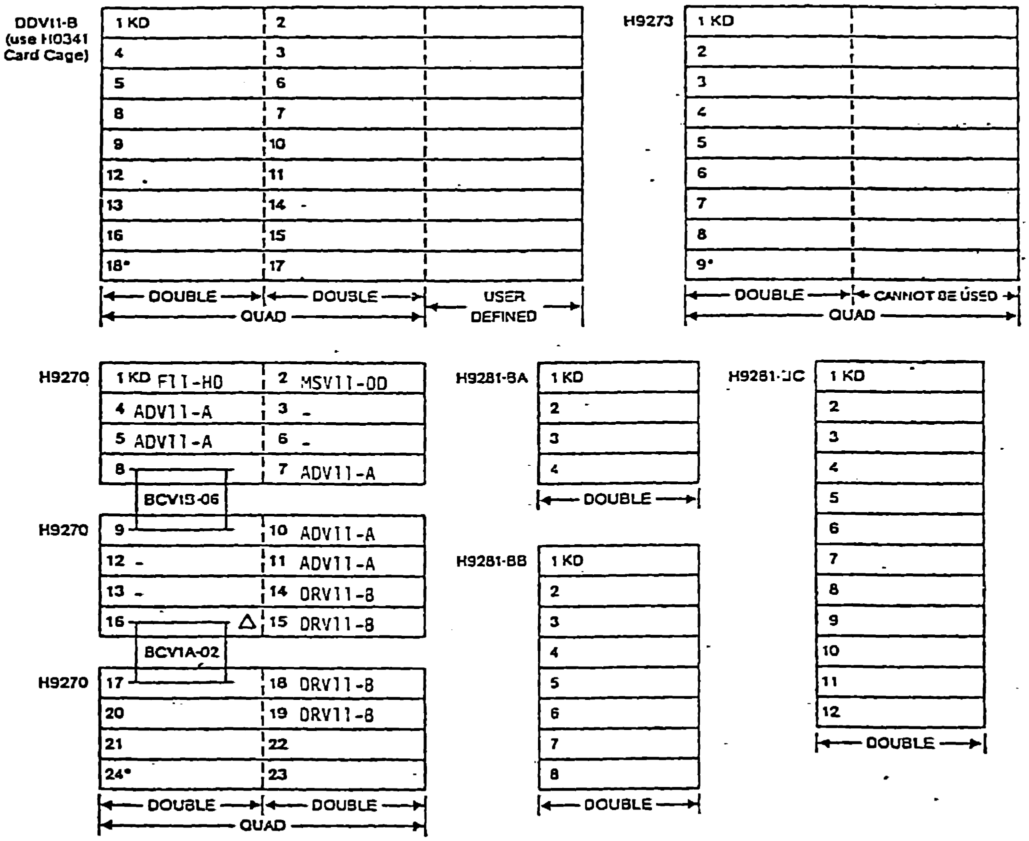
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SUs		BOX			SUs		BOX			SUs		BOX			UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						18			13.7					13.7					4.4				6400	
				Enter space, power, and loads required or supplied by options																				
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	Add all prices		
	3	H960			18																	1800	5400	
		BALANCE			18	18			13.7					13.7					4.4				11800	
	1	BA11-P (3)							25					25					15			4150	4150	
		BALANCE			18	18			38.7					38.7					19.4				15950	
	7	DD11-DF			14		21	6				21	6				7	2				860	6020	
		BALANCE			4	18	21	6	38.7			21	6	38.7			7	2	19.4				21970	
	14	DR11-B			4	14	21	6	19.8			21	6	19.8			7	2	6.6			1750	24500	
		BALANCE			4	14	-	-	18.9			-	-	18.9			-	-	12.8				46470	
	168	BC07D-25			-	-	-	-	-			-	-	-			-	-	-			116	19488	
		BALANCE																					65958	*
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		TOTAL EXPANSION SPACE LEFT																						
																						TOTALS		

DIAGNOSIS MICROPROCESSOR (Dual Star Architecture) (Parallel Transmission)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In		DRV11-B	4	4Q	13.2	4	7.6	-	2480
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	50	9.5	5	7.5	2	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	3		15.3				600
Power Supplies				H780-H	2				26	5.0	1400
Cables											
				TOTALS		2D 90	42	11	18.8	2.57	15480

BACKPLANE SELECTOR



DDV11-B (use H0341 Card Cage)

DOUBLE	DOUBLE	USER DEFINED
1 KD	2	
4	3	
5	6	
8	7	
9	10	
12	11	
13	14	
16	15	
18*	17	
QUAD		

H9273

DOUBLE	CANNOT BE USED
1 KD	
2	
3	
4	
5	
6	
7	
8	
9*	
QUAD	

	DOUBLE	DOUBLE
H9270	1 KD F11-HD	2 MSV11-DD
	4 ADV11-A	3 -
	5 ADV11-A	6 -
	8	7 ADV11-A
	BCV1B-06	
H9270	9	10 ADV11-A
	12 -	11 ADV11-A
	13 -	14 DRV11-B
	16 △	15 DRV11-B
	BCV1A-02	
H9270	17	18 DRV11-B
	20	19 DRV11-B
	21	22
	24*	23
	QUAD	

H9281-BA

DOUBLE
1 KD
2
3
4

H9281-BB

DOUBLE
1 KD
2
3
4
5
6
7
8

H9281-BC

DOUBLE
1 KD
2
3
4
5
6
7
8
9
10
11
12

△ Termination required if only two backplane system.

*120 Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply Master Slave	 H780-H H780-K	 13 A. 13 A.	 2.5 A. 2.5 A.
Boxes H9281-BA Backplane w/ps H9270 Backplane w/ps H9273 Backplane w/ps Enclosure for DDV11-B	 BA11-VA BA11-ME BA11-NE H909-C	 5.1 A. 13.0 15.5 A. –	 1.5 A. 2.5 A. 8.0 –

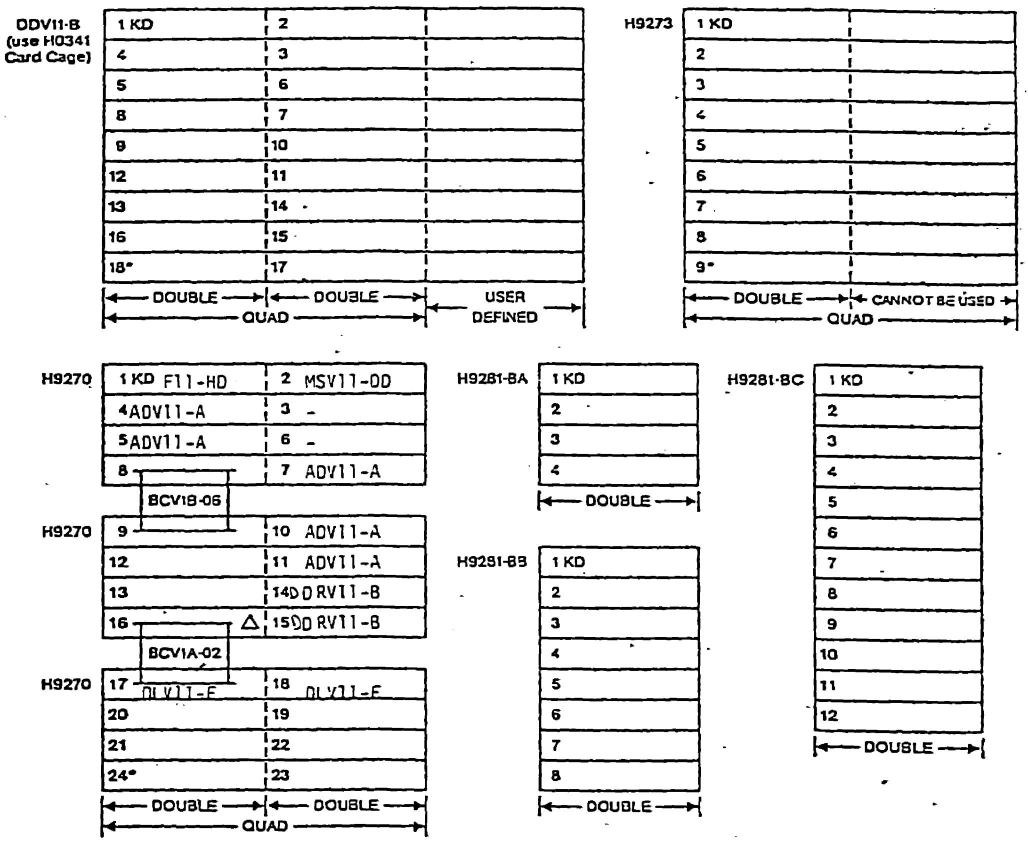
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

C.5 DIAGNOSIS MICROPROCESSOR (Du l Star Architecture) (Serial Alternative)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC			DLV-11F	2	2D	4.4	2	2	0.36	
	EIA Non-Modem Async										
	EIA Modem Async										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In	16	DRV11-B	2	2Q	6.6	2	3.8	-	1240
		Bits Out	16								
	DMA	Bits In									
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	5Q	9.5	5	7.5	2	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	3		15.3				600
Power Supplies				H780-H	2				26	5.0	1400
Cables											
				TOTALS		4D 7Q	39.8	11	17	2.93	14860

BACKPLANE SELECTOR



△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply Master Slave	 H780-H H780-K	 13 A. 13 A.	 2.5 A. 2.5 A.
Boxes H9281-BA Backplane w/ps H9270 Backplane w/ps H9273 Backplane w/ps Enclosure for DDV11-B	 BA11-VA BA11-ME BA11-NE H909-C	 5.1 A. 13.0 15.5 A. –	 1.5 A. 2.5 A. 3.0 –

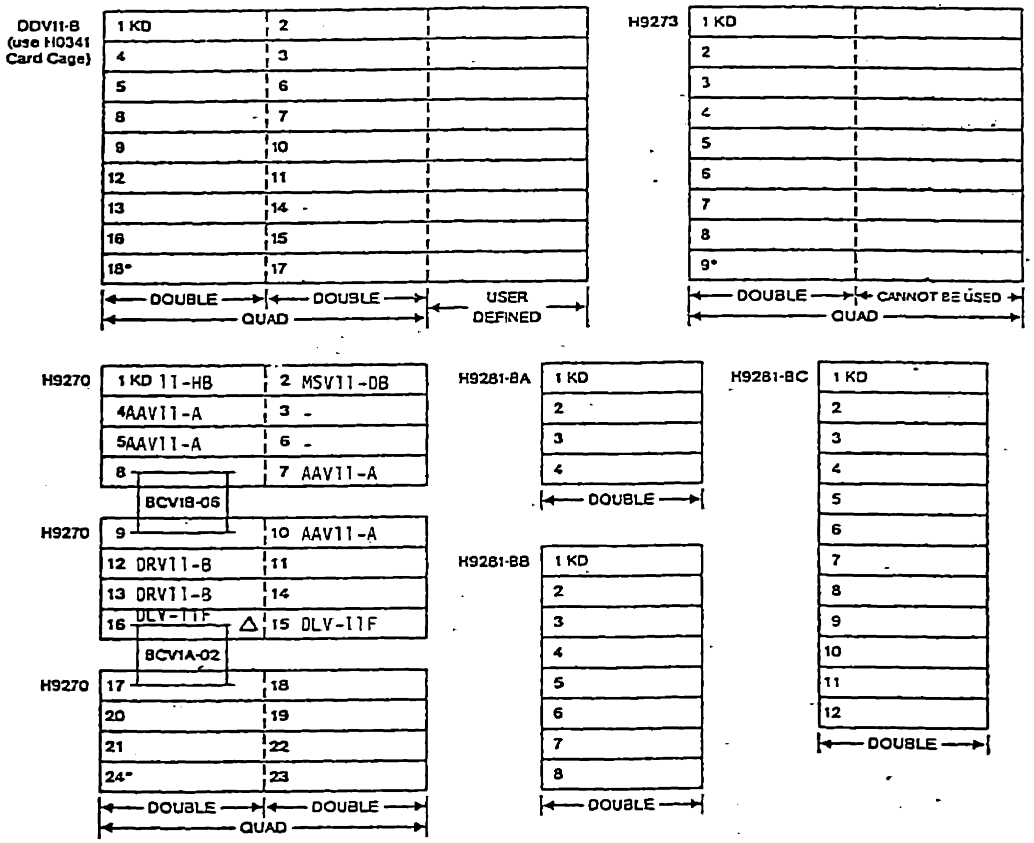
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

CONTROL MICROPROCESSOR (Dual Star Architecture) (Serial Alternative)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KD11-HB	1	2D	3.7	2	2.7	.57	1400
Processor Option											
RAM Memory				MSV11-DB							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC			DLV-11F	2	2D	4.4	2	2	0.36	620
	EIA Non-Modem Async										
	EIA Modem A-ync										
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In	16	DRV11-8	2	2R	6.6	2	3.8	-	1240
		Bits Out	16								
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs										
	Outputs			AAV11-A	4	4Q	13.2	4	8	1.8	6000
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	2				26	5.0	1400
Cables											
Switch			MPC8S	8							108
				TOTALS		6Q 4D	38.1	10	16.3	2.73	11168

BACKPLANE SELECTOR



△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply Master Slave	 H780-H H780-K	 13 A 13 A	 2.5 A 2.5 A
Boxes H9281-BA Backplane w/ps H9270 Backplane w/ps H9273 Backplane w/ps Enclosure for DDV11-B	 BA11-VA BA11-ME BA11-NE H909-C	 5.1 A 13.0 15.5 A -	 1.5 A 2.5 A 8.0 -

Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

C.6 GLOBAL BUS ARCHITECTURE (Serial Transmission)

CONFIGURING WORKSHEET

SM-60LLA-CA

PAGE: 1 OF 1

DATE: ______________

EXPANSION SPACE

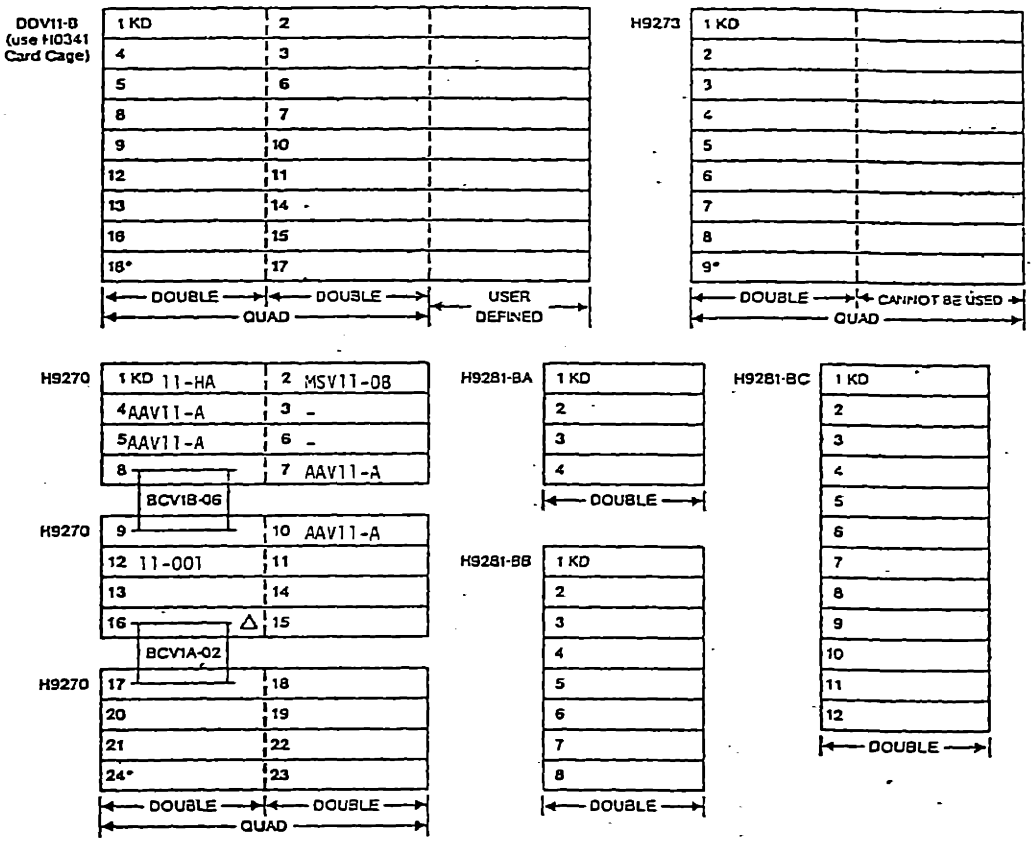
LINE ITEM	QTY	SYSTEM/OPTION NUMBER	PRE DESIGNATED MOUNTING SPACE	PANEL SPACE AVAIL	SYSTEM UNITS AVAIL	BUS LOADS AVAIL	SU: 1-2 BOX 1					SU: 3-4 BOX 1					SU: 5-6 BOX 1					UNIT PRICE	TOTAL PRICE	FIELD SERVICE MONTHLY MAINT
							HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V	HEX	QUAD	+5V	+15V	-15V			
						11	7	2	25			7	2	25			-	-	1.5				100300	
				Enter space, power, and loads required or supplied by options																		Add all prices		
				PANEL SPACE	SYSTEM UNITS	BUS LOADS	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V	HEX SLOTS	QUAD SLOTS	+5V	+15V	-15V			
	1	11-0016				1	-	-	-				1	3.5								5375	5375	
		BALANCE				10	7	2	25			7	1	21.5									105675	
		BALANCE																						
	5	BC08B-25																				244	1220	
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
		BALANCE																						
TOTAL EXPANSION SPACE LEFT																							106895 *	
																					TOTALS			

CONTROL MICROPROCESSOR (Global Data Bus) .(Serial Transmission)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KD11-HB	1	20	3.7	2	2.7	.57	1400
Processor Option											
RAM Memory				MSV11-0B							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async		Computrol	11-0011	1	20	1.5		1.5	-	2235
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In									
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs										
	Outputs			AAV11-A	4	4R	13.2	4	8	1.3	6000
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	1				13	2.5	700
Cables											
				TOTALS		40 40	28.6		12.2	2.37	10843

BACKPLANE SELECTOR



Δ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A	2.5 A
Slave	H780-K	13 A	2.5 A
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A	1.5 A
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A
H9273 Backplane w/ps	BA11-NE	15.5 A	8.0
Enclosure for DDV11-B	H909-C	-	-

Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

DIAGNOSIS MICROPROCESSOR (Global Bus Architecture) (Serial Transmission)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem As:nc		Comoutrol	11-0011	1	20	1.5		1.5	-	2225
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In									
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	5Q	9.5	5	7.5	2	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	1				13	2.5	700
Cables											
				TOTALS		5Q 10	25.2		12.7	2.57	14335

BACKPLANE SELECTOR

DDV11-B (use H0341 Card Cage)

1 KD	2	
4	3	
5	6	
8	7	
9	10	
12	11	
13	14	
16	15	
18*	17	
DOUBLE	DOUBLE	USER DEFINED
QUAD		

H9273

1 KD	
2	
3	
4	
5	
6	
7	
8	
9*	
DOUBLE	CANNOT BE USED
QUAD	

H9270

1 KD F11-HD	2 MSV11-DD
4 ADV11-A	3
5 ADV11-A	6
8	7 ADV11-A

BCV1B-06

H9270

9	10 ADV11-A
12	11 ADV11-A
13 11-0011	14
16	△ 15

BCV1A-02

H9270

17	18
20	19
21	22
24*	23
DOUBLE	DOUBLE
QUAD	

H9281-BA

1 KD
2
3
4
DOUBLE

H9281-BB

1 KD
2
3
4
5
6
7
8
DOUBLE

H9281-BC

1 KD
2
3
4
5
6
7
8
9
10
11
12
DOUBLE

△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

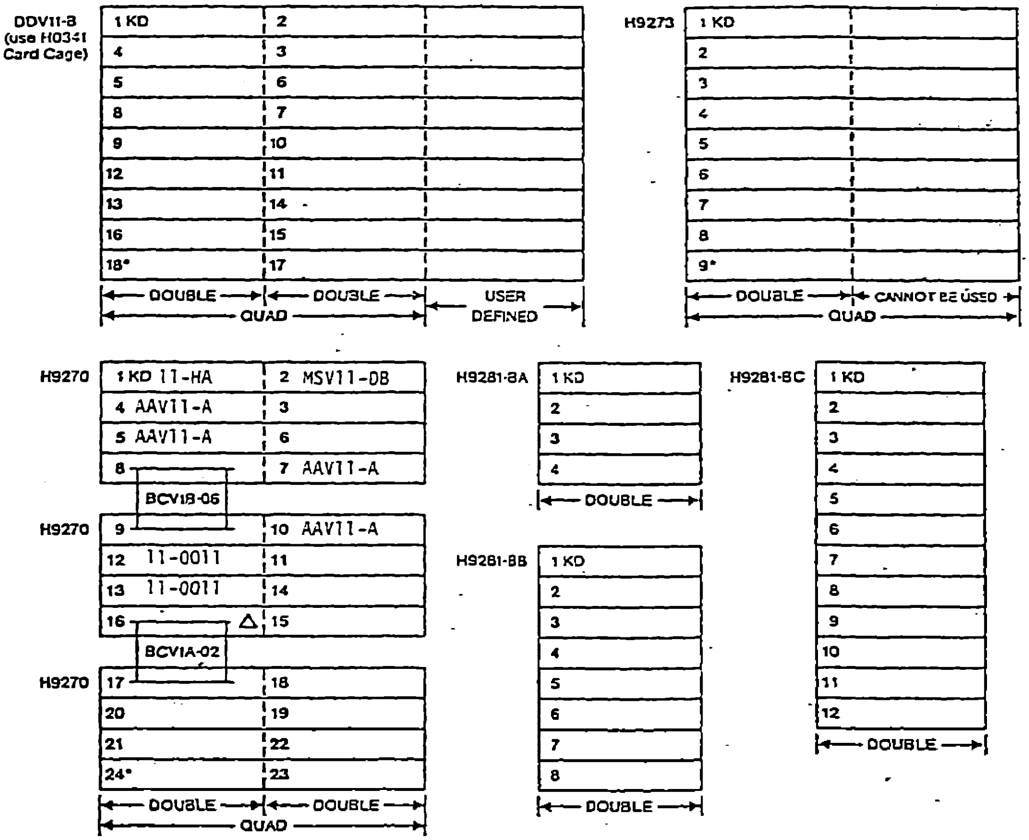
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

C.7 CONTROL MICROPROCESSOR (Dual Global Bus) (Serial Transmission)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price S
				Type	#		AC	DC	+5	+12	
Processor				KD11-HB	1	2D	3.7	2	2.7	.57	1400
Processor Option											
RAM Memory				MSV11-DB							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async		Computrol	11-0011	2	4D	3.0		3.0	-	4470
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In									
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs										
	Outputs			AAV11-A	4	4Q Q	13.2	4	8	1.8	6000
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	1				13	2.5	700
Cables											
Switch				MPC8S	8						108
				TOTALS		6D 4Q	30.1		13.7	2.37	13078

BACKPLANE SELECTOR



△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

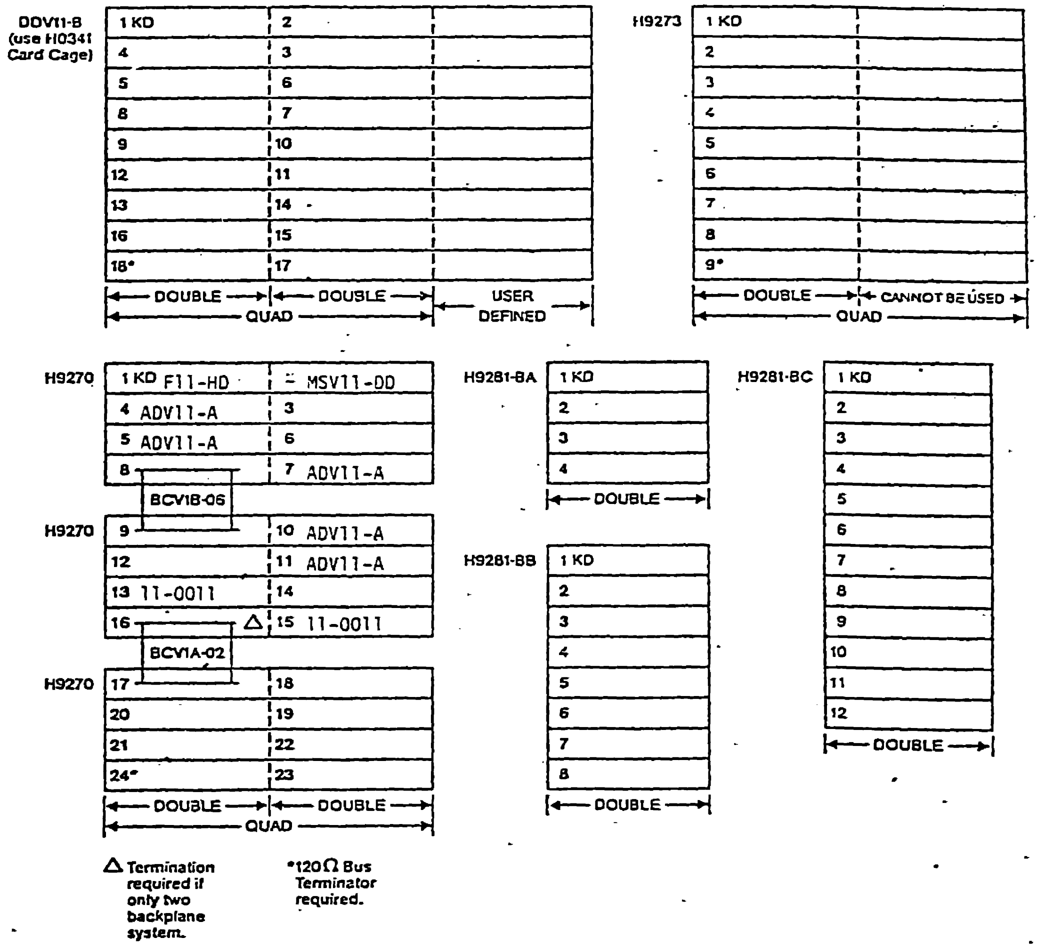
Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

DIAGNOSIS MICROPROCESSOR (Dual Global Bus Architecture) (Serial Transmission)

MICROCOMPUTER SYSTEM CONFIGURATION WORKSHEET

Option Function			System Requirement	Selected Option		Size	Bus Loading		Power Supply Loading		Price $
				Type	#		AC	DC	+5	+12	
Processor				KDF11-HD	1	2D	4	2	3.7	.57	3000
Processor Option											
RAM Memory				MSV11-DD							
PROM Memory											
Run Time Software											
Serial Ports	20 Ma ASYNC										
	EIA Non-Modem Async										
	EIA Modem Async			11-0011	2	4D	3		30	-	4470
	EIA Modem Sync										
Parallel Ports	Program Control	Bits In									
		Bits Out									
	DMA	Bits In									
		Bits Out									
Mass Storage	Cartridge Tape Drives										
	Floppy Disk Drives										
	Cartridge Disk Drives										
Mass Storage Bootstrap											
Analog	Inputs			ADV11-A	5	5Q	9.5	5	7.5	2	8000
	Outputs										
Line Printer											
Programmable Clock											
IEEE 488 Controller											
Custom Interfaces											
Terminal											
Backplanes/Boxes				H9270	2		10.2				400
Power Supplies				H780-H	2				26	5.0	1400
Cables											
				TOTALS		6D 5D	26.7		14.2	2.57	17270

BACKPLANE SELECTOR



DDV11-B (use H0341 Card Cage)

1 KD	2	
4	3	
5	6	
8	7	
9	10	
12	11	
13	14	
16	15	
18*	17	
← DOUBLE →	← DOUBLE →	← USER DEFINED →
← QUAD →		

H9273

1 KD	
2	
3	
4	
5	
6	
7	
8	
9*	
← DOUBLE →	← CANNOT BE USED →
← QUAD →	

H9270

1 KD F11-HD	2 MSV11-DD
4 ADV11-A	3
5 ADV11-A	6
8	7 ADV11-A

BCV1B-06

H9270

9	10 ADV11-A
12	11 ADV11-A
13 11-0011	14
16 △	15 11-0011

BCV1A-02

H9270

17	18
20	19
21	22
24*	23
← DOUBLE →	← DOUBLE →
← QUAD →	

H9281-BA

1 KD
2
3
4
← DOUBLE →

H9281-BB

1 KD
2
3
4
5
6
7
8
← DOUBLE →

H9281-BC

1 KD
2
3
4
5
6
7
8
9
10
11
12
← DOUBLE →

△ Termination required if only two backplane system.

*120Ω Bus Terminator required.

Power Supplies and Boxes		Capacity	
		+5 V	+12 V
Power Supply			
Master	H780-H	13 A.	2.5 A.
Slave	H780-K	13 A.	2.5 A.
Boxes			
H9281-BA Backplane w/ps	BA11-VA	5.1 A.	1.5 A.
H9270 Backplane w/ps	BA11-ME	13.0	2.5 A.
H9273 Backplane w/ps	BA11-NE	15.5 A.	8.0
Enclosure for DDV11-B	H909-C	–	–

Backplane	AC loads
H9270	5.1
H9273	2.6
DDV11-B	6.4
H9281-BA	1.3
H9281-BB	2.4
H9281-BC	3.6

APPENDIX D

FAULT TREE ANALYSIS

The following fault trees (FT) have been developed under the assumptions made in Chapter 2, Section 2.6. Each alternative has a separated fault tree and its own set of equations. The only exception to that rule are fault trees for the single star serial alternative, conditions one and two, and dual star serial condition two. The former have exactly the same FT and equations that single star parallel architecture; they only differ in the values to be input to the probability equations. The latter has the same FT and equations than dual star parallel architecture, and also they differ in the values to be input to the probability equations.

The probability equations are given in implicit form which makes them easier to implement in a computer code.

At the end of each set of FT and equations there is a table which serves the purpose of identifying the symbols given in the fault tree diagram with their incomings as events. These tables also have the results of the numerical analysis of the fault trees. The way the numbers given in the tables are obtained is explained in Subsection 2.7.

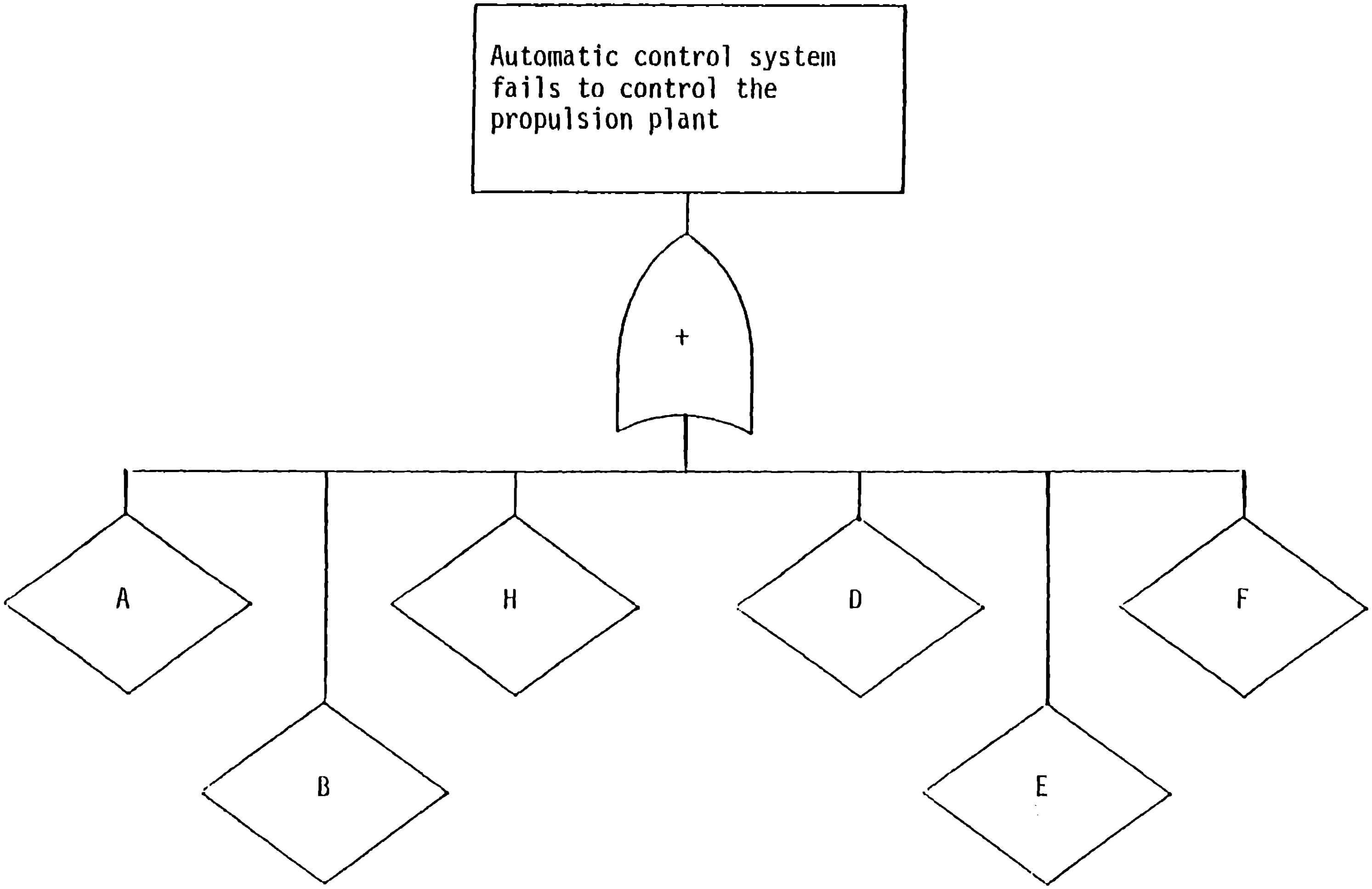

Automatic control system fails to control the propulsion plant
+
A
B
H
D
E
F

Figure D.1 Central computer architecture, situation one.

Table D.1

CENTRAL COMPUTER ARCHITECTURE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10 h^6)	
A	.06	3.0	1.0	1.0	.18	$4.457\text{x}10^{-4}$
B	3557.2	1.0	6.3	1.0	$2.241\text{x}10^4$	0.41599
D	173.392	1.0	6.3	1.0	$1.092\text{x}10^3$	$1.731\text{x}10^{-5}$
E	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
F	.06	3.0	1.0	1.0	.18	$4.69343\text{x}10^{-3}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
A	Control cables	Control line fails
B	Central processor	Processor hardware fails
D	Monitor and keyboard	MMI system fails (Man-machine interface)
E	Control software	Control software fails
F	Diagnosis cables	Diagnosis line fails

CENTRAL COMPUTER ARCHITECTURE

PROBABILISTIC EQUATIONS (SITUATION ONE)

TE = A + B + D + E + F + H (from the fault tree)

$TE = F_3 + F_4$ $\quad$ $p(TE) = p(F_3) + p(F_4) - p(F_3)p(F_4)$

$F_3 = F_1 + F_2$ $\quad$ $p(F_3) = p(F_1) + p(F_2) - p(F_1)p(F_2)$

$F_4 = A + E$ $\quad$ $p(F_4) = p(A) + p(E) - p(A)p(E)$

$F_1 = B$ $\quad$ $p(F_1) = p(B)$

$F_2 = D + F + H$ $\quad$ $p(F_2) = p(D) + p(F) + p(H) + p(D)p(F)p(H)$

$- p(D)p(F) - p(D)p(H) - p(F)p(A)$

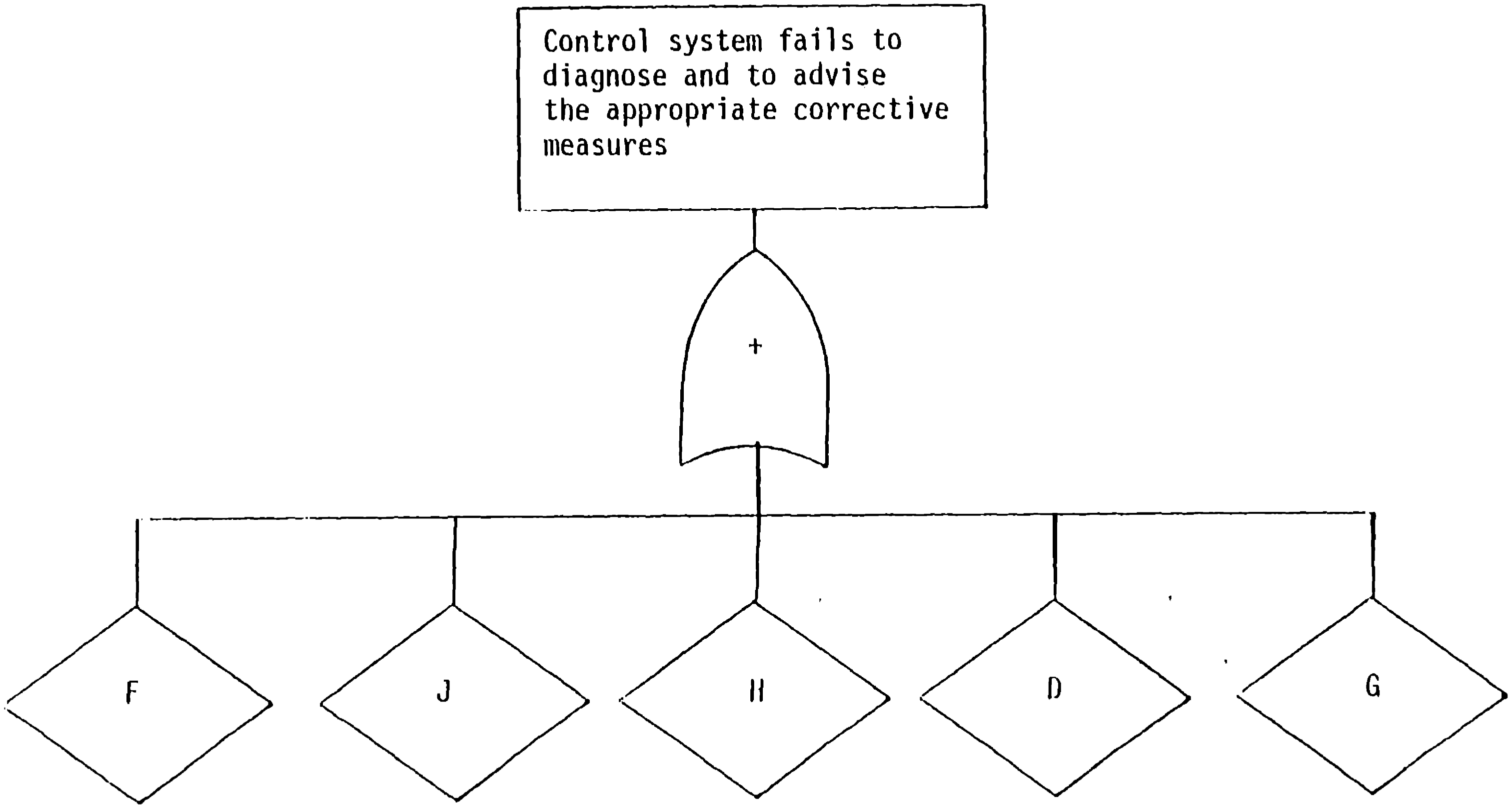

Control system fails to diagnose and to advise the appropriate corrective measures
+
F
J
H
D
G

Figure D.2 Central computer architecture, situation two.

Table D.2

CENTRAL COMPUTER ARCHITECTURE (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
I	1247.36	1.0	6.3	1.0	7.858×10^3	0.17187
H						8.997×10^{-4}
G	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
I	Central processor	Processor hardware fails
H	Secondary storage	Storage system fails
G	Diagnosis software	Diagnosis software fails

CENTRAL COMPUTER ARCHITECTURE

PROBABILISTIC EQUATIONS (SITUATION TWO)

TE = F + I + H + D + G (from the fault tree)

$P(TE) = F_1 + F_2 + G$ $\qquad p(TE) = p(F_1) + p(F_2) + p(G) + p(F_1)p(F_2)p(G)$

$\qquad - p(F_1)p(F_2) - p(F_1)p(G) - p(F_2)P(G)$

$F_1 = F + I$ $\qquad p(F_1) = p(F) + p(I) - p(F)p(I)$

$F_2 = H + D$ $\qquad p(F_2) = p(H) + p(D) - p(H)p(D)$

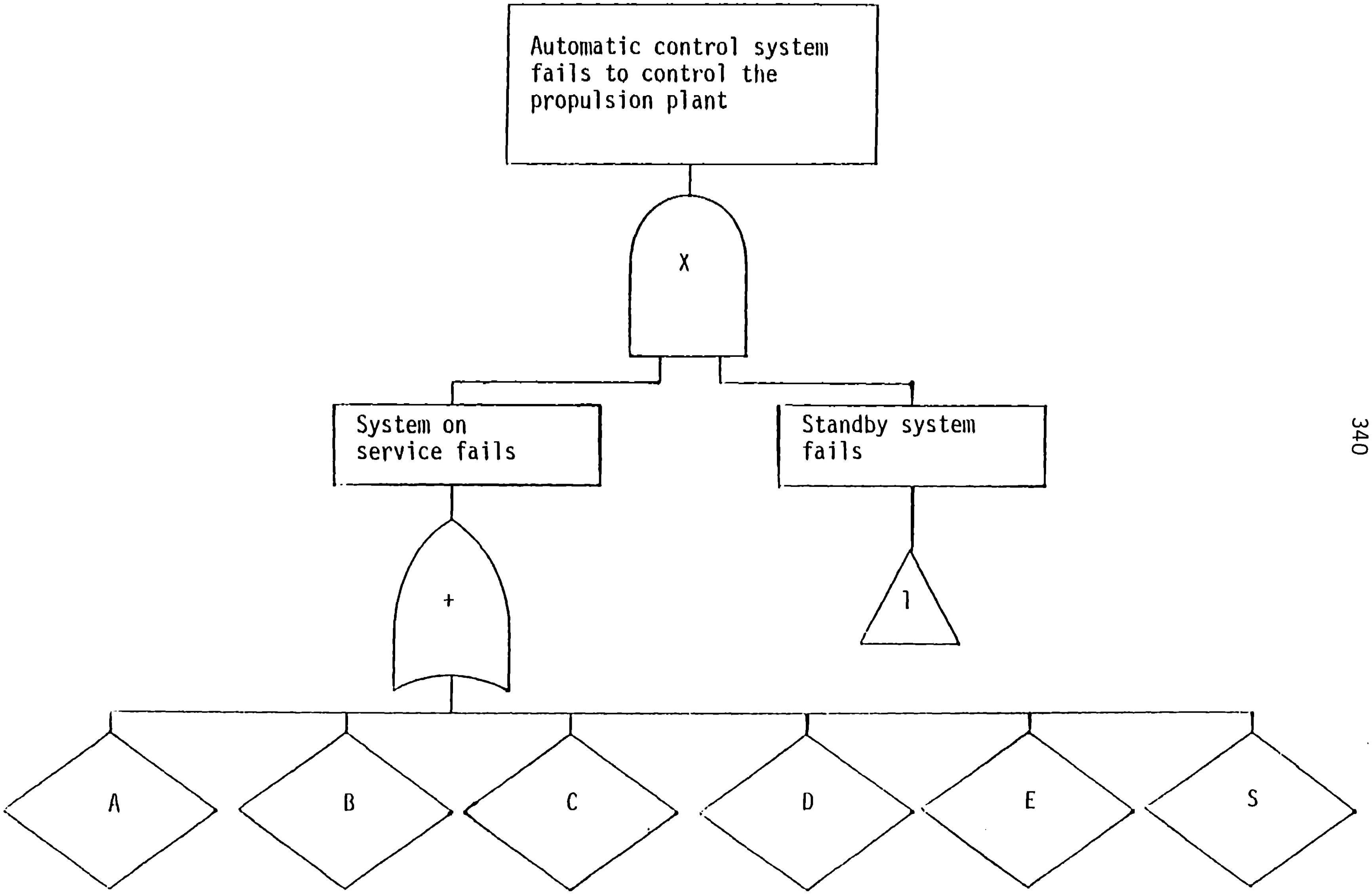

Automatic control system fails to control the propulsion plant
X
System on service fails
Standby system fails
+
1
A
B
C
D
E
S

Figure D.3 Dual central computer, situation one.

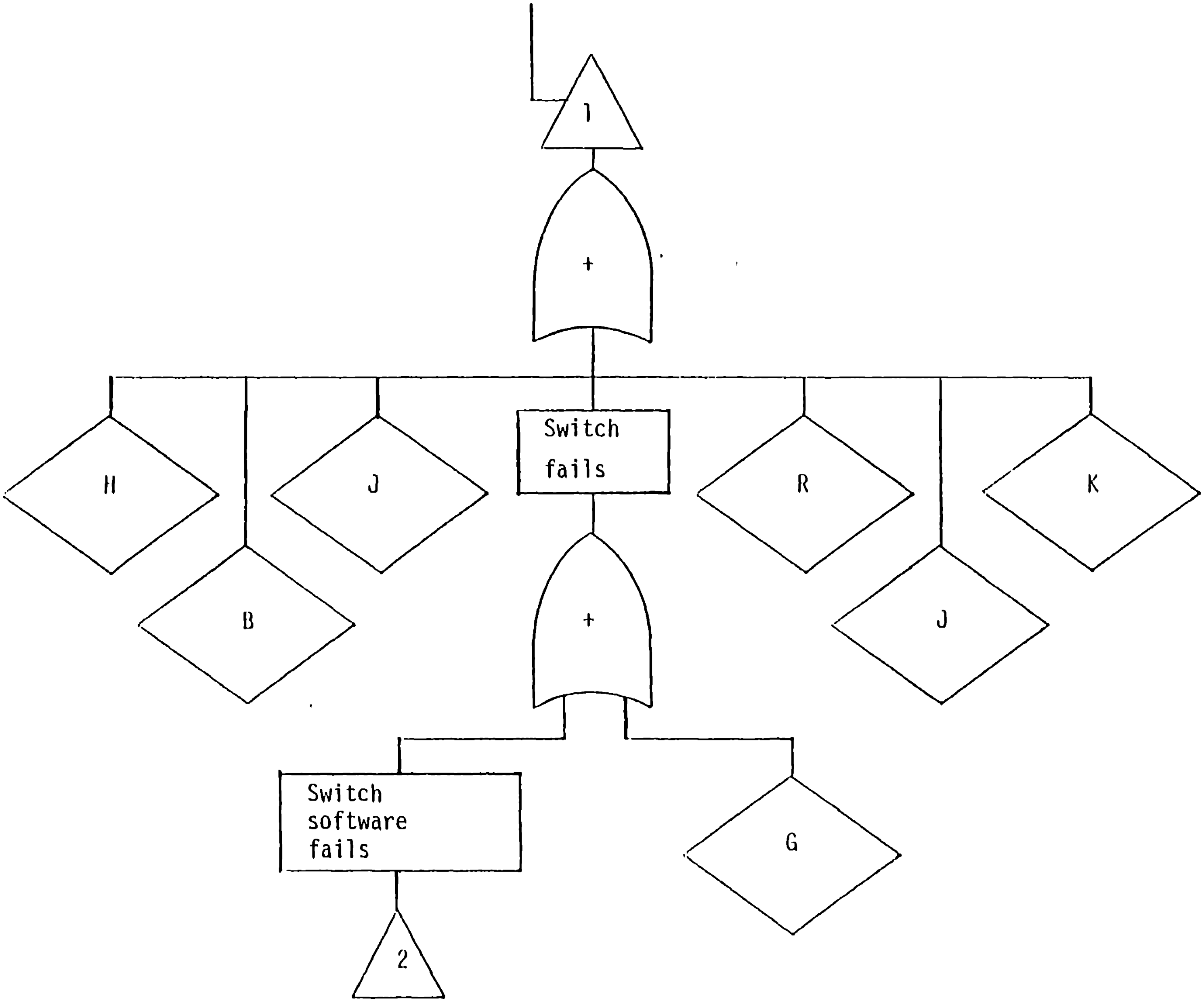


Figure D.3   (continued)

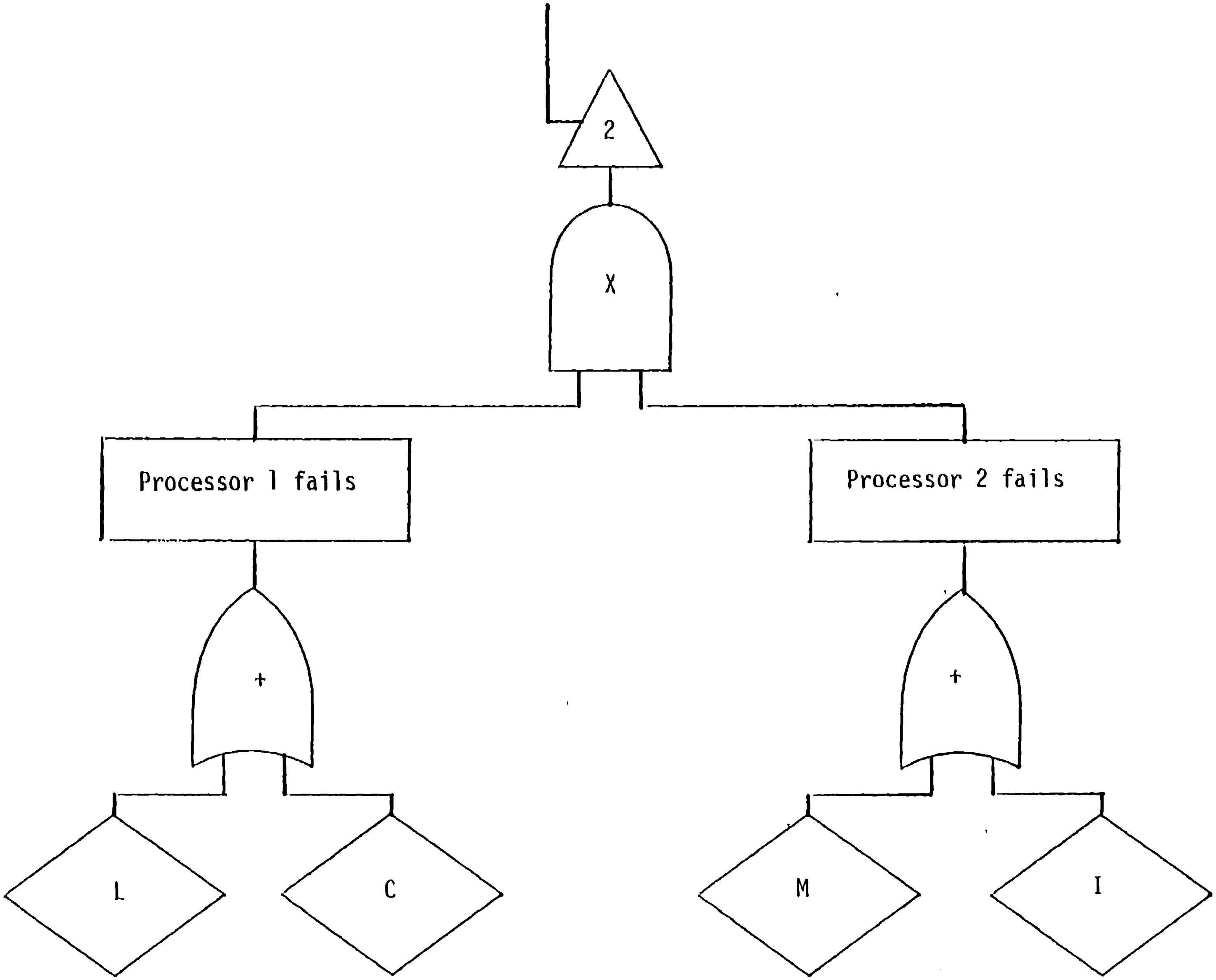


Figure D.3 (continued)

Table D.3

DUAL CENTRAL COMPUTER ARCHITECTURE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
A	3557.2	1.0	6.3	1.0	$2.241\text{x}10^4$	0.41599
B	.06	3.0	1.0	1.0	.18	$4.578\text{x}10^{-4}$
C	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
D	173.392	1.0	6.3	1.0	$1.092\text{x}10^3$	$1.731\text{x}10^{-5}$
E	.06	3.0	1.0	1.0	.18	$4.6934\text{x}10^{-3}$
H	3557.2	1.0	6.3	1.0	$2.241\text{x}10^4$	0.41599
I	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
J	173.392	1.0	6.3	1.0	$1.092\text{x}10^3$	$1.731\text{x}10^{-5}$
K	.06	3.0	1.0	1.0	.18	$4.6934\text{x}10^{-3}$
G	.155	1.0	6.3	1.0	$9.765\text{x}10^{-1}$	$2.4811\text{x}10^{-3}$
L	2696.05	1.0	6.3	1.0	$1.698\text{x}10^4$	0.3347
M	2696.05	1.0	6.3	1.0	$1.698\text{x}10^4$	0.3347
S						$8.997\text{x}10^{-4}$
R						$8.997\text{x}10^{-4}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
A	Processor 1	Central processor hardware 1 fails
B	Control cables	Control line fails
C	Control software	Control software 1 fails
D	MMI 1	MMI 1 system fails
E	Diagnosis cables 1	Diagnosis line 1 fails
H	Processor 2	Central processor hardware 2 fails
J	MMI 2	MMI 2 system fails
K	Diagnosis cables 2	Diagnosis line 2 fails

Table D.3 (continued)
DUAL CENTRAL COMPUTER ARCHITECTURE (SITUATION ONE)

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
G	Switch hardware	Switch hardware fails
L	Processor 1 hardware	Processor hardware 1 fails (SR)
M	Processor 2 hardware	Processor hardware 2 fails (SR)
S	Secondary storage system 1	Secondary storage system 1 fails
R	Secondary storage system 2	Secondary storage system 2 fails

DUAL CENTRAL COMPUTER ARCHITECTURE

PROBABILISTIC EQUATIONS (SITUATION ONE)

$TE = (A + B + C + D + E + S) \times [H + B + I + + R J + K + G + (L+C) \times (M + I)]$ (from the fault tree)

$TE = F_0$ $\qquad p(TE) = p(F_0)$

$F_0 = F_1 \times F_2$ $\qquad p(F_0) = p(F_1) \times p(F_2)$

$F_1 = F_8 + F_9$ $\qquad p(F_1) = p(F_8) + p(F_9) - p(F_8)p(F_9)$

$F_8 = F_3 + F_4$ $\qquad p(F_8) = p(F_3) + p(F_4) - p(F_3)p(F_4)$

$F_9 = B + C$ $\qquad p(F_9) = p(B) + p(C) - p(B)p(C)$

$F_3 = A + D$ $\qquad p(F_3) = p(A) + p(D) - p(A)p(D)$

$F_4 = E + S$ $\qquad p(F_4) = p(E) + p(S) - p(E)p(S)$

$F_2 = F_{10} + F_{11}$ $\qquad p(F_2) = p(F_{10}) + p(F_{11}) - p(F_{10})p(F_{11})$

$F_{10} = F_5 + F_6 + F_7$ $\qquad p(F_2) = p(F_5) + p(F_6) + p(F_7) + p(F_5)p(F_6)p(F_7) - p(F_5)p(F_6) - p(F_5)p(F_7) - p(F_6)p(F_7)$

$F_{11} = B + I + G$ $\qquad p(F_{11}) = p(B) + p(I) + p(G)$

$F_5 = H + R$ $\qquad p(F_5) = p(H) + p(R) - p(H)p(R)$

$F_6 = J + K$ $\qquad p(F_6) = p(J) + p(K) - p(J)p(K)$

$F_7 = (L+C) X (M + I)$ $\qquad p(F_7) = [p(L) + p(C) - p(L) + p(C)] \times [p(M) + p(I) - p(M) \times p(I)]$

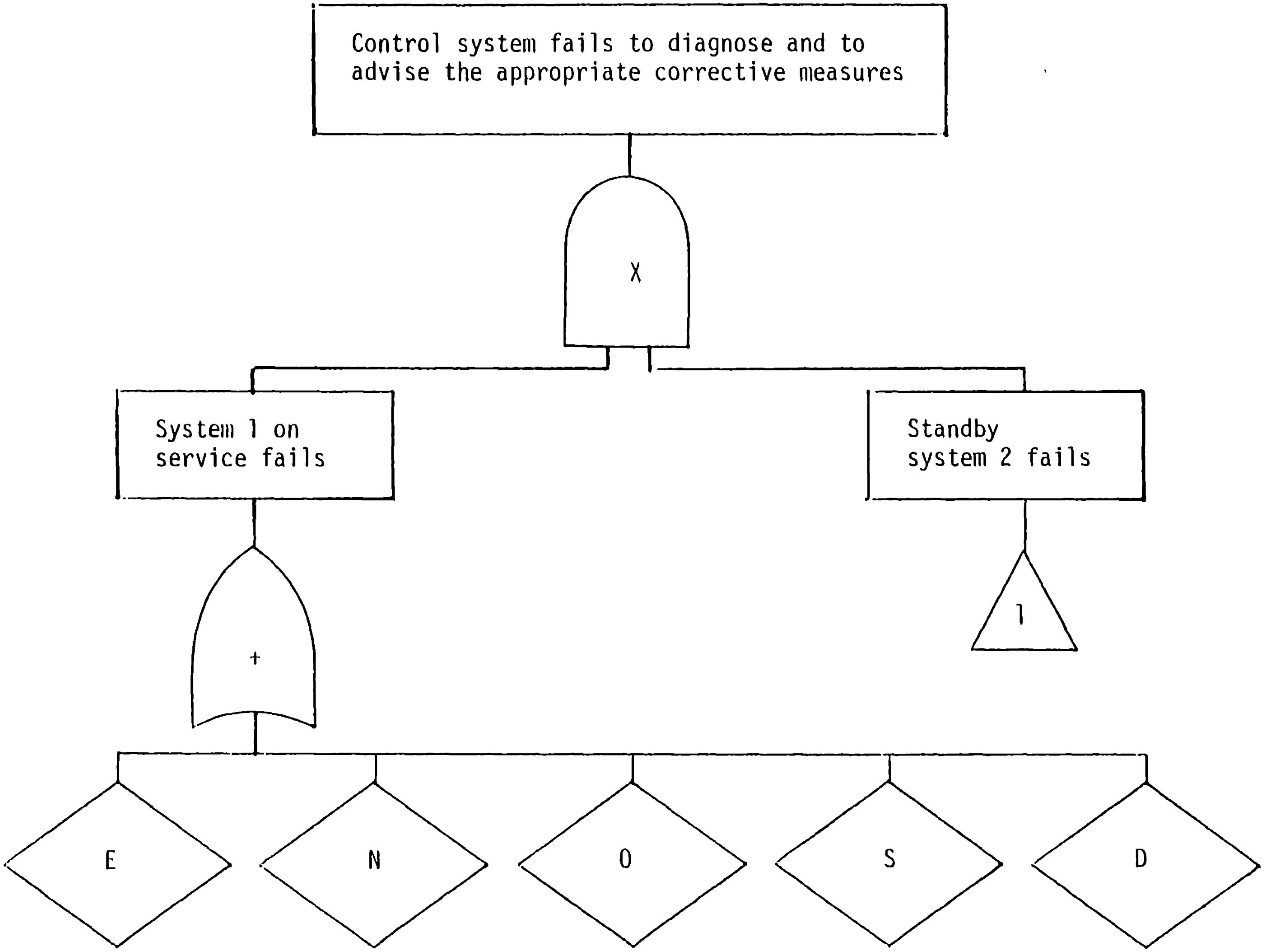

Control system fails to diagnose and to advise the appropriate corrective measures
X
System 1 on service fails
Standby system 2 fails
+
1
E
N
O
S
D

Figure D.4 Dual central computer architecture, situation two.

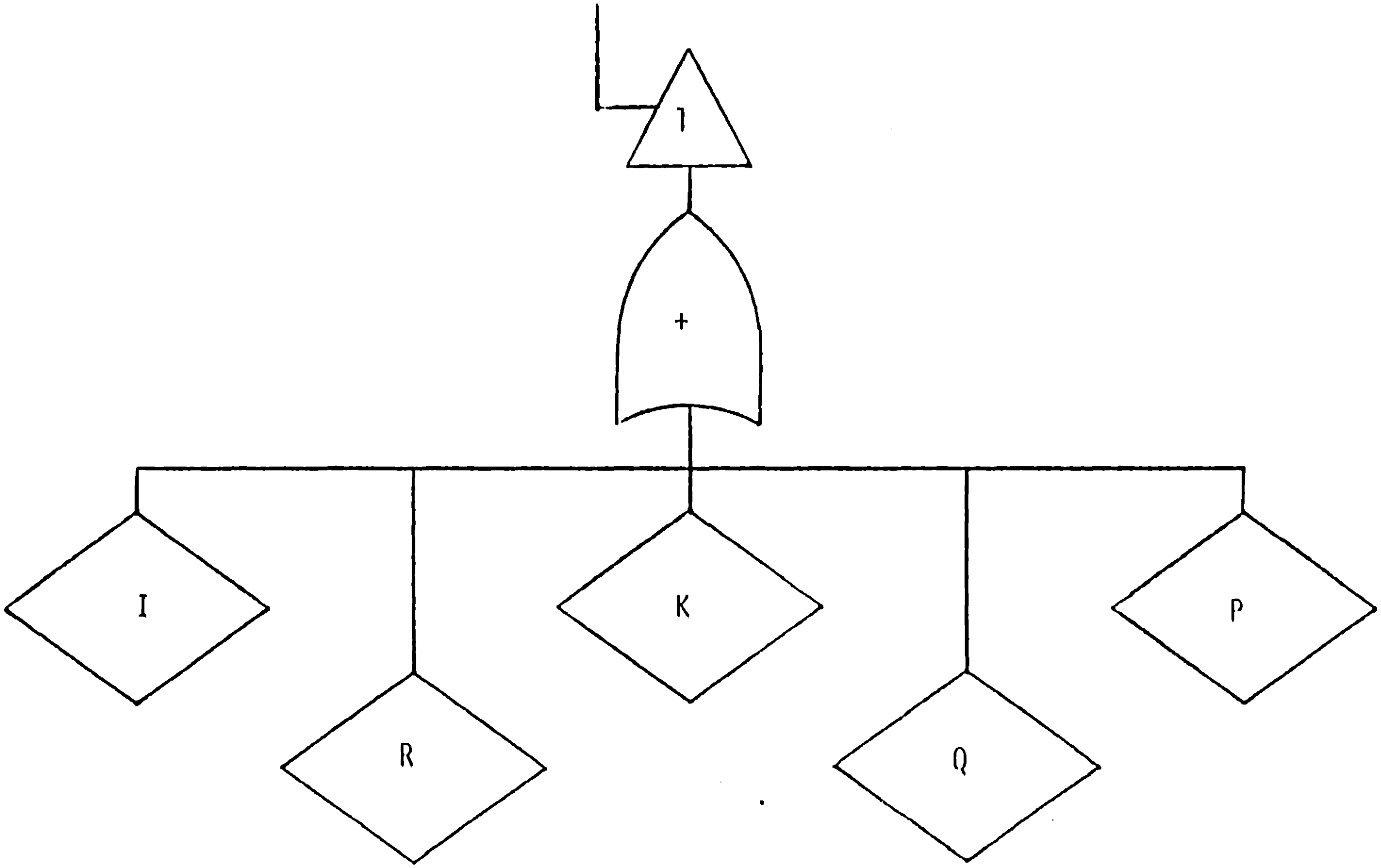


Figure D.4 (continued)

Table D.4

DUAL CENTRAL COMPUTER ARCHITECTURE (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	($F/10^6h$)	π_Q	π_E	π_L	($F/10^6h$)	
N	1247.36	1.0	6.3	1.0	7.858×10^3	0.1719
O	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
S						8.997×10^{-4}
P	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
Q	1247.36	1.0	6.3	1.0	7.858×10^3	0.1719
R						8.997×10^{-4}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
N	Processor 1 hardware	Central processor hardware 1 fails
O	Diagnosis software 1	Diagnosis software 1 fails
S	Secondary storage system 1	Storage system 1 fails
P	Diagnosis software 2	Diagnosis software fails
Q	Processor 2 hardware	Processor 2 hardware fails
R	Secondary storage system 2	Storage system 1 fails

DUAL CENTRAL COMPUTER ARCHITECTURE

PROBABILISTIC EQUATIONS (SITUATION TWO)

$TE = (E + N + O + S + D) \times (J + K + P + Q + R)$ (from the fault tree)

$TE = F_1 \times F_2$ $\qquad p(TE) = p(F_1) \times p(F_2)$

$F_1 = F_3 + F_4 + O$ $\qquad p(F_1) = p(O) + p(F_3) + p(F_4) + p(F_3)p(F_4)p(O)$

$\qquad - p(F_3)p(F_4) - p(F_3)p(F_0) - p(F_4)p(F_0)$

$F_3 = E + N$ $\qquad p(F_3) = p(E) + p(N) - p(E)p(N)$

$F_4 = S + D$ $\qquad p(F_4) = p(S) + p(D) - p(S)p(D)$

$F_2 = P + F_5 + F_6$ $\qquad p(F_2) = p(P) + p(F_5) + p(F_0) + p(F_5)p(F_6)p(P)$

$\qquad\qquad - p(F_5)(F_6) - p(F_5)p(P) - p(F_6)p(P)$

$F_5 = J + K$ $\qquad p(F_5) = p(J) + p(K) - p(J)p(K)$

$F_6 = Q + R$ $\qquad p(F_6) = p(Q) + p(R) - p(Q)p(R)$

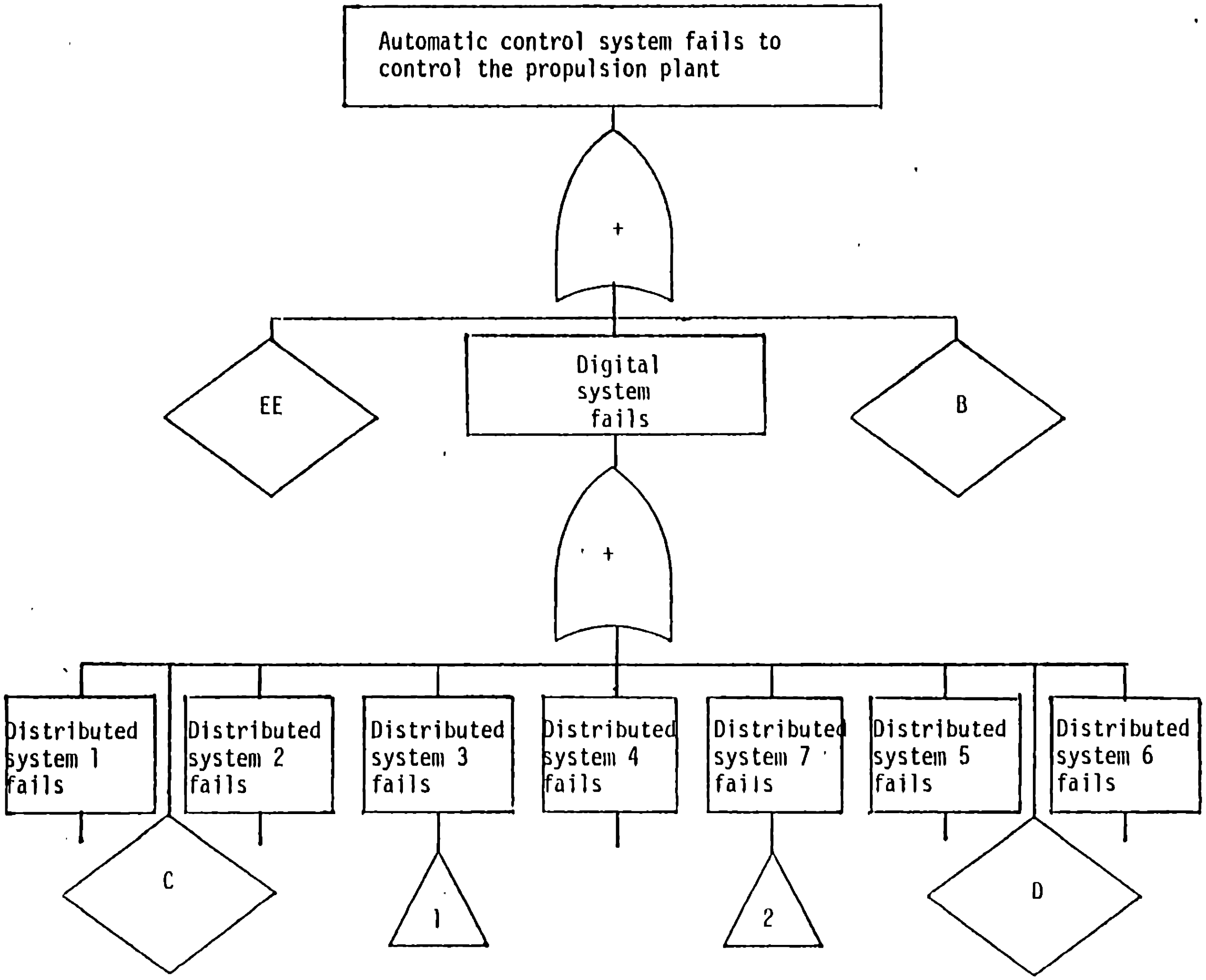

Automatic control system fails to control the propulsion plant
+
EE
Digital system fails
B
+
Distributed system 1 fails
Distributed system 2 fails
Distributed system 3 fails
Distributed system 4 fails
Distributed system 7 fails
Distributed system 5 fails
Distributed system 6 fails
C
1
2
D

Figure D.5 Star architecture, parallel transmission alternative, situation one.

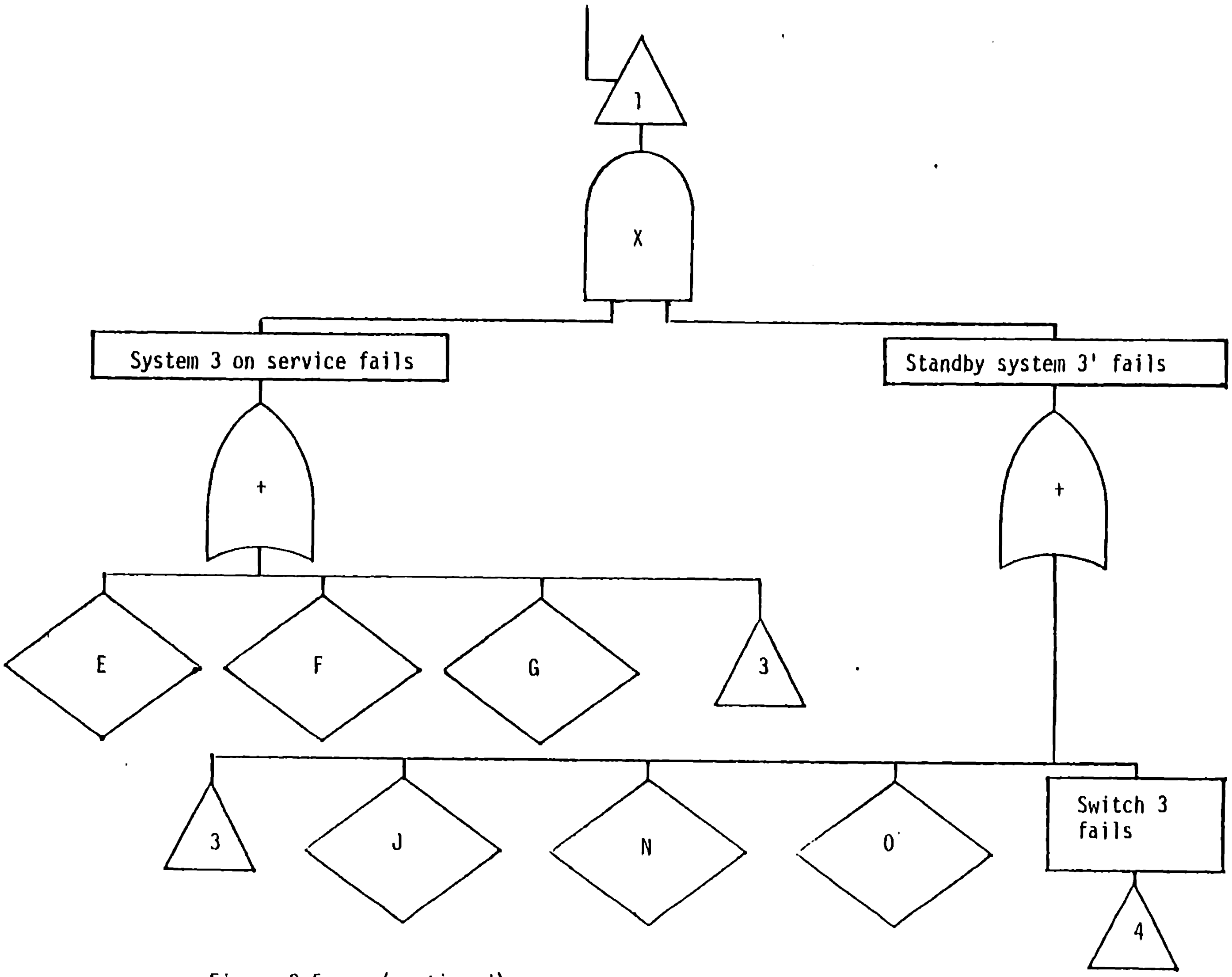


Figure D.5 (continued)

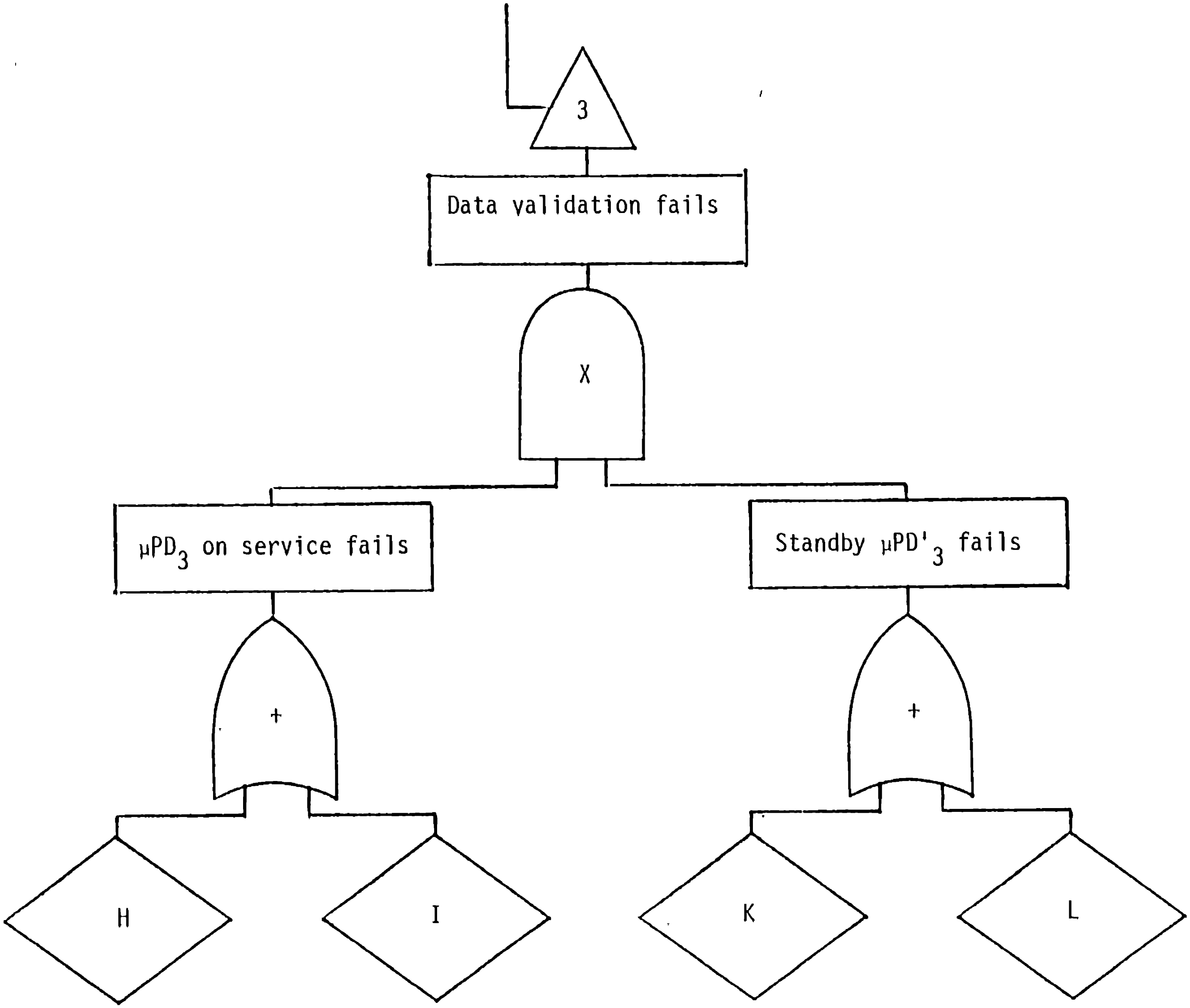


Figure D.5 (continued)

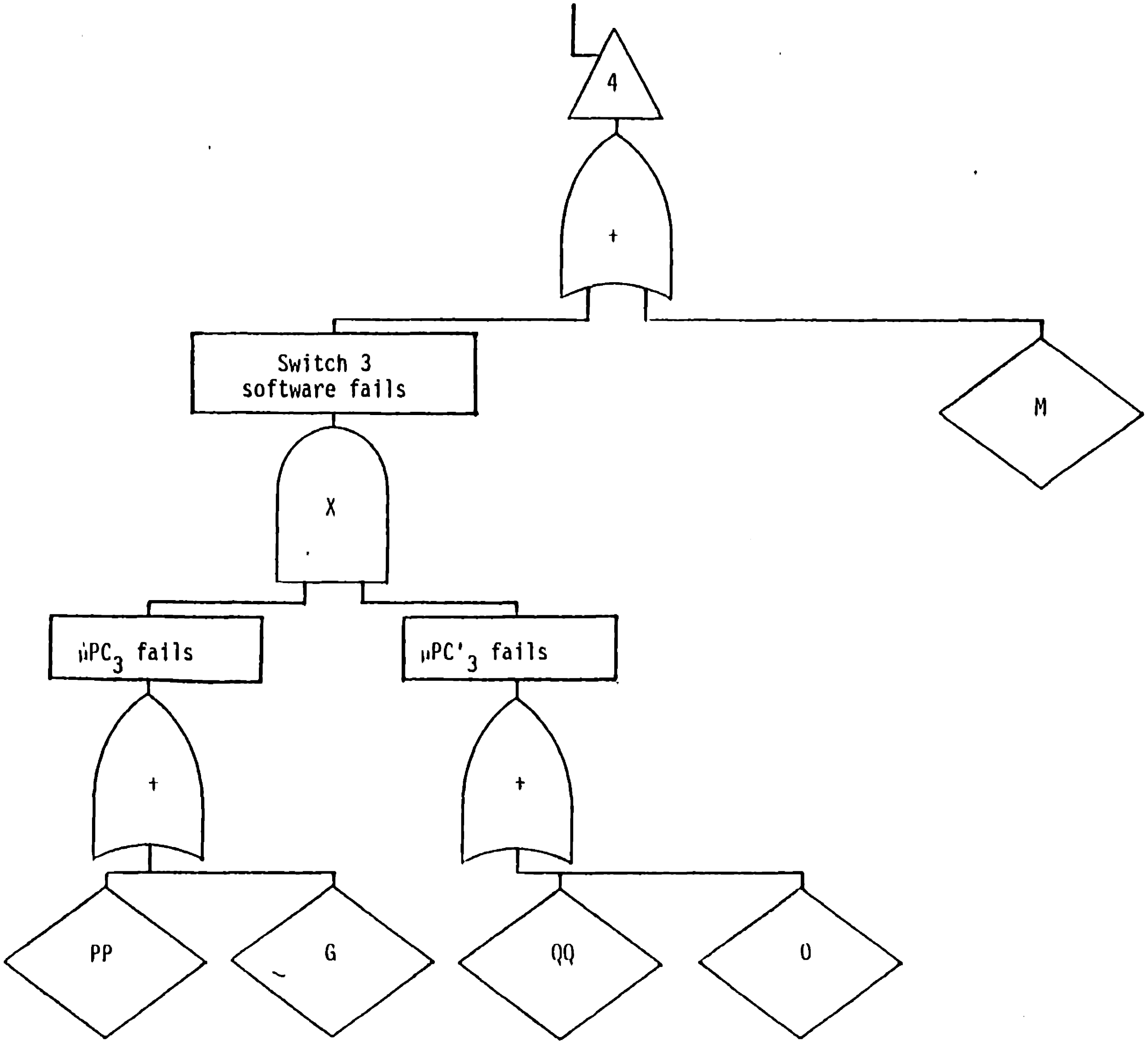


Figure D.5 (continued)

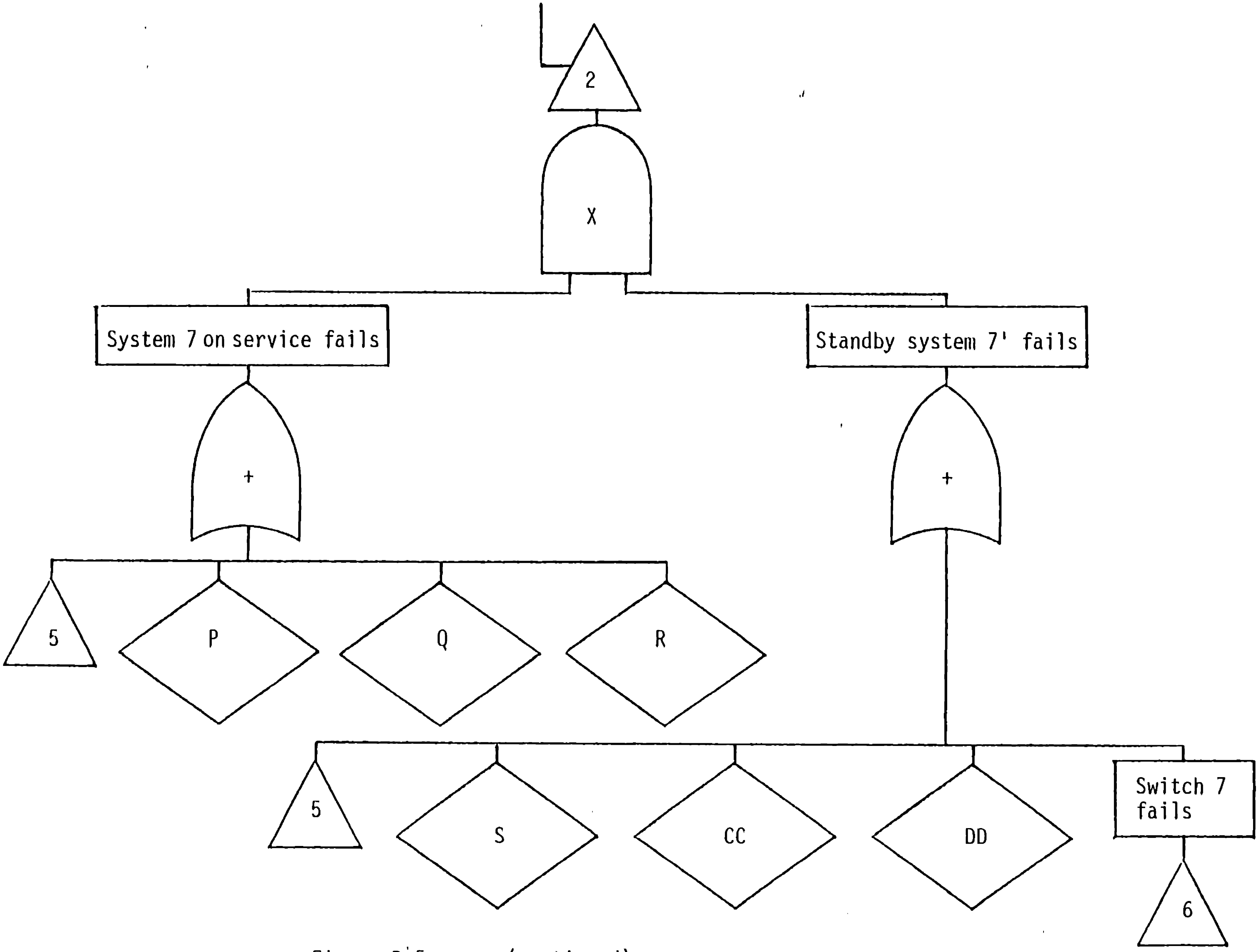


Figure D.5 (continued)

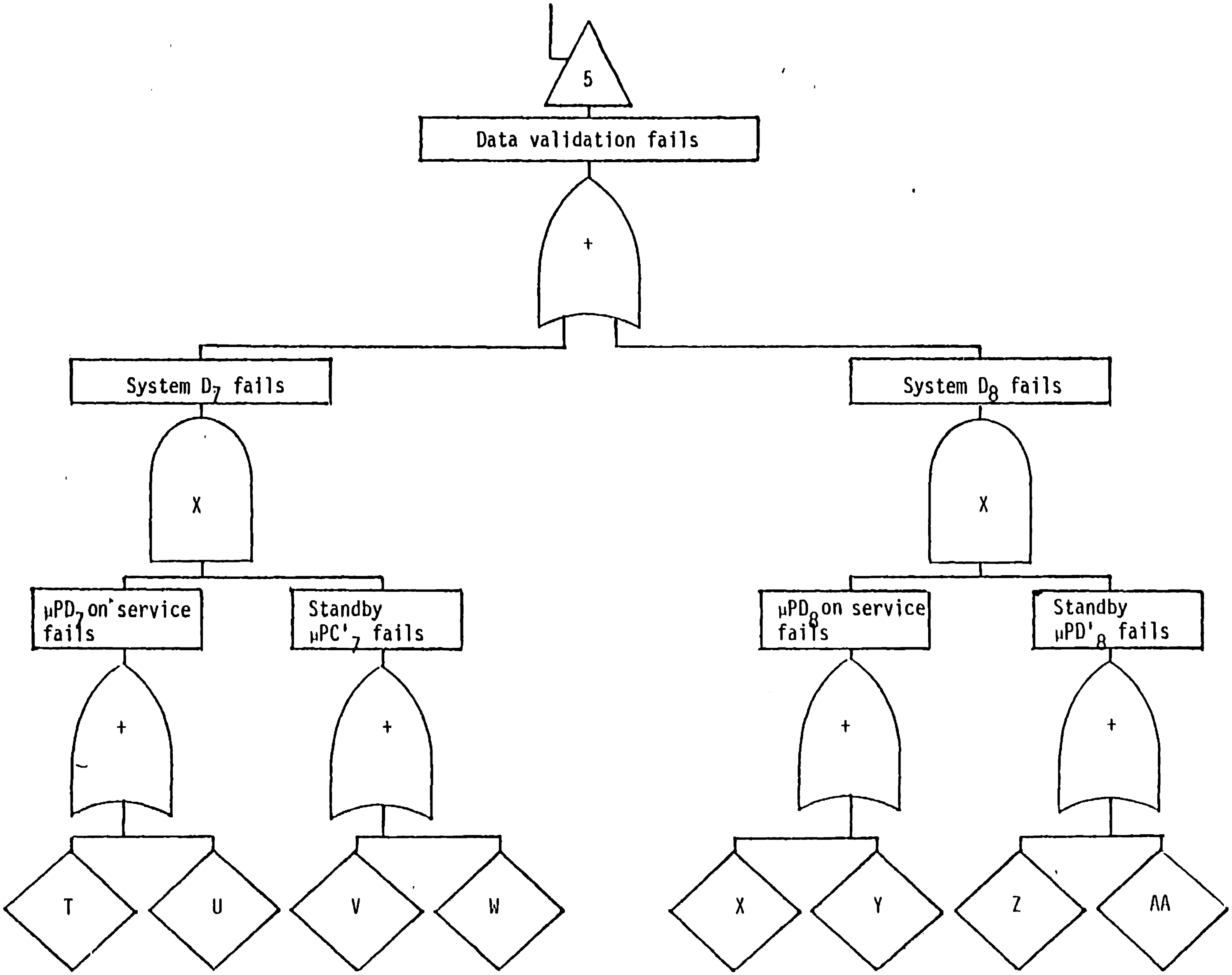

5
Data validation fails
+
System D_7 fails
System D_8 fails
X
X
μPD_7 on service fails
Standby $\mu PC'_7$ fails
μPD_8 on service fails
Standby $\mu PD'_8$ fails
+
+
+
+
T
U
V
W
X
Y
Z
AA

Figure D.5 (continued)

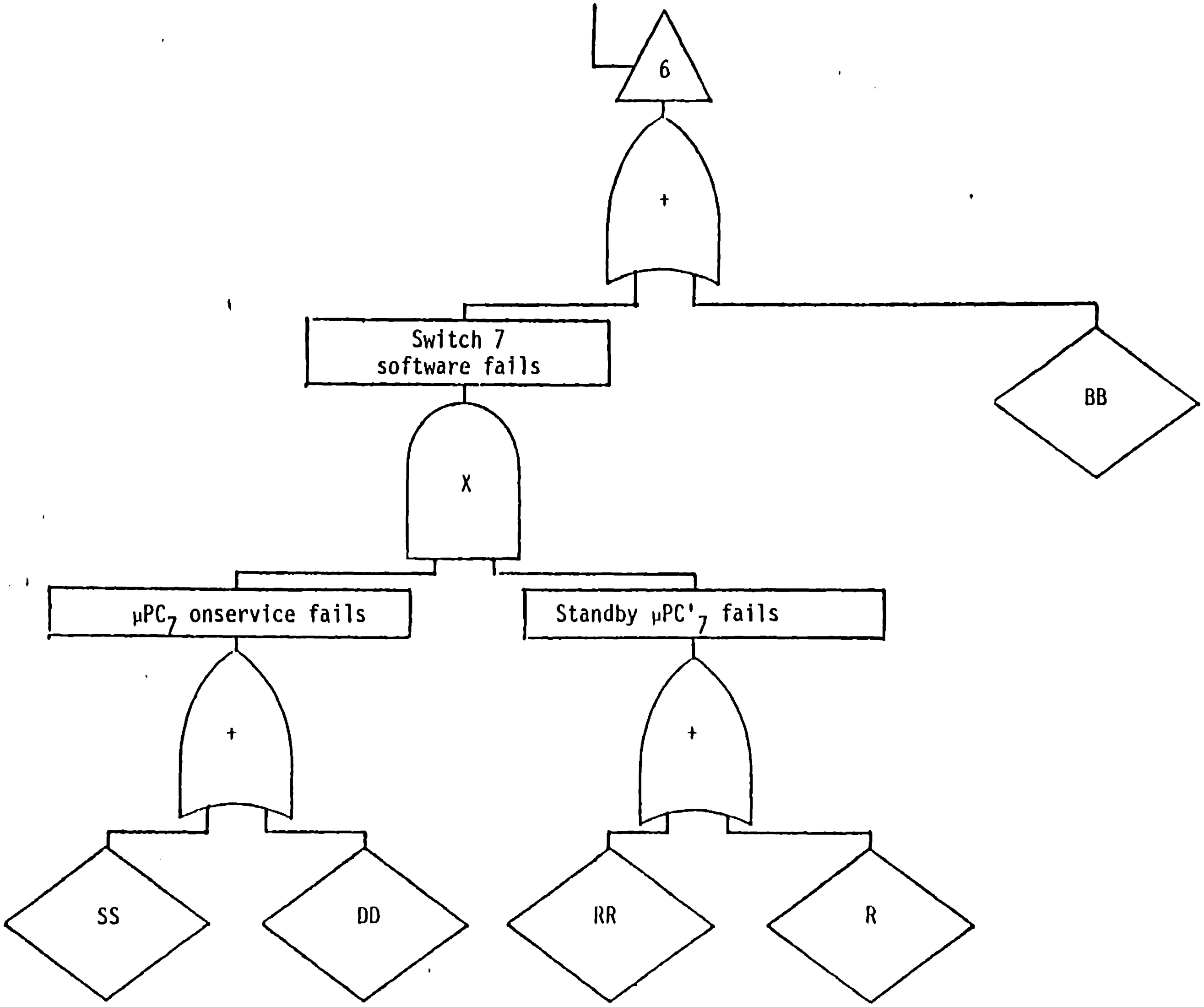


Figure D.5 (continued)

Table D.5

STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^{6}h)	π_Q	π_E	π_L	(F/10^{6}h)	
B	173.392	1.0	6.3	1.0	1.092x10^{3}	1.731x10^{-5}
C	539.1	1.0	6.3	1.0	3.396x10^{3}	7.827x10^{-2}
D	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
E	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
F	106.837	1.0	1.0	1.0	673.07	1.602x10^{-2}
G	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
H	101.065	1.0	6.3	1.0	636.71	1.516x10^{-2}
I	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
J	.06	2.0	1.0	1.0	.18	4.32x10^{-6}
K	101.065	1.0	6.3	1.0	636.71	1.516x10^{-2}
L	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
N	106.837	1.0	1.0	1.0	673.07	1.602x10^{-2}
O	5.479	1.0	1.0	1.0	916.00	1.31419x10^{-4}
M	.155	1.0	6.3	1.0	.9765	1.8747x10^{-4}
PP	67.6105	1.0	6.3	1.0	425.95	1.017x10^{-2}
QQ	67.6105	1.0	6.3	1.0	425.95	1.017x10^{-2}
Q	106.837	1.0	6.3	1.0	673.07	1.602x10^{-2}
P	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
R	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}

Table D.5 (continued)

STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
S	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
T	101.065	1.0	6.3	1.0	636.71	$1.516\text{x}10^{-2}$
U	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
V	101.065	1.0	6.3	1.0	636.71	$1.516\text{x}10^{-2}$
W	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
X	101.065	1.0	6.3	1.0	636.71	$1.516\text{x}10^{-2}$
Y	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
Z	101.065	1.0	6.3	1.0	636.71	$1.516\text{x}10^{-2}$
AA	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
CC	106.837	1.0	6.3	1.0	673.07	$1.602\text{x}10^{-2}$
DD	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
BB	.155	1.0	6.3	1.0	0.9675	$1.8747\text{x}10^{-4}$
RR	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
SS	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
EE						$8.997\text{x}10^{-4}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
B	MMI	MMI system fails
C	MC hardware	Central MC hardware fails
D	MC control software	MC control software fails
E	Cable	C3-MC line fails
F	μPC3 hardware	μPC3 hardware fails

Table D.5 (continued)

STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
G	μPC3 software	μPC3 software fails
J	Cable	C3'-MC line fails
H	μPD3 hardware	μPD3 hardware fails
I	μPD3 software	μPD3 software fails
K	μPD'3 hardware	μPD'3 hardware fails
L	μPD'3 software	μPD'3 software fails
N	μPC'3 hardware	μPC'3 hardware fails
O	μPC'3 software	μPC'3 software fails
M	Switch 3	Switch 3 hardware fails
PP	μPC3 hardware (SR)	μPC3 hardware fails
QQ	μPC3 software (SR)	μPC3 software fails
P	Cable	C7-MC line fails
Q	μPC7 hardware	μPC7 hardware fails
R	μPC3 software	μPC3 software fails
S	Cable	C7-MC line fails
T	μPD7 hardware	μPD7 hardware fails
U	μPD7 software	μPD7 software fails
V	μPD'7 hardware	μPD'7 hardware fails
W	μPD'7 software	μPD'7 software fails
X	μPD8 hardware	μPD8 hardware fails
Y	μPD8 software	μPD8 software fails
Z	μPD'8 hardware	μPD'8 hardware fails
AA	μPD'8 software	μPD'8 software fails
CC	μPC'7 hardware	μPD'7 hardware fails
DD	μPC'7 software	μPD'7 software fails
BB	Switch 7	Switch 7 hardware fails
RR	μPC7 hardware (SR)	μPC7 hardware (SR) fails
SS	μPC'7 software (SR)	μPC'7 software (SR) fails
EE	Secondary storage system	Secondary storage system fails

STAR ARCHITECTURE

PROBABILISTIC EQUATIONS PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

$$TE = B + EE + <C + D + \{ E + F + G + [H + I] \times [K + L] \} \times \{ J + N + O + M$$

$$+ [PP + G] \times [QQ + O] + [H + I] \times [K + L] \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ \}$$

$$+ \{ P + Q + R + [T + U] \times [V + W] + [X + Y] \times [Z + AA] \} > \times < \{ S + CC$$

$$+ DD + BB + [R + RR] \times [DD + SS] + [T + U] \times [V + W] + [X + Y] \times [Z + AA]\}>$$

(from the fault tree)

Note: Blank parentheses represent the other five similar distributed control systems; these are not the same events, but because the hardware and the software will be similar, they will end up with the same probability of failure. (All the sofware is debugged until it has reached a required probability of failure, in this case the $(P_f)_{reg}$ is the same for all the distributed systems.)

By using the following Boolean law $(C_1 + C_2) \times (C_1 + C_3) = C_1 + (C_2 \times C_3)$, the latter expression is reduced to:

$$TE = B + EE + C + D + \{[H + I] + [K + L] + [J + N + O + M + (PP + G)] \times [(QQ + O] \times [E + F + G]\} + \{\ \} + \{\ \} + \{\ \} + \{\ \} + \{\ \} + \{[T + U] \times [V + W] + [X + Y] \times [Z + AA] + [P + Q + R] \times [S + CC + DD + BB + (R + RR) \times (DD + SS)]\}$$

The next step is to apply the probabilistic equations to the Boolean expressions. When the probabilities involved are higher (0.1 or higher) the full equation is used. If values of probabilities are small, it will be used the standard approximation of deleting the product terms of the full equation.

The expressions for the full equations are:

$$p(A + B) = p(A) + p(B) - p(A)p(B)$$

$$p(A + B + C) = p(A) + p(B) + P(C) + p(A)p(B)p(C) - p(A)p(B) - p(A)p(C) - p(B)p(C)$$

Applying the Boolean expression to the probabilistic equations, the following implicit equations are obtained.

$$TE = F_1 + F_2 + F_3 \qquad p(TE) = p(F_1) + p(F_2) + p(F_3) + p(F_1)p(F_2)p(F_3)$$

$$- p(F_1)p(F_2) - p(F_1)p(F_3) - p(F_2)p(F_3)$$

$$F_1 = D + F_4 + F_5 \qquad p(F_1) = p(D) + p(F_4) + p(F_5) + p(F_4)p(F_5)p(D)$$

$$- p(F_4)p(F_5) - p(F_4)p(D) - p(F_5)p(D)$$

$$-p(F_5)p(D)$$

$$F_4 = B \qquad p(F_4) = p(B)$$

$$F_5 = EE + C \qquad p(F_5) = p(EE) + p(C) - p(EE)p(C)$$

$$F_6 = F_7 + F_7 + F_7 \qquad p(F_6) = 3p(F_7) + p(F_7)^3 - 3p(F_7)^2$$

$$F_7 = F_8 + F_9 \qquad p(F_7) = p(F_8) + p(F_9) - p(F_8)p(F_9)$$

$$F_8 = (H + I) \times (K + L) \qquad p(F_8) = [p(H) + p(I)] \times [p(K) + p(L)]$$

$$F_9 = F_{10} \times F_{11} \qquad p(F_9) = p(F_{10}) \times p(F_{11})$$

$$F_{10} = E + F + G \qquad p(F_{10}) = p(E) + p(F) + p(G)$$

$$F_{11} = F_{12} + F_{13} \qquad p(F_{11}) = p(F_{12}) + p(F_{13}) - p(F_{12})p(F_{13})$$

$$F_{12} = J + N + O + M \qquad p(F_{12}) = p(J) + p(N) + p(O) + p(M)$$

$$- p(O)p(N)$$

$$F_{13} = F_{14} \times F_{15} \qquad p(F_{13}) = p(F_{14}) \times p(F_{15})$$

$$F_{14} = PP + G \qquad p(F_{14}) = p(PP) + p(G)$$

$$F_{15} = QQ + O \qquad p(F_{15}) = p(QQ) + p(O) - p(QQ)p(O)$$

$$F_3 = F_{16} + F_{17} + F_{18} \qquad p(F_3) = p(F_{16}) + p(F_{17}) + p(F_{18})$$

$$+ p(F_{16})p(F_{17})p(F_{18}) - p(F_{16})p(F_{17})$$

$$- p(F_{16})p(F_{18}) - p(F_{17})p(F_{18})$$

$$F_{16} = (T + U) \times (V + W) \qquad p(F_{16}) = [p(T) + p(U)] \times [P(V) + p(W)]$$

$$F_{17} = (X + Y) \times (T + AA) \qquad p(F_{17}) = [p(X) + p(Y)] \times [P(z) + p(AA)]$$

$$F_{18} = F_{19} \times F_{20} \qquad p(F_{18}) = p(F_{19}) \times p(F_{20})$$

$$F_{19} = P + Q + R \qquad p(F\quad) = p(P) + p(Q) + P(R)$$

$$F_{20} = F_{21} \div F_{22} \qquad p(F_{20}) = p(F_{21}) + p(F_{22}) - p(F_{21})p(F_{22})$$

$$F_{21} = S + CC + DD + BB \qquad p(F_{21}) = p(S) + p(CC) + p(DD) + p(BB)$$

$$- \ p(CC)p(BB)$$

$$F_{22} = (R + RR) \times (DD + SS) \qquad p(F_{22}) = [p(R) + p(RR)] \times [p(DD) + p(SS)]$$

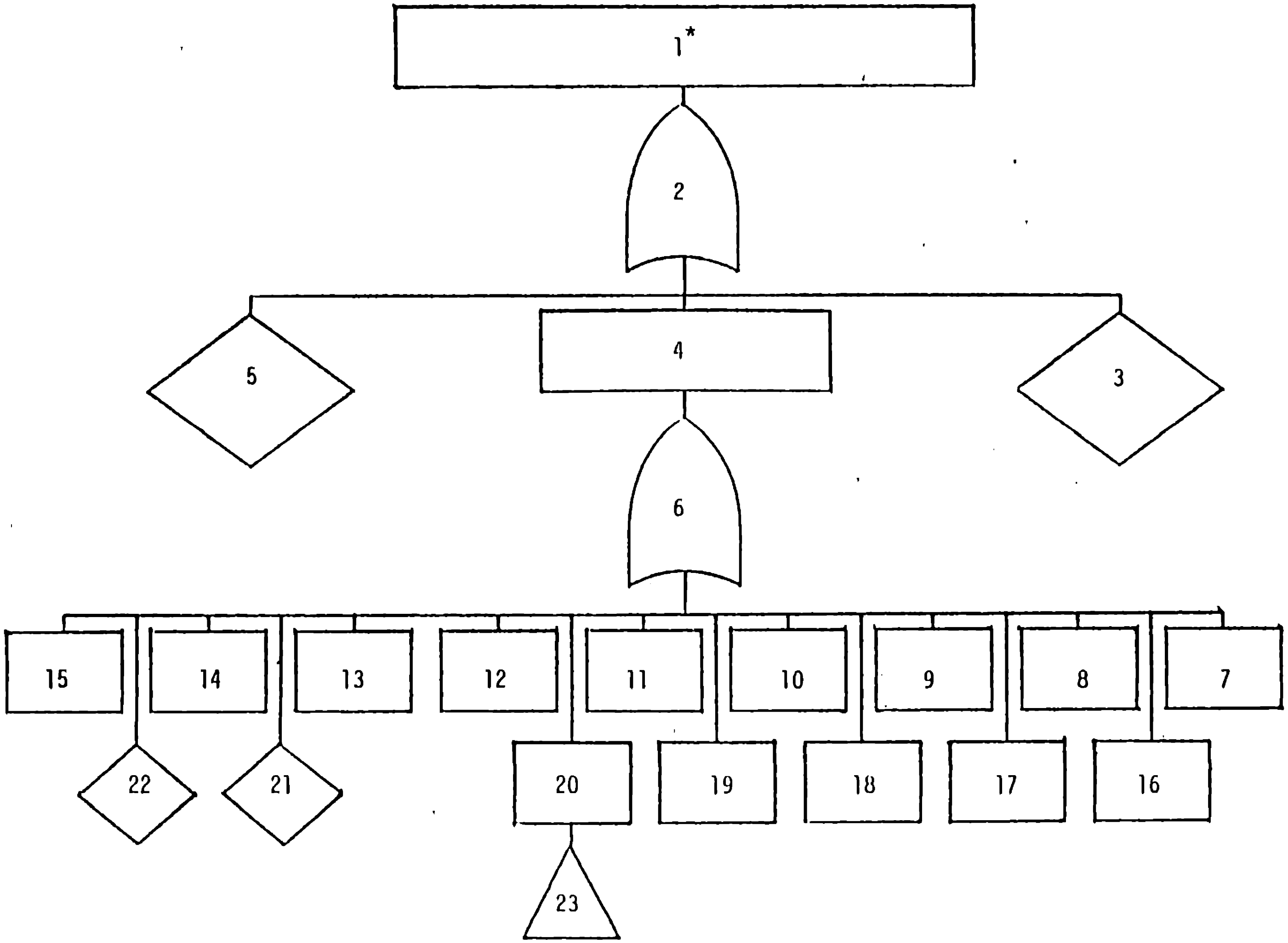


Figure D.6 Star architecture, parallel transmission alternative, situation 2

*See legend next page

1. Control system fails to diagnose and to advise the appropriate corrective measures
2. +
3. FF
4. Digital diagnosis system fails
5. EE
6. +
7. System D_1 fails
8. System D_2 fails
9. System D_4 fails
10. System D_5 fails
11. System D_6 fails
12. System D_7 fails
13. System D_8 fails
14. System D_9 fails
15. System D_{10} fails
16. System D_{11} fails
17. System D_{12} fails
18. System D_{13} fails
19. System D_{14} fails
20. System D_3 fails
21. GG
22. HH
23. 1

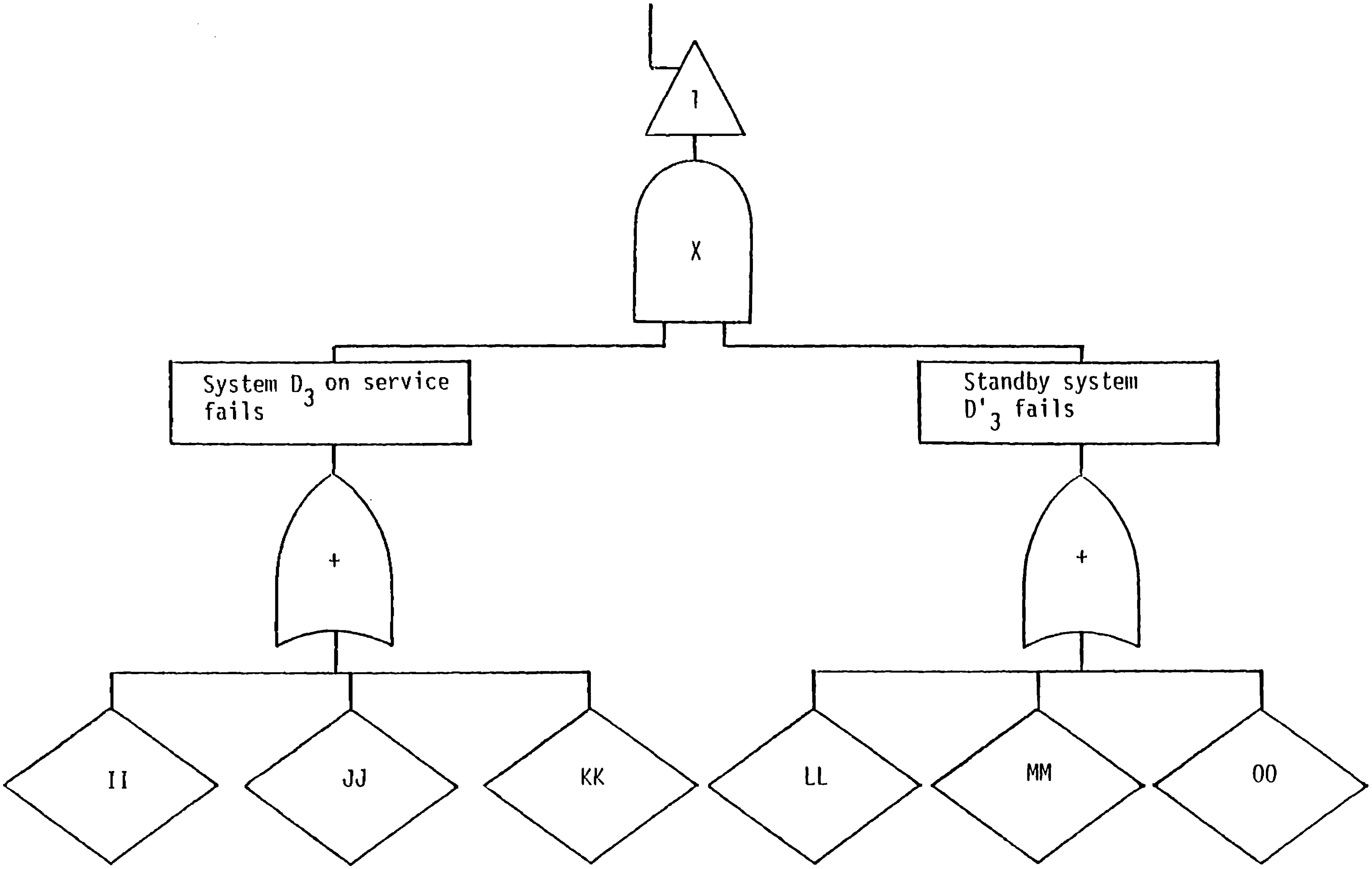


Figure D.6 (continued)

STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	$(F/10^6h)$	π_Q	π_E	π_L	$(F/10^6h)$	
EE						$8.997x10^{-4}$
FF	173.392	1.0	6.3	1.0	$1.092x10^3$	$1.731x10^{-5}$
GG	435.31	1.0	6.3	1.0	$2.741x10^3$	$6.367x10^{-2}$
HH	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
II	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
JJ	85.4216	1.0	6.3	1.0	538.157	$1.283x10^{-2}$
KK	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
LL	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
MM	85.4216	1.0	6.3	1.0	538.157	$1.283x10^{-2}$
OO	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
EE	Secondary storage system	Secondary storage sysem fails
FF	MMI	MMI system fails
GG	MC hardware	MC hardware fails
HH	MC Diagnosis software	MC diagnosis software fails
II	Cable	D3-MC line fails
JJ	μPD3 hardware	μPD3 hardware fails
KK	μPD3 software	μPD3 software fails
LL	Cable	D3-MC line fails
MM	μPD'3 hardware	μPD'3 hardware fails
OO	μPD'3 software	μPD'3 hardware fails

Table D.6 (continued)

STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

PROBABILISTIC EQUATIONS PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

$$TE = EE + FF + GG + HH + [II + JJ + KK] \times [LL + MM + OO] + [\ ] + [\ ] + + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ]$$

(from the fault tree)

The same observation about the blank brackets applies here. After applying the probability laws, the equations are:

$TE = F_1 + F_2$ $\qquad p(TE) = p(F_1) + p(F_2) - p(F_1)p(F_2)$

$F_1 = F_8 + F_9$ $\qquad p(F_1) = p(F_8) + p(F_9) - p(F_8)p(F_9)$

$F_8 = EE + FF$ $\qquad p(F_8) = p(EE) + p(FF) - p(EE)p(FF)$

$F_9 = GG + HH$ $\qquad p(F_9) = p(GG) + p(HH) - p(GG)p(HH)$

$F_2 = F_3 + F_3$ $\qquad p(F_2) = 2p(F_3) - p(F_3)^2$

$F_3 = F_4 + F_5$ $\qquad p(F_3) = p(F_4) + p(F_5) - p(F_4)p(F_5)$

$F_4 = F_6 + F_6$ $\qquad p(F_4) = 2p(F_6) - p(F_6)^2$

$F_5 = F_7 + F_7 + F_7$ $\qquad p(F_5) = 3p(F_7) + p(F_7)^3 - 2p(F_7)^2$

$F_6 = F_7 + F_7$ $\qquad p(F_6) = 2p(F_7) - p(F_7)^2$

$F_7 = [II + JJ + KK] \times [LL + MM + OO] = [p(II) + p(JJ) + p(KK)] \times [p(LL) + p(MM) + p(OO)]$

Table D.7

SERIAL TRANSMISSION ALTERNATIVE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	($F/10^6h$)	π_Q	π_E	π_L	($F/10^6h$)	
C	352.6944	1.0	6.3	1.0	2222.00	$5.193x10^{-2}$
F	104.301	1.0	6.3	1.0	651.096	$1.5647x10^{-2}$
H	98.256	1.0	6.3	1.0	620.7	$1.4786x10^{-2}$
Q	104.301	1.0	6.3	1.0	651.096	$1.5647x10^{-2}$
T	98.256	1.0	6.3	1.0	620.7	$1.4786x10^{-2}$
X	98.256	1.0	6.3	1.0	620.7	$1.4786x10^{-2}$
V	98.256	1.0	6.3	1.0	620.7	$1.4786x10^{-2}$
Z	98.256	1.0	6.3	1.0	620.7	$1.4786x10^{-2}$
CC	104.301	1.0	6.3	1.0	651.096	$1.5647x10^{-2}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
C	mC hardware	Central mC hardware fails
F	μPC3 hardware	μPC3 hardware fails
H	μPD3 hardware	μPD3 hardware fails
Q	μPC7 hardware	μPC7 hardware fails
T	μPD7 hardware	μPD7 hardware fails
X	μPD8 hardware	μPD8 hardware fails
V	μPD'7 hardware	μPD'7 hardware fails
Z	μPD'8 hardware	μPD'8 hardware fails
CC	μPC'7 hardware	μPC'7 hardware fails

Table D.7 (continued)

PROBABILISTIC EQUATIONS D.7 SERIAL TRANSMISSION ALTERNATIVE (SITUATION ONE)

The fault tree and the probablistic equations are exactly the same as the case of parallel transmission. Only few probabilities are different and these values are given in Table D.7.

Table D.8

SERIAL TRANSMISSION ALTERNATIVE (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	($F/10^6h$)	π_Q	π_E	π_L	($F/10^6h$)	
GG	327.052	1.0	6.3	1.0	2060.43	4.825×10^{-2}
JJ	83.6731	1.0	6.3	1.0	527.14	1.257×10^{-2}
MM	83.6731	1.0	6.3	1.0	527.14	1.257×10^{-2}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
GG	mC hardware	Central mC hardware fails
JJ	μPD3 hardware	μPD3 hardware fails
MM	μPD'3 hardware	μPD'3 hardware fails

STAR ARCHITECTURE

PROBABILISTIC EQUATIONS D.8 SERIAL TRANSMISSION ALTERNATIVE

(SITUATION TWO)

The fault tree and the probablistic equations are exactly the same as the case of parallel transmission. Only few probabilities are different and these values are given in Table D.8.

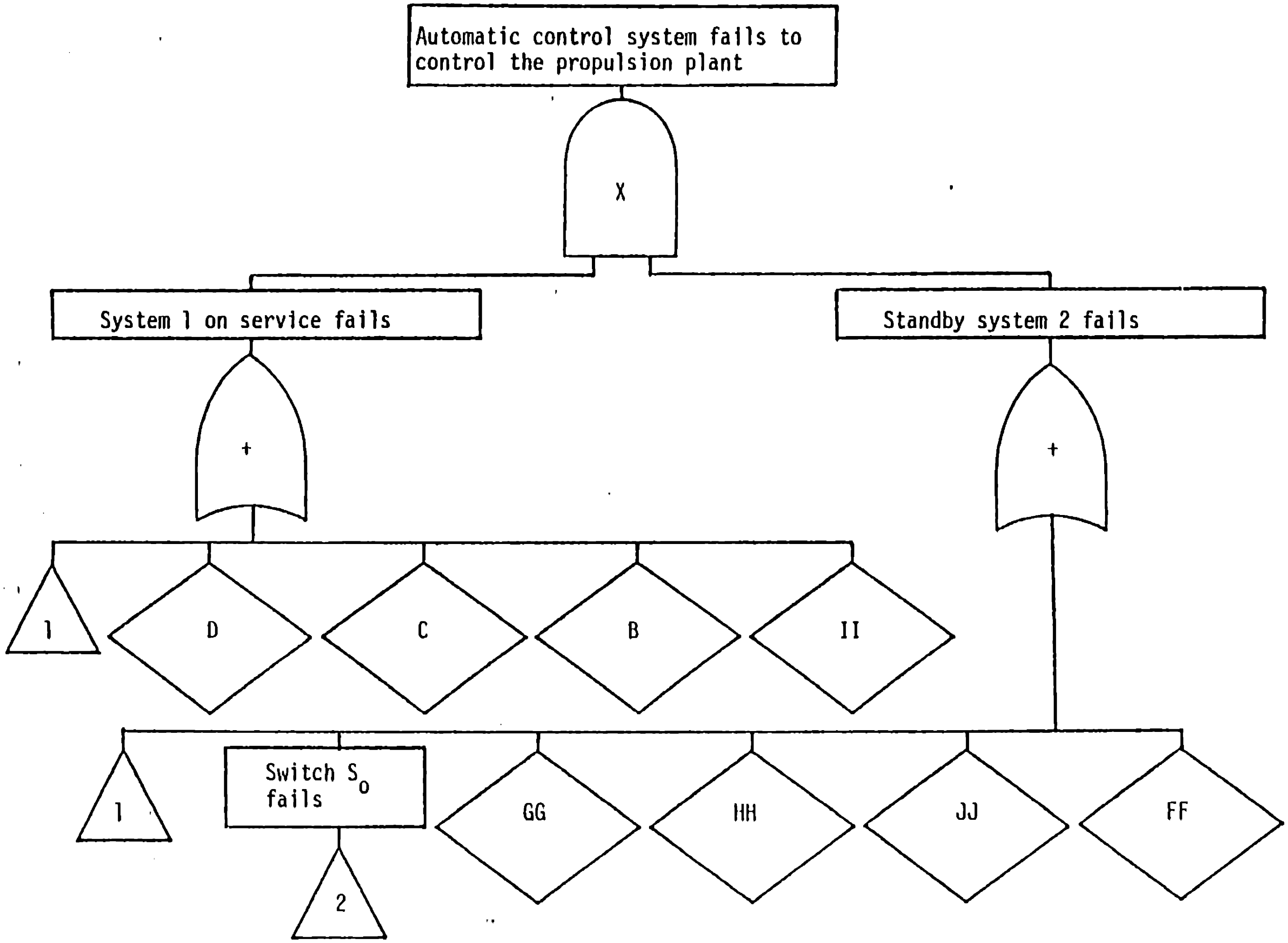

Automatic control system fails to control the propulsion plant
X
System 1 on service fails
Standby system 2 fails
+
+
1
D
C
B
II
1
Switch S_o fails
2
GG
HH
JJ
FF

Figure D.9 Dual star architecture, parallel transmission alternative, situation one.

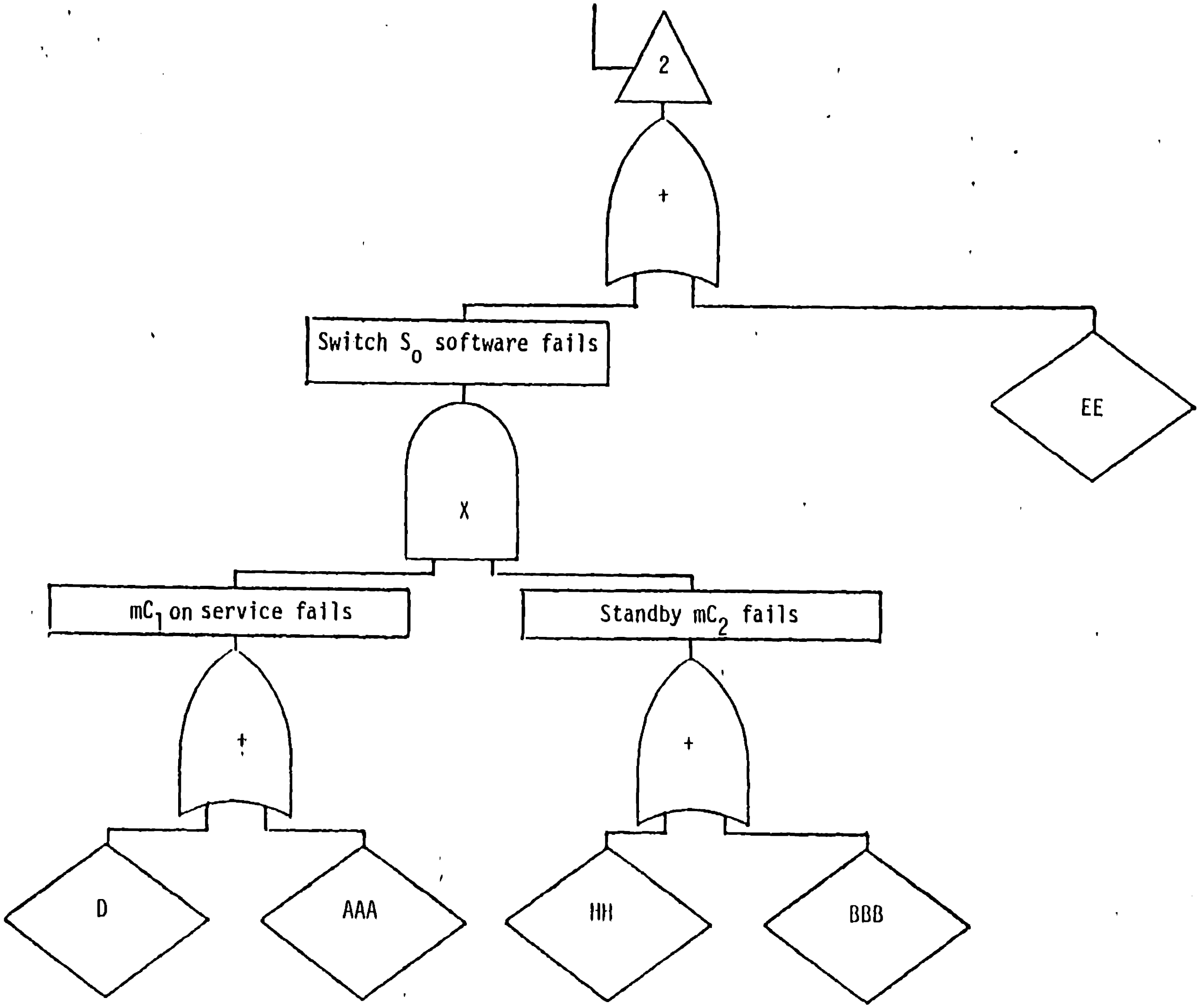


Figure D.9 (continued)

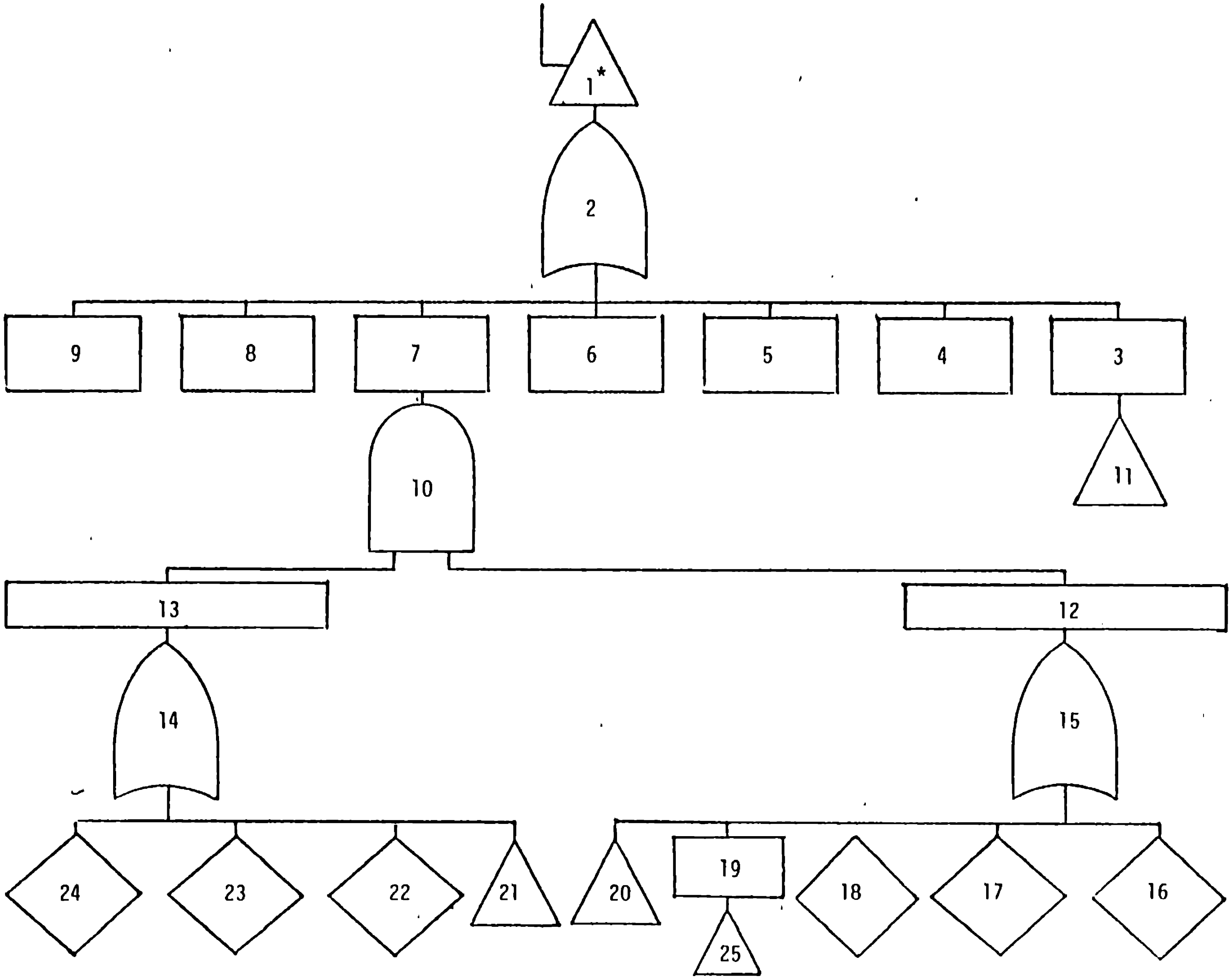


Figure D.9 (continued)
*See legend next page

1. 1
2. +
3. Distributed system 7 fails
4. Distributed system 6 fails
5. Distributed system 5 fails
6. Distributed system 4 fails
7. Distributed system 3 fails
8. Distributed system 2 fails
9. Distributed system 1 fails
10. X
11. 5
12. Standby system 3' fails
13. System 3 on service fails
14. +
15. +
16. 0
17. N
18. M
19. Switch 3 fails
20. 3
21. 3
22. F
23. E
24. G
25. 4

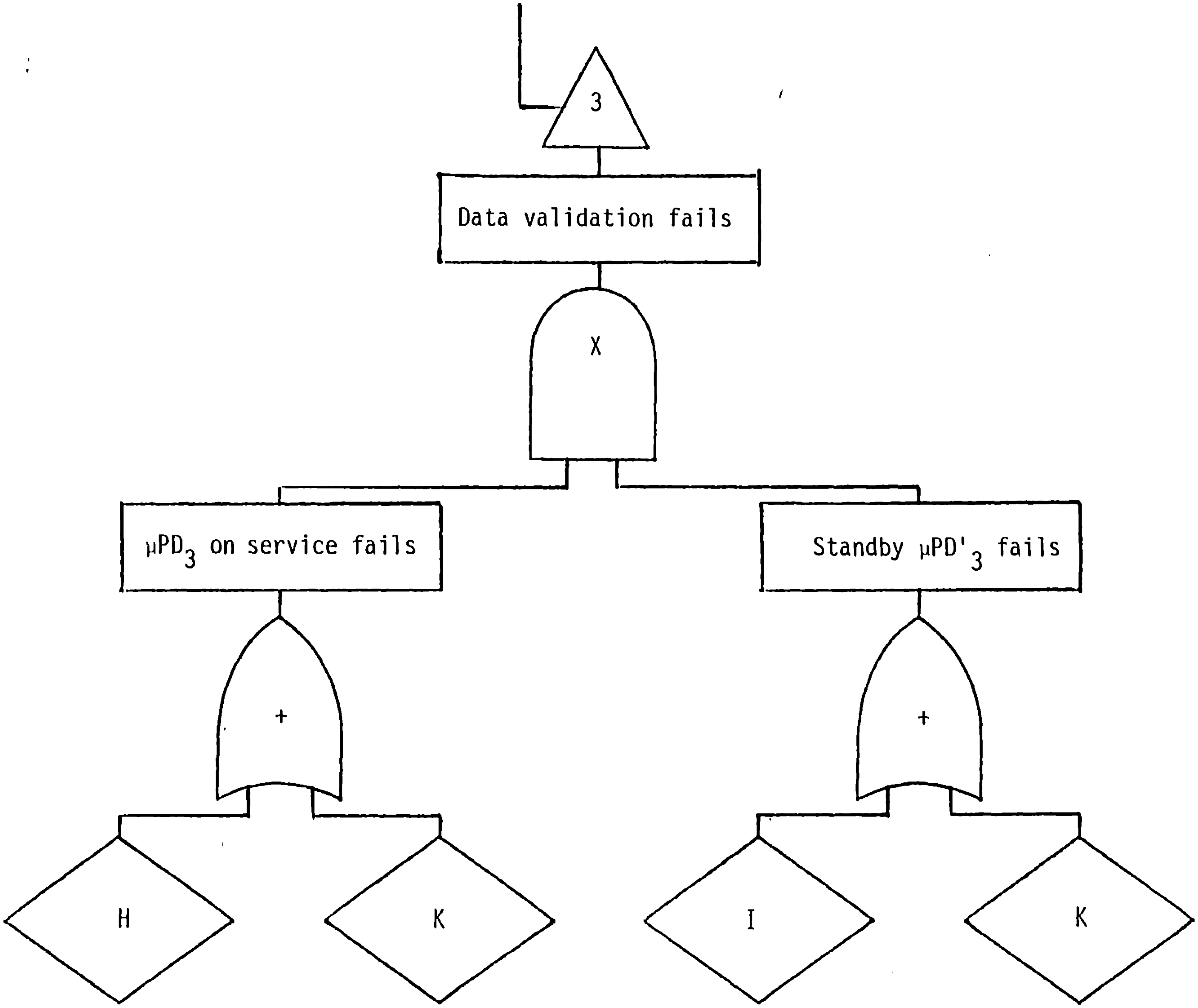


Figure D.9 (continued)

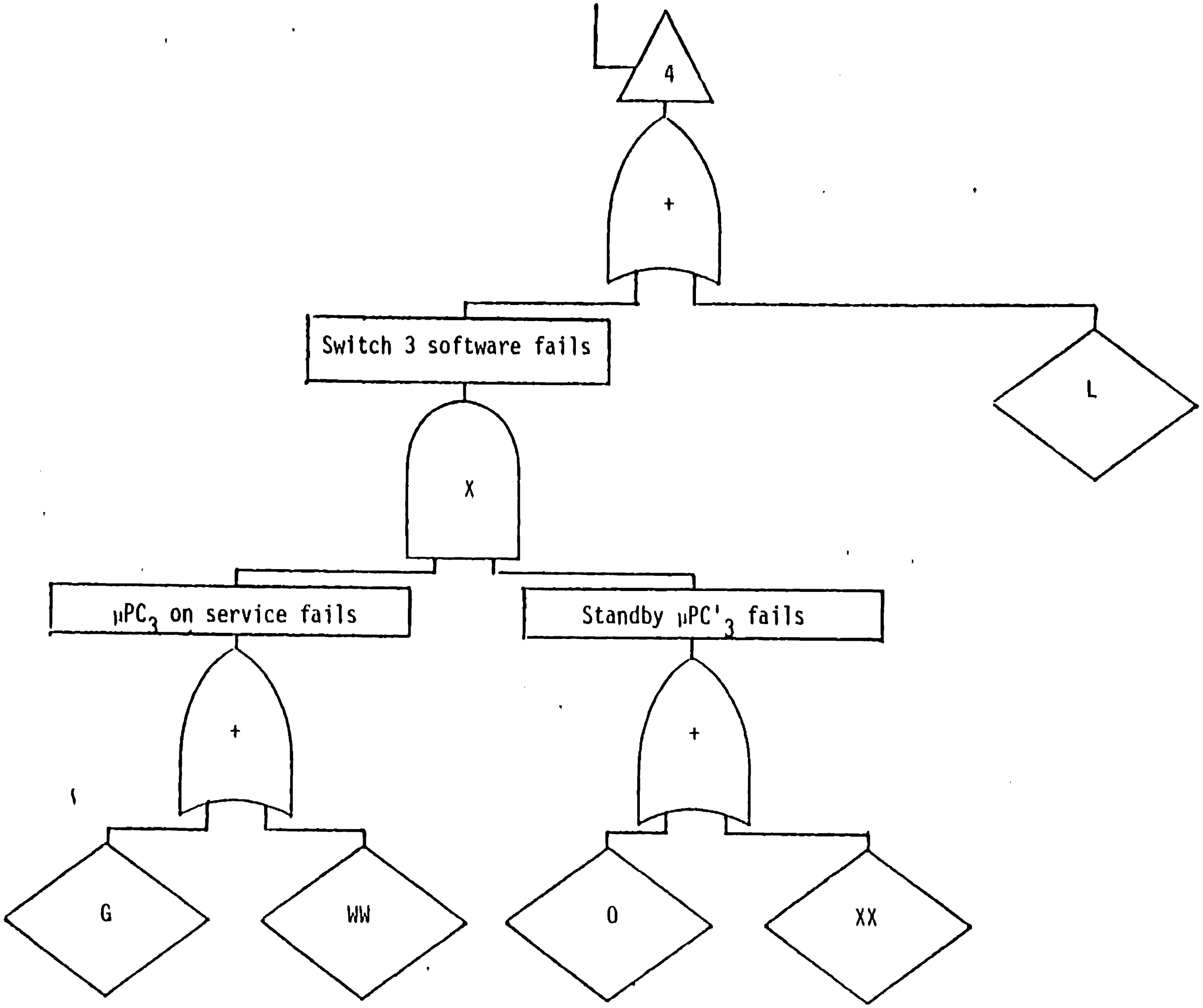


Figure D.9 (continued)

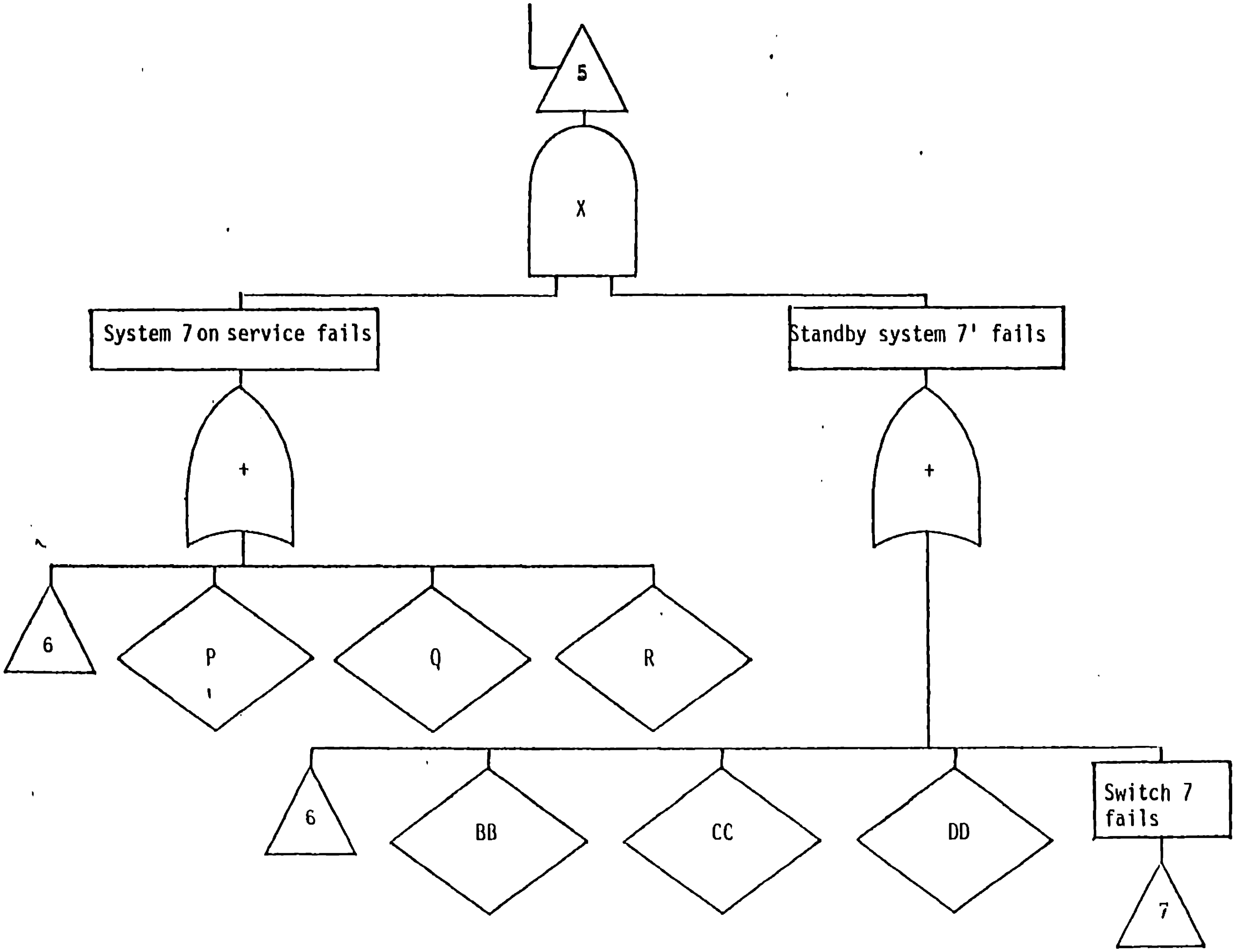


Figure D.9 (continued)

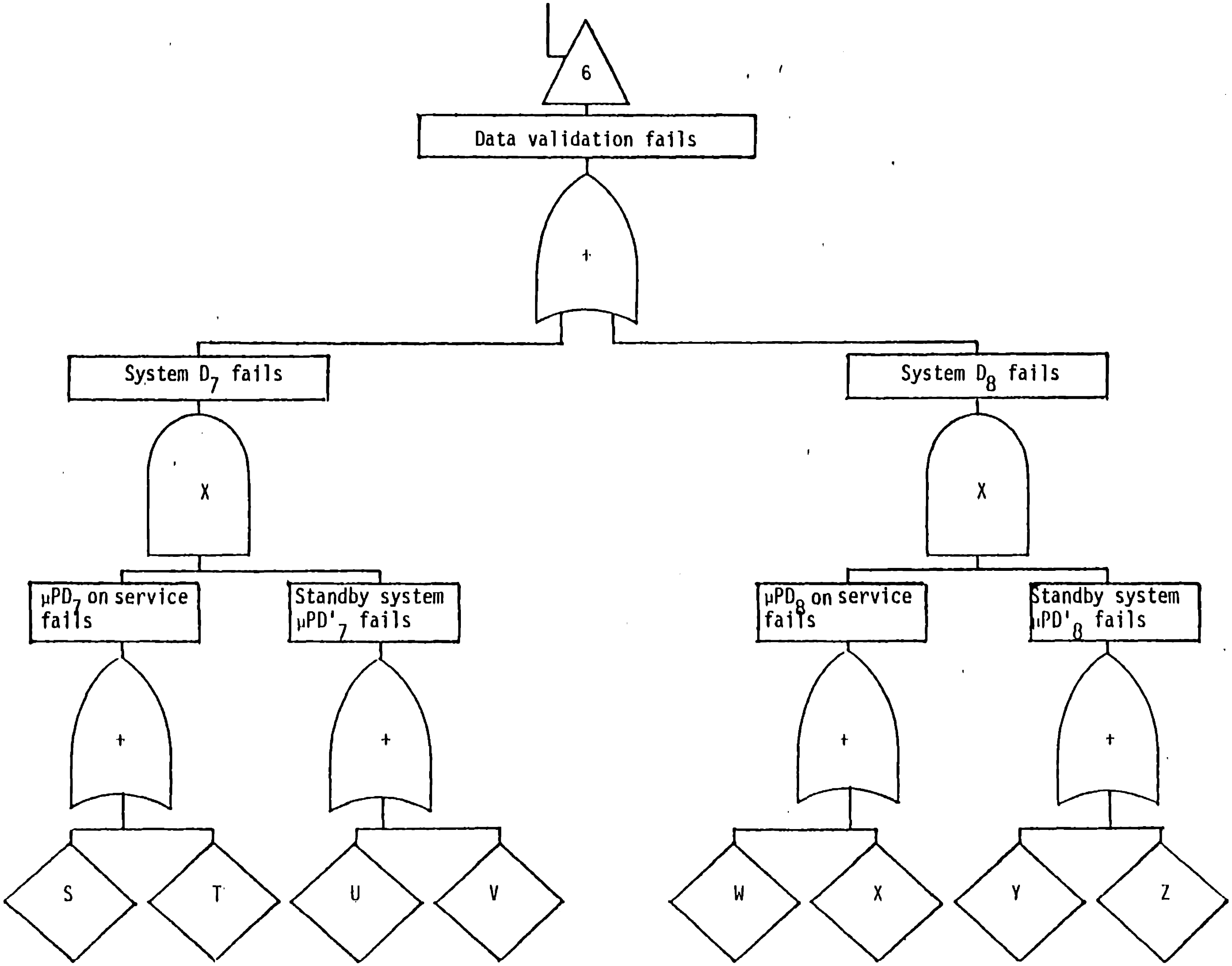


Figure D.9 (continued)

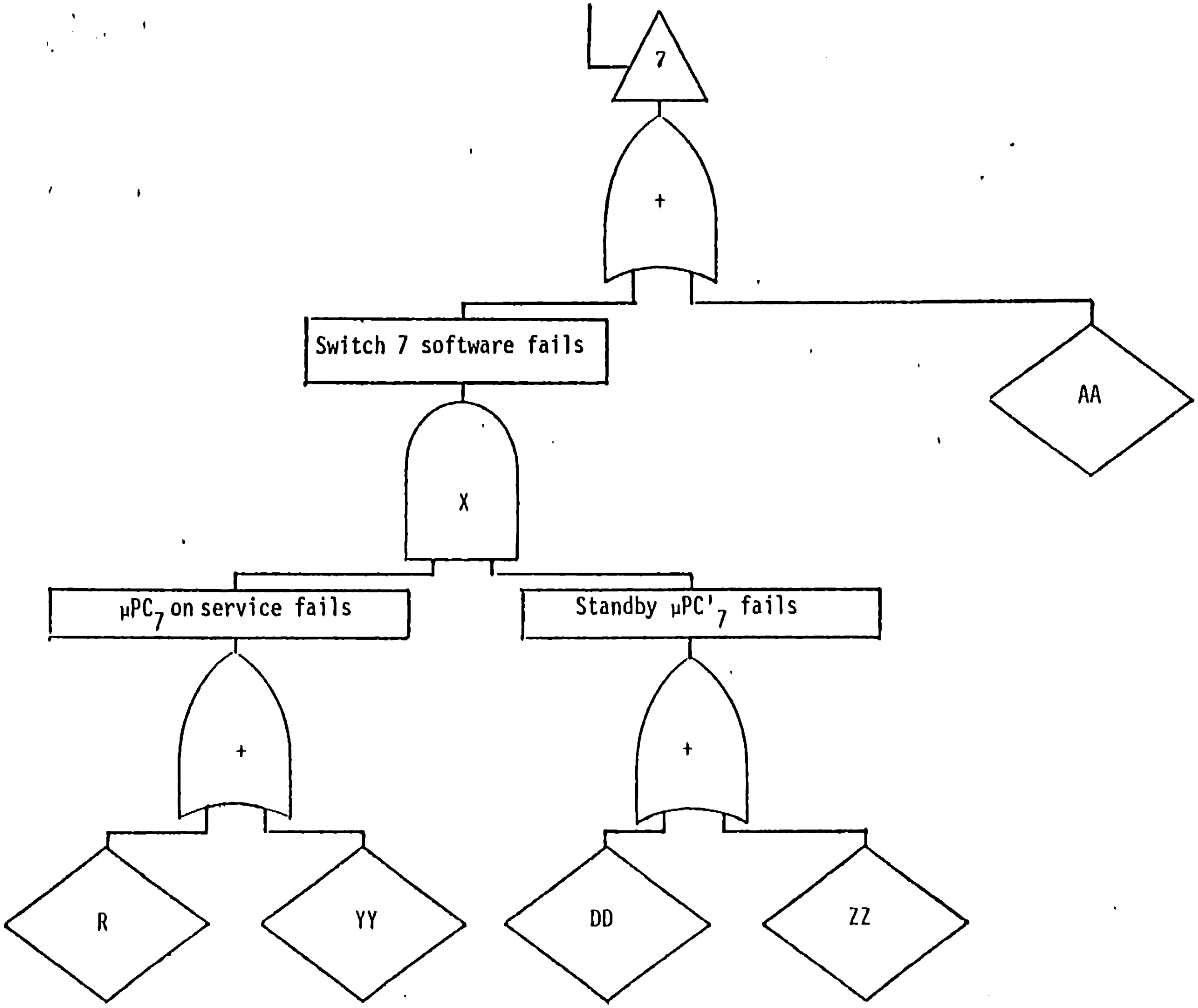


Figure D.9 (continued)

Table D.9

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
B	173.392	1.0	6.3	1.0	$1.092\text{x}10^3$	$1.731\text{x}10^{-5}$
C	435.629	1.0	6.3	1.0	$2.7445\text{x}10^3$	$6.374\text{x}10^{-2}$
D	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
E	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
F	106.837	1.0	6.3	1.0	673.07	$1.602\text{x}10^{-2}$
G	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
H	108.576	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$
I	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
J	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
K	108.76	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$
M	0.06	3.0	1.0	1.0	5.71	$1.3149\text{x}10^{-2}$
N	106.837	1.0	6.3	1.0	673.07	$1.602\text{x}10^{-2}$
O	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
L	.155	1.0	6.3	1.0	$9.765\text{x}10^{-1}$	$1.875\text{x}10^{-4}$
WW	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
XX	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
P	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
Q	106.837	1.0	6.3	1.0	673.07	$1.602\text{x}10^{-2}$
R	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
S	108.576	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$

Table D.9 (continued)

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
T	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
U	108.576	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$
V	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
W	108.576	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$
X	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
Y	108.576	1.0	6.3	1.0	685.16	$1.6309\text{x}10^{-2}$
Z	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
BB	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
CC	106.837	1.0	6.3	1.0	673.07	$1.602\text{x}10^{-2}$
DD	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
AA	.155	1.0	6.3	1.0	0.9763	$1.8747\text{x}10^{-4}$
YY	67.6125	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
ZZ	67.6125	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
FF	173.392	1.0	6.3	1.0	1092.00	$1.731\text{x}10^{-5}$
GG	435.629	1.0	6.3	1.0	2744.00	$6.374\text{x}10^{-2}$
HH	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
EE	142.3255	1.0	6.3	1.0	896.65	$2.129\text{x}10^{-2}$
AAA	221.965	1.0	6.3	1.0	1398.4	$3.3\text{x}10^{-2}$
BBB	221.965	1.0	6.3	1.0	1398.4	$3.3\text{x}10^{-2}$
II						$8.997\text{x}10^{-4}$
JJ						$8.997\text{x}10^{-4}$

Table D.9 (continued)

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
B	MMI 1	MMI 1 system fails
C	MC 1 hardware	MC 1 hardware fails
D	MC 1 software	MC 1 software fails
E	Cable	SO-C3 line fails
F	μPC3 hardware	μPC3 hardware fails
G	μPC3 software	μPC3 software fails
H	μPD3 hardware	μPD3 hardware fails
I	μPD3 software	μPD3 software fails
J	μPD'3 software	μPD'3 software fails
K	μPD'3 hardware	μPD'3 hardware fails
M	Cable	SO-C3' line fails
N	μPC'3 hardware	μPC'3 hardware fails
O	μPC'3 software	μPC'3 software fails
L	Switch 3	Switch 3 hardware fails
WW	μPC3 hardware (SR)	μPC3 hardware (SR) fails
XX	μPC3 hardware (SR)	μPC3' hardware (SR) fails
P	Cable	SO-C7 line fails
R	μPC7 hardware	μPC7 hardware fails
R	μPC7 software	μPC7 software fails
S	μPD7 hardware	μPD7 hardware fails
T	μPD7 software	μPD7 software fails
U	μPD'7 hardware	μPD'7 hardware fails
V	μPD'7 software	μPD'7 software fails
W	μPD8 hardware	μPD8 hardware fails
X	μPD8 software	μPD8 software fails
Y	μPD'8 hardware	μPD'8 hardware fails
Z	μPD'8 software	μPD8 software fails
BB	Cable	SO-C7' line fails
CC	μPC'7 hardware	μPC'7 hardware fails
DD	μPC'7 software	μPC'7 software fails
AA	Switch 7	Switch 7 fails
YY	μPC7 hardware	μPC7 hardware fails
ZZ	μPC'7 hardware	μPC'7 hardware fails
FF	MMI2	MMI2 fails
GG	MC 2 hardware	MC 2 hardware fails
HH	MC 2 software	MC 2 software fails
EE	Switch SO	Switch SO fails
AAA	MC 1 hardware	MC 1 hardware fails (SR)
BBB	MC 1 software	MC 1 software fails (SR)
II	Secondary storage 1	Secondary 1 storage fails
JJ	Secondary storage 2	Secondary 2 storage fails

Table D.9 (continued)

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

PROBABILISTIC EQUATIONS PARALLEL TRANSMISSION ALTERNATIVE (SITUATION ONE)

$$TE = < B + C + D + II + \{ E + F + G + [H + I] \times [J + K] \} \times \{ M + N + O + L$$

$$+ [G + WW] \times [O + XX] + [H + I] \times [J + K] \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ \} +$$

$$+ \{ P + R + Q + [S + T] \times [U + V] + [W + X] \times [Y + Z] \} > \times < BB + CC + DD$$

$$+ AA + [R + YY] \times [DD + ZZ] + [S + T] \times [U + V] + [W + X] \times [Y + Z]$$

$$\times \ FF + GG + HH + JJ + EE + [D + AAA] \times [HH + BBB] + \{ E + F + G +$$

$$+ [H + I] \times [J + K] \} \times \{ M + N + O + L + [G + WW] \times [O + XX] +$$

$$+ [H + I] \times [J + K] \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ P + Q + R + [S + T]$$

$$\times [U + V] + [W + X] \times [Y + Z] \} \times \{ BB + CC + DD + AA +$$

$$[R + YY] \times [DD + ZZ] + [S + T] \times [U + V] + [W + X] \times [Y + Z] \} >$$

Now making Boolean reductions:

$$TE = < B + C + D + II + \{ [H + J] \times [J + K] + [E + F + G] \times [M + N + O + L + (G + WW)$$

$$\times (O + XX)] + \{ \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ [S + T] \times [U + V] + [W + X]$$

$$\times [Y + Z] + [P + R + Q] \times [BB + CC + DD + AA + (R + YY) \times (DD + ZZ)] \} >$$

$$\times < FF + GG + HH + EE + JJ + [D + AAA] \times [HH + BBB] + \{ [H + I] \times$$

$$+ [J + K] + [E + F + G] \times [M + N + O + L + (G + WW) \times (O + XX)] \}$$

$$+ \{ \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ [S + T] \times [U + V] + [W + X]$$

$$\times [Y + Z] + [P + Q + R] \times [BBB + CC + DD + AA + (R + YY) X (DD + ZZ)] \} >$$

A further reduction follows:

$$TE = < \{ [H + I] \times [J + K] + [E + F + G] \times [M + N + O + L + (G + WW) \times (O + XX)] \}$$

$$+ \{ \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ [S + T] \times [U + V] + [W + X]$$

$$\times [Y + Z] + [P + R + Q] \times [BB + CC + DD + AA + (R + YY) \times (DD + ZZ)] \}$$

$$+ \{ [B + C + D + II] \times [JJ + FF + GG + HH + EE + (D + AAA) \times (HH + BBB)] \} :$$

Applying the probabilistics laws, the following implicit equations are obtained.

$TE = F_1 + F_2$ $\quad$ $p(TE) = p(F_1) + p(F_2) - p(F_1)p(F_2)$

$F_1 = F_3 + F_3$ $\quad$ $p(F_1) = 2p(F_3) - p(F_3)^2$

$F_3 = F_4 + F_4 + F_4$ $\quad$ $p(F_4) = 3p(F_4) + p(F_4)^3 - 3p(F_4)^2$

$F_4 = F_5 + F_6$ $\quad$ $p(F_4) = p(F_5) + p(F_6) - p(F_5)p(F_6)$

$F_5 = (H + I) x (J + K)$ $\quad$ $p(F_5) = [p(H) + p(I)] x [p(J) + p(K)]$

$F_6 = F_7 + F_8$ $\quad$ $p(F_6) = p(F_7) x p(F_8)$

$F_7 = E + F + G$ $\quad$ $p(F_7) = p(E) + p(F) + p(G)$

$F_8 = F_9 + F_{10}$ $\quad$ $p(F_8) = p(F_9) + p(F_{10}) - p(F_9)p(F_{10})$

$F_9 = M + N + O + L$ $\quad$ $p(F_9) = p(M) + p(N) + p(O) + p(L)$

$F_{10} = (G + WW) x (O + XX)$ $\quad$ $p(F_{10}) = [p(G) + p(WW)] X [p(O) + p(XX)]$

$F_2 = F_{11} + F_{12}$ $\quad$ $p(F_2) = p(F_{11}) + p(F_{12}) - p(F_{11})p(F_{12})$

$F_{11} = F_{13} + F_{14}$ $\quad$ $p(F_{11}) = p(F_{13}) + p(F_{14}) - p(F_{13})p(F_{14})$

$F_{13} = F_{15} + F_{16}$ $\quad$ $p(F_{13}) = p(F_{15}) + p(F_{16}) - p(F_{15})p(F_{16})$

$F_{15} = (S + T) x (U + V)$ $\quad$ $p(F_{15}) = [p(S) + p(T)] x [p(U) + p(V)]$

$F_{16} = (W + X) x (Y + Z)$ $\quad$ $p(F_{16}) = [p(W) + p(X)] x [p(Y) + p(Z)]$

$F_{14} = F_{17} x F_{18}$ $\quad$ $p(F_{14}) = p(F_{17}) x p(F_{18})$

$F_{18} = P + Q + R$ $\quad$ $p(F_{17}) = p(P) + p(Q) + p(R)$

$F_{19} = BB + CC + DD + AA$ $\quad$ $p(F_{19}) = p(BB) + p(CC) + p(DD) + p(AA)$

$F_{20} = (R + YY) x (D + ZZ)$ $\quad$ $p(F_{20}) = [p(R) + p(YY)] x [p(DD) + p(ZZ)]$

$F_{12} = F_{21} x F_{22}$ $\quad$ $p(F_{11}) = p(F_{21}) x p(F_{22})$

$F_{21} = F_{27} + F_{28}$ $\quad$ $p(F_{21}) = p(F_{27}) + p(F_{28}) - p(F_{27})p(F_{28})$

$F_{27} = C + D$ $\quad$ $p(F_{27}) = p(C) + p(D) - P(C)p(D)$

$F_{28} = B + II$ $\quad$ $p(F_{28}) = p(B) + p(II) - p(B)p(II)$

$F_{22} = F_{23} + F_{24}$ $\quad$ $p(F_{22}) = p(F_{23}) + p(F_{24}) - p(F_{23})p(F_{24})$

$$F_{23} = F_{25} + F_{26} \qquad p(F_{23}) = p(F_{25}) + p(F_{26}) - p(F_{25})p(F_{26})$$

$$F_{25} = FF + GG \qquad p(F_{25}) = p(FF) + p(GG) - p(FF)p(GG)$$

$$F_{26} = HH + EE + JJ \qquad p(F_{26}) = p(HH) + p(EE) + p(JJ) - p(EE)p(JJ)$$

$$F_{24} = (D + AAA) \times (HH + BBB) \qquad p(F_{24}) = [p(D) + p(AAA)] \times [p(HH) + p(BBB)]$$

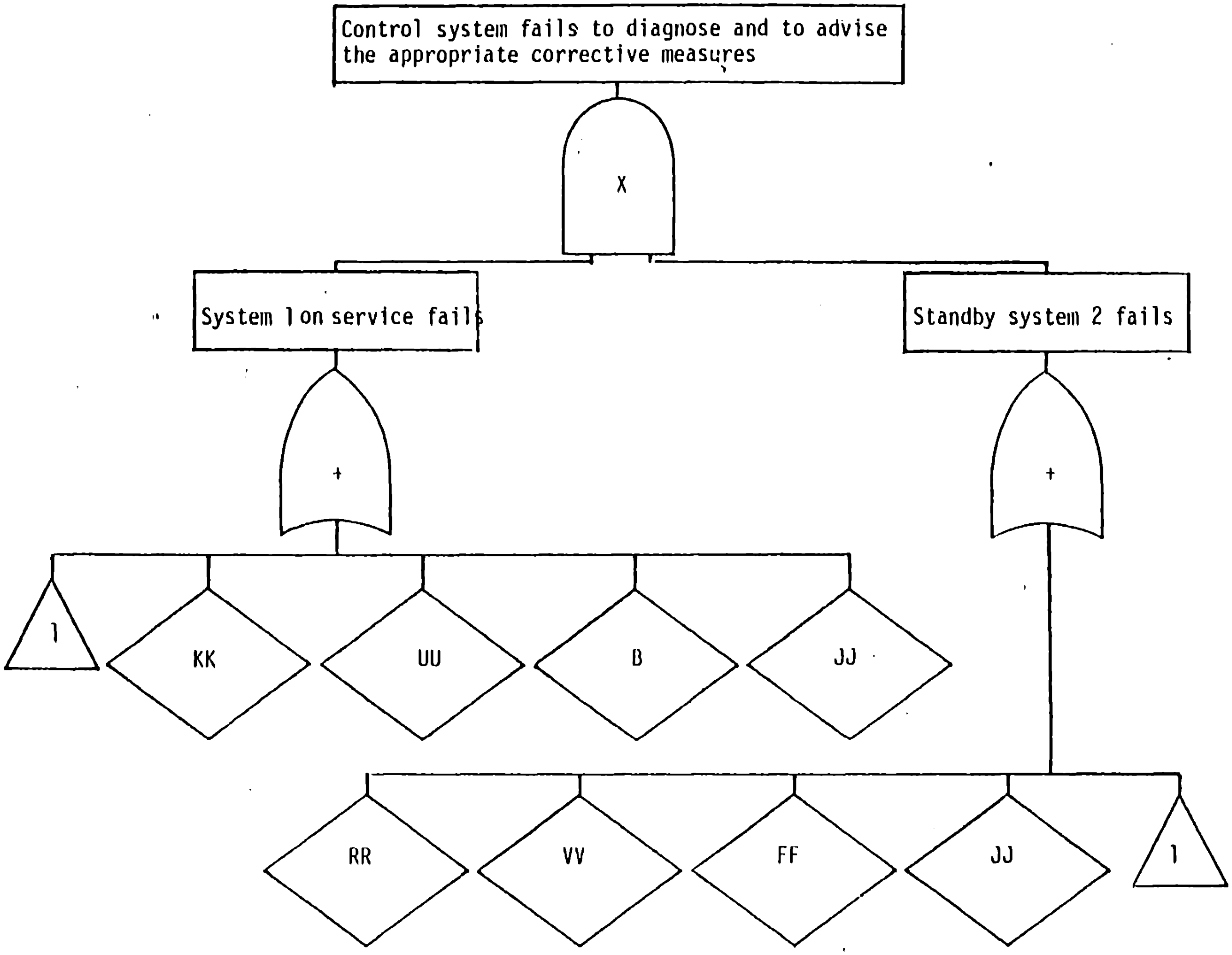

Control system fails to diagnose and to advise the appropriate corrective measures
X
System 1 on service fails
Standby system 2 fails
+
+
1
KK
UU
B
JJ
RR
VV
FF
JJ
1

Figure D.10 Dual star architecture, parallel transmission, situation two.

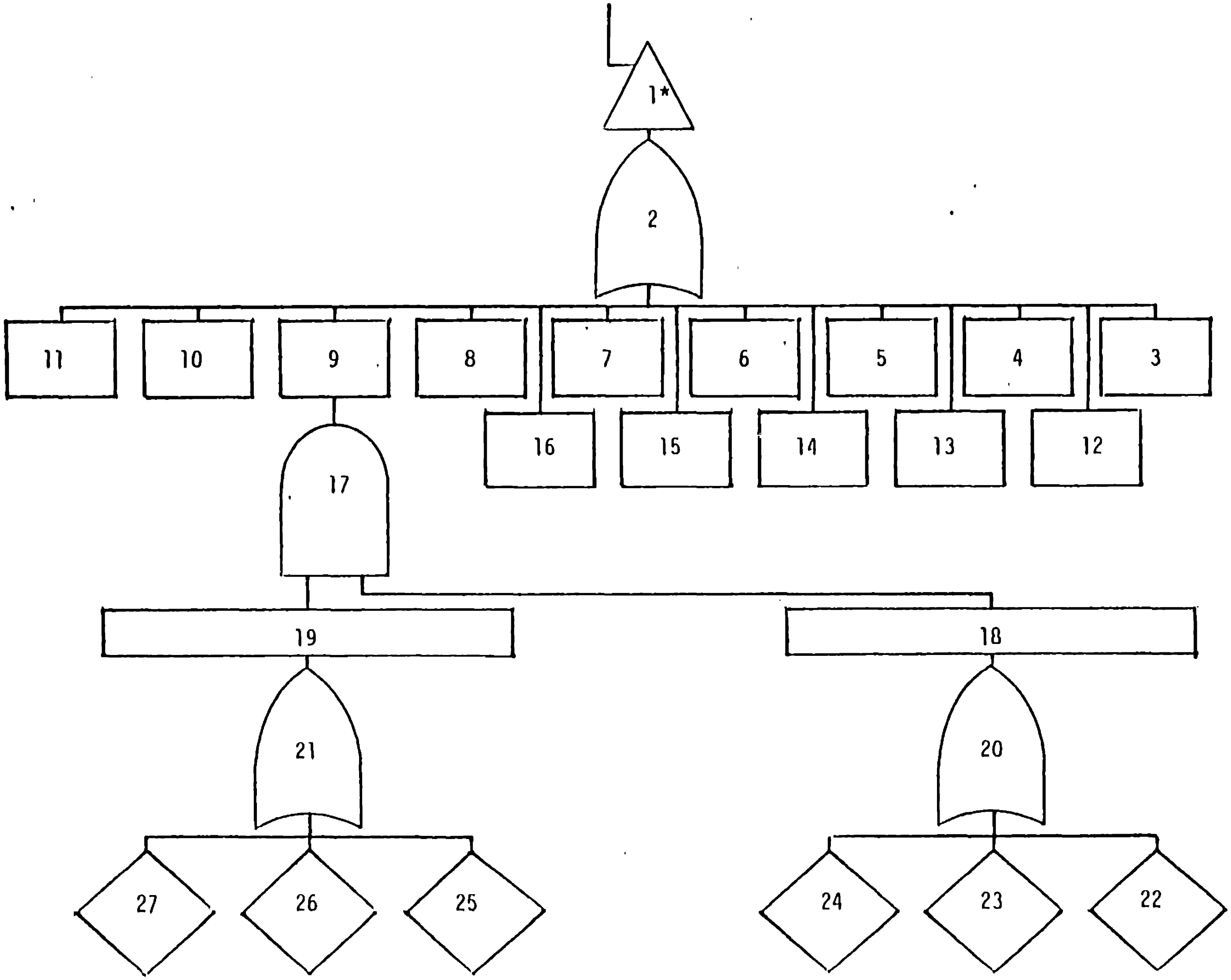


Figure D.10 (continued)
*See legend next page.

1. 1
2. +
3. System D_9 fails
4. System D_8 fails
5. System D_7 fails
6. System D_6 fails
7. System D_5 fails
8. System D_4 fails
9. System D_3 fails
10. System D_2 fails
11. System D_1 fails
12. System D_{14} fails
13. System D_{13} fails
14. System D_{12} fails
15. System D_{11} fails
16. System D_{10} Fails
17. X
18. Standby system D_3' fails
19. System D_3 on service fails
20. +
21. +
22. RQ
23. PP
24. TT
25. NN
26. MM
27. SS

Table D.10

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
II						8.997×10^{-4}
JJ						8.997×10^{-4}
VV	405.802	1.0	6.3	1.0	2556.55	5.591×10^{-2}
RR	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
SS	.06	3.0	1.0	1.0	.18	4.32×10^{-6}
MM	93.375	1.0	6.3	1.0	588.262	1.4019×10^{-2}
NN	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
TT	.06	3.0	1.0	1.0	.18	4.32×10^{-6}
PP	93.375	1.0	6.3	1.0	588.262	1.4019×10^{-2}
QQ	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
UU	405.802	1.0	6.3	1.0	2556.55	5.951×10^{-2}
KK	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
LL	0.06	3.0	1.0	1.0	.18	4.3210^{-6}
OO	0.06	3.0	1.0	1.0	.18	4.3210^{-6}
B	173.392	1.0	6.3	1.0	1092.00	1.731×10^{-5}
FF	173.392	1.0	6.3	1.0	1092.00	1.731×10^{-5}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
II	Secondary storage 1	Secondary storage 1 fails

Table D.10 (continued)

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
JJ	Secondary storage 2	Secondary storage 2 fails
VV	MC 2 hardware	MC 2 hardware fails
RR	MC 2 software	MC 2 diagnosis software fails
SS	Cable	D3-MC 2 line fails
MM	μPC3 hardware	μPD3 hardware fails
NN	μPD3 software	μPD3 software fails
TT	Cable	D3-MC 2 line fails
PP	μPD'3 hardware	μPD'3 hardware fails
QQ	μPD'3 software	μPC'3 software fails
UU	MC 1 hardware	MC 1 hardware fails
KK	MC 1 software	MC1 software fails
LL	Cable	D3-MC1 line fails
OO	Cable	D3'-MC1 line fails
B	MMI 1	MMI 1 fails
FF	MMI 2	MMI 2 fails

PROBABILISTIC EQUATIONS PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

From the corresponding fault tree:

$$\begin{aligned} TE = \Big\{ & B + II + UU + KK + [LL + MM + NN] \times [OO + PP + QQ] + [\ ] + [\ ] + \\ & + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + \\ & + [\ ] \Big\} \quad \times \Big\{ FF + JJ + VV + RR + [SS + MM + NN] \times [TT + PP + QQ] \\ & + [\ ]' + [\ ]' + [\ ]' + [\ ]' + [\ ]' + [\ ]' + [\ ]' + [\ ]' + [\ ]' \\ & + [\ ]' + [\ ]' + [\ ]' + [\ ]' \Big\} \end{aligned}$$

Table D.10 (continued)

DUAL STAR ARCHITECTURE PARALLEL TRANSMISSION ALTERNATIVE (SITUATION TWO)

Applying the probabilistics laws, the following implicit equations are obtained.

$TE = F_1 \times F_2$	$p(TE) = p(F_1) \times p(F_2)$
$F_1 = F_3 + F_4$	$p(F_1) = p(F_3) + p(F_4) - p(F_3)p(F_4)$
$F_3 = F_{19} + F_{20}$	$p(F_3) = p(F_{19}) + p(F_{20}) - p(F_{19})p(F_{20})$
$F_{19} = B + II$	$p(F_{19}) = p(B) + p(II) - p(B)p(II)$
$F_{20} = UU + KK$	$p(F_{20}) = p(UU) + p(KK) - p(UU)p(KK)$
$F_4 = F_5 + F_5$	$p(F_4) = 2p(F_5) - p(F_5)^2$
$F_5 = F_6 + F_7$	$p(F_5) = p(F_6) + p(F_7) - p(F_6)p(F_7)$
$F_6 = F_{15} + F_{15}$	$p(F_6\ ) = 2p(F_{15}) - p(F_{15})^2$
$F_{15} = F_8 + F_8$	$p(F_{15}) = 2p(F_8) - p(F_8)^2$
$F_7 = F_8 + F_8 + F_8$	$p(F_7) = 3p(F_8) + p(F_8)^3 - 3p(F_8)^2$
$F_8 = (LL+MM+NN) \times (OO+ PP+QQ)$	$p(F_8) = [p(LL) + p(MM) + p(NN)]$
	$\times [p(OO) + p(PP) + p(QQ)]$
$F_2 = F_9 + F_{10}$	$p(F_2) = p(F_9) + p(F_{10}) - p(F_9)p(F_{10})$
$F_9 = F_{17} + F_{18}$	$p(F_9) = p(F_{17}) + p(F_{18}) - p(F_{17})p(F_{18})$
$F_{17} = VV + RR$	$p(F_{17}) = p(VV) + p(RR) - p(VV)p(RR)$
$F_{18} = FF + JJ$	$p(F_{18}) = p(FF) + p(JJ) - p(JJ)p(FF)$
$F_{10} = F_{11} + F_{11}$	$p(F_{10}) = 2p(F_{11}) - p(F_{11})^2$
$F_{11} = F_{12} + F_{13}$	$p(F_{11}) = p(F_{12}) + p(F_{13}) - p(F_{12})p(F_{13})$
$F_{12} = F_{14} + F_{14}$	$p(F_{12}) = 2p(F_{14}) - p(F_{14})^2$
$F_{14} = F_{16} + F_{16}$	$p(F_{14}) = 2p(F_{16}) - p(F_{16})^2$

$$F_{13} = F_{16} + F_{16} + F_{16} \qquad p(F_{13}) = 3p(F_{16})^3 - p(F_{16})^2$$

$$F_{16} = (SS+MM+NN) \times (TT+PP+QQ) \qquad p(F_{16}) = [p(SS) + p(MM) + p(NN)] \times$$

$$[p(TT) + p(PP) + p(QQ)]$$

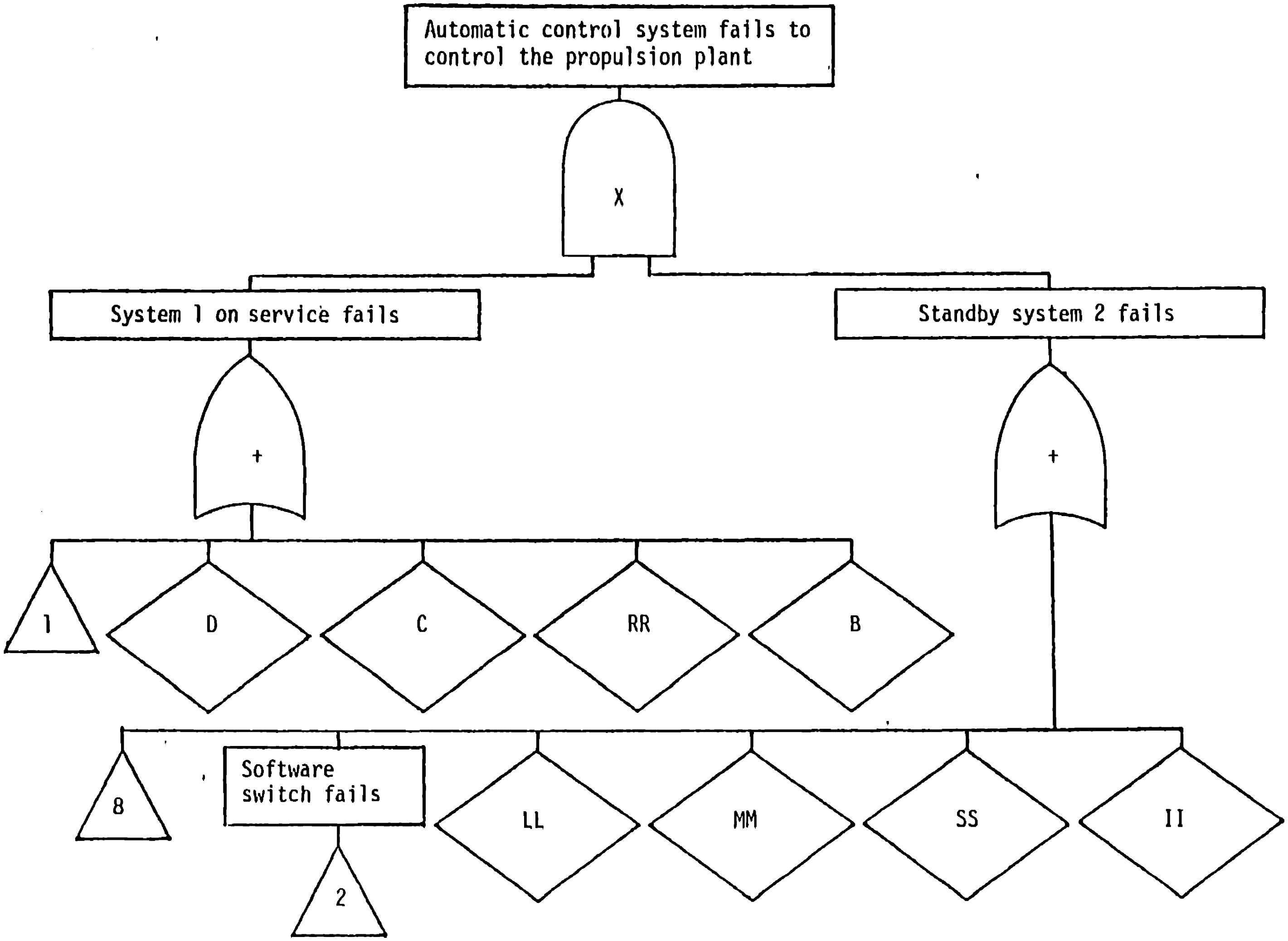

Automatic control system fails to control the propulsion plant
X
System 1 on service fails
Standby system 2 fails
+
+
1
D
C
RR
B
8
Software switch fails
2
LL
MM
SS
II

Figure D.11 Dual star architecture, serial transmission alternative, situation one.

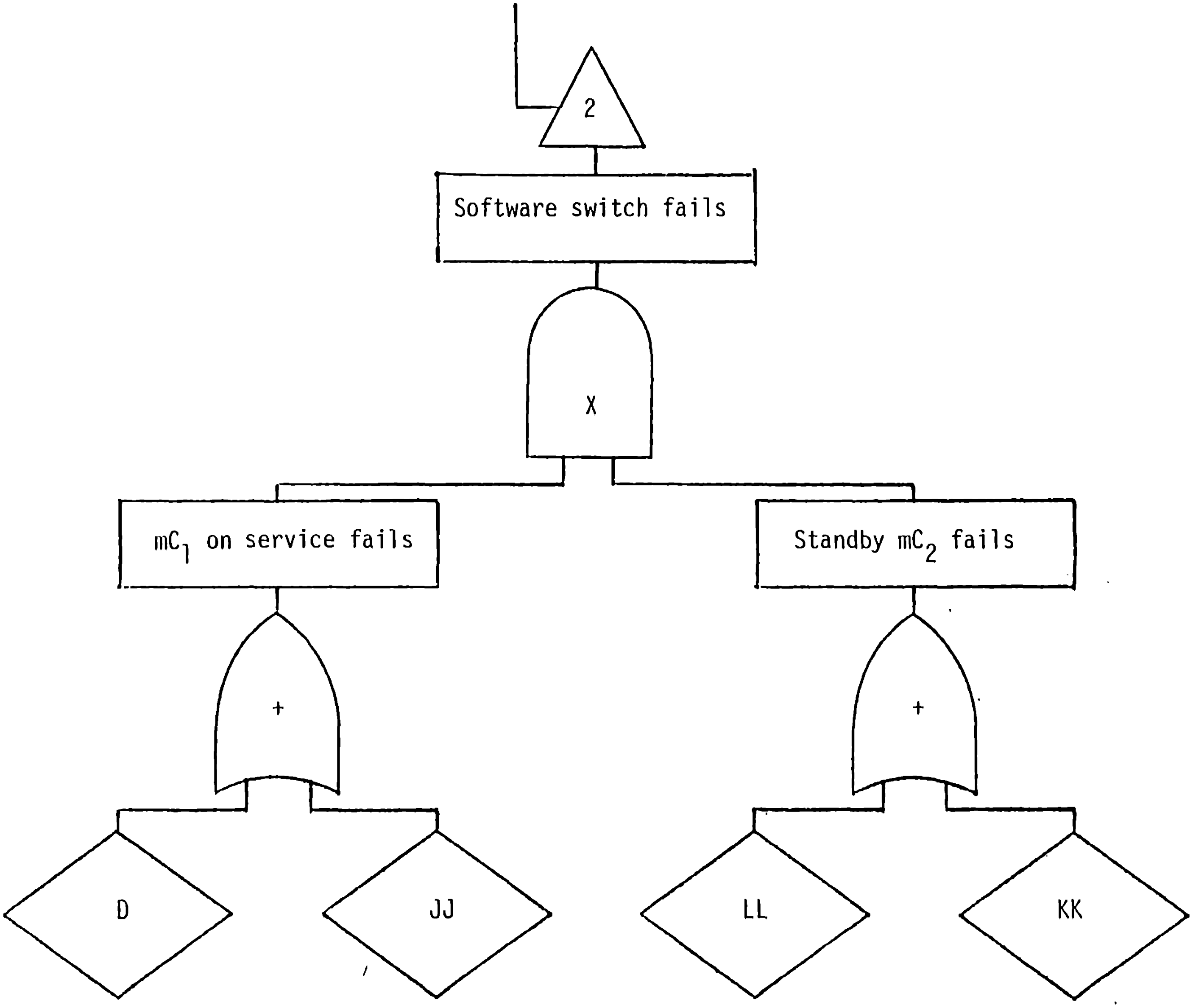


Figure D.11 (continued)

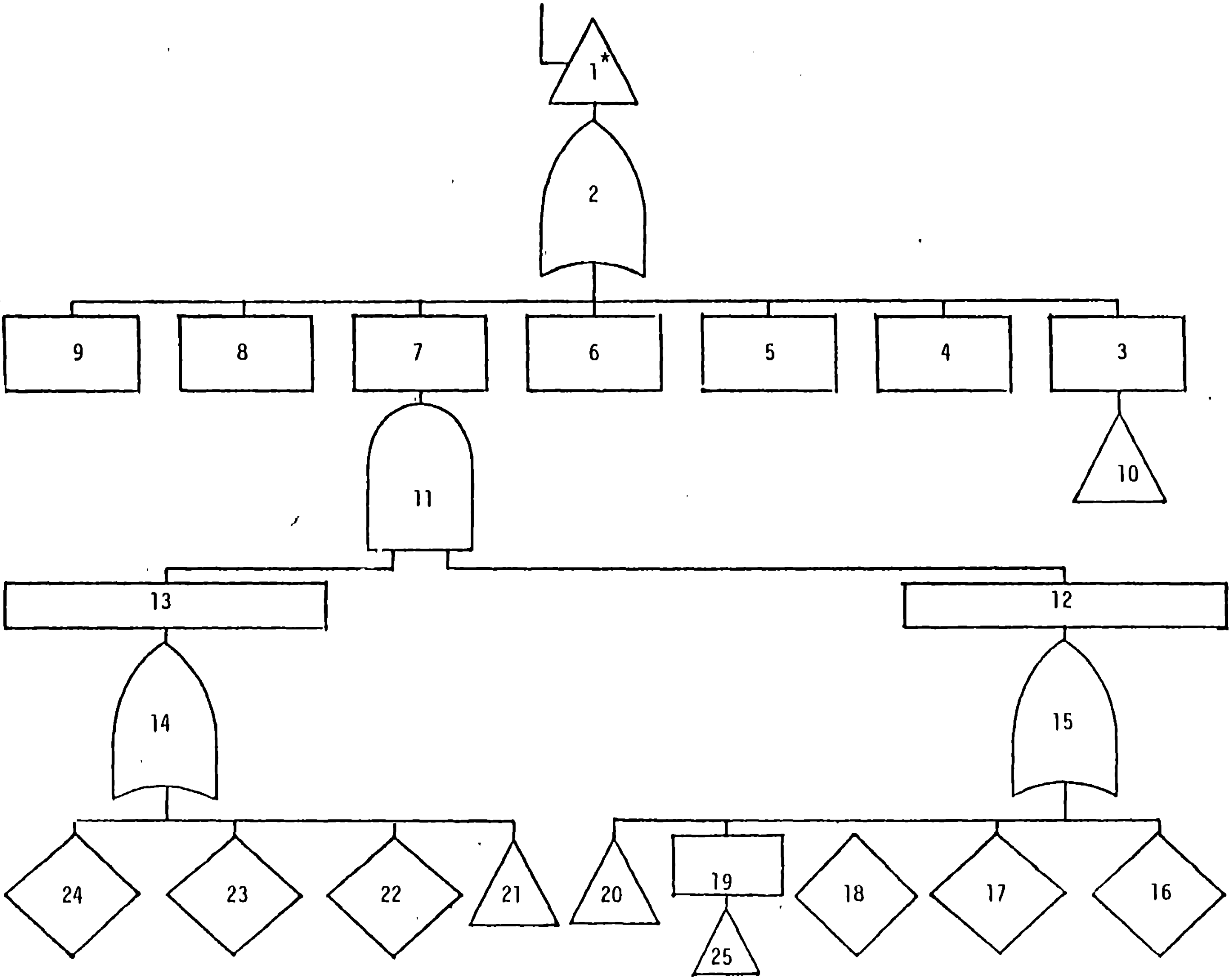


Figure D.11 (continued)
* See legend on next page.

1. 1
2. +
3. Distributed system 7 fails
4. Distributed system 6 fails
5. Distributed system 5 fails
6. Distributed system 4 fails
7. Distributed system 3 fails
8. Distributed system 2 fails
9. Distributed system 1 fails
10. 3
11. X
12. Standby system 3' fails
13. System 3 on service fails
14. +
15. +
16. N
17. M
18. L
19. Switch 3 fails
20. 4
21. 4
22. G
23. F
24. E
25. 5

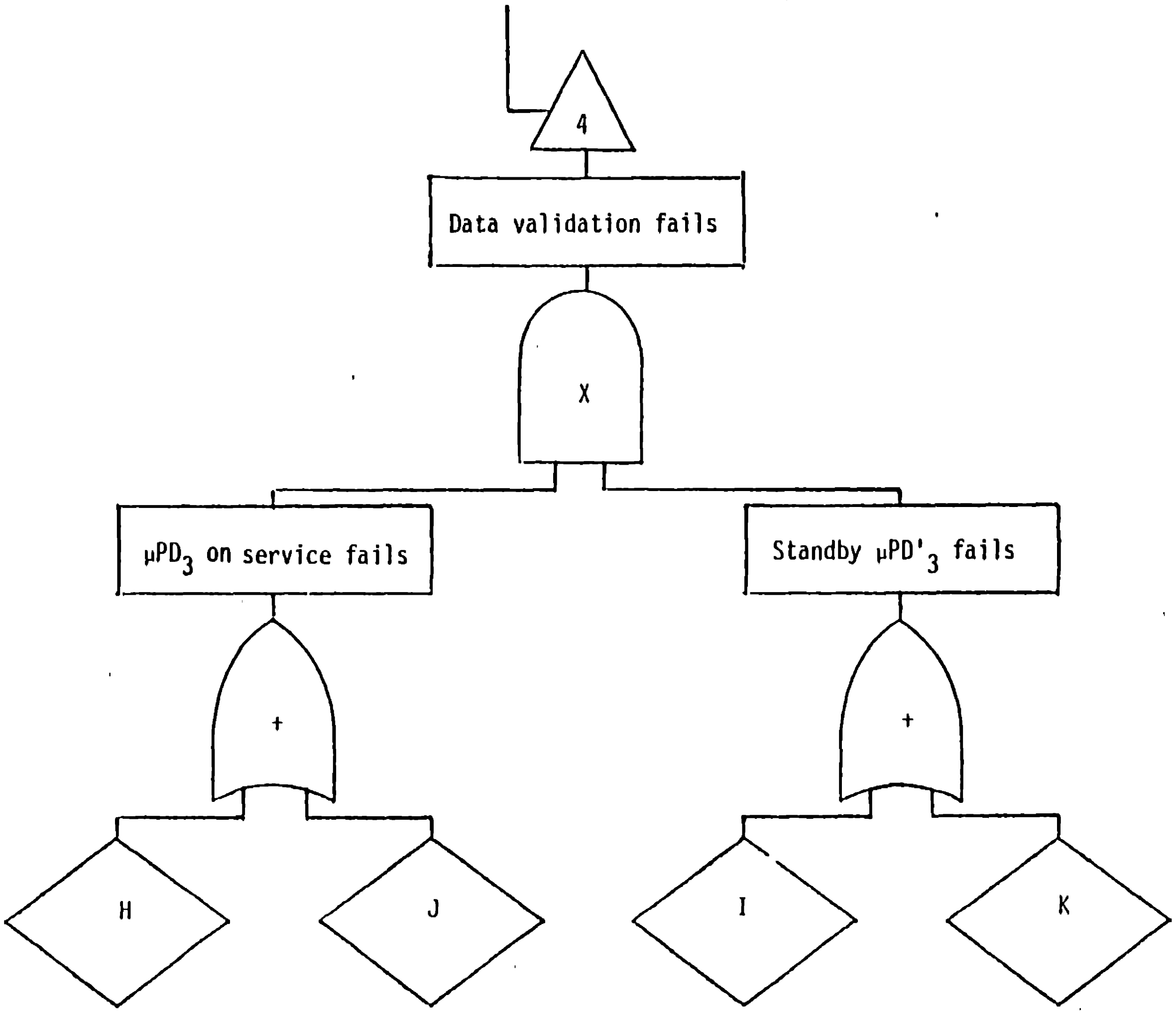


Figure D.11 (continued)

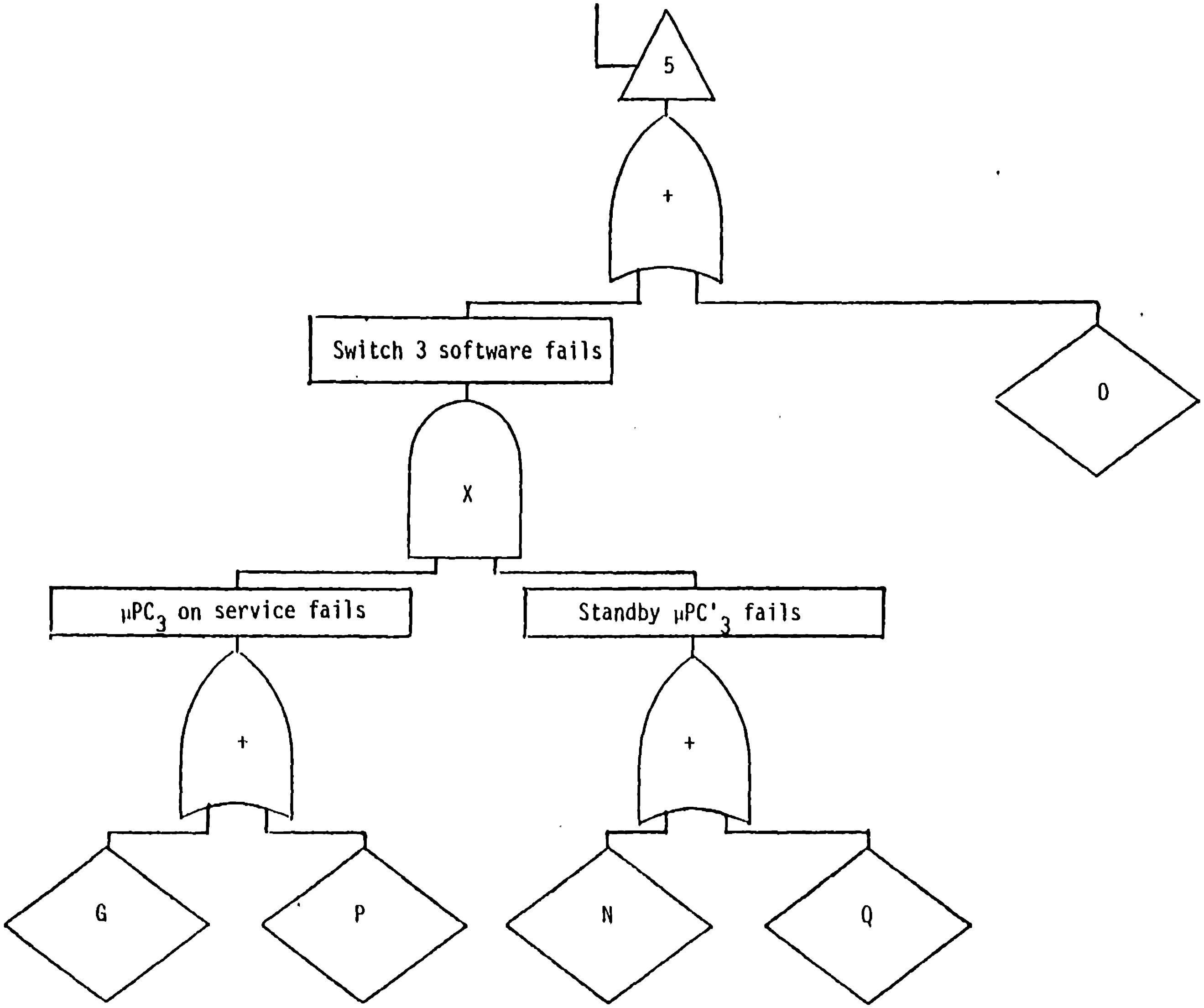


Figure D.11 (continued)

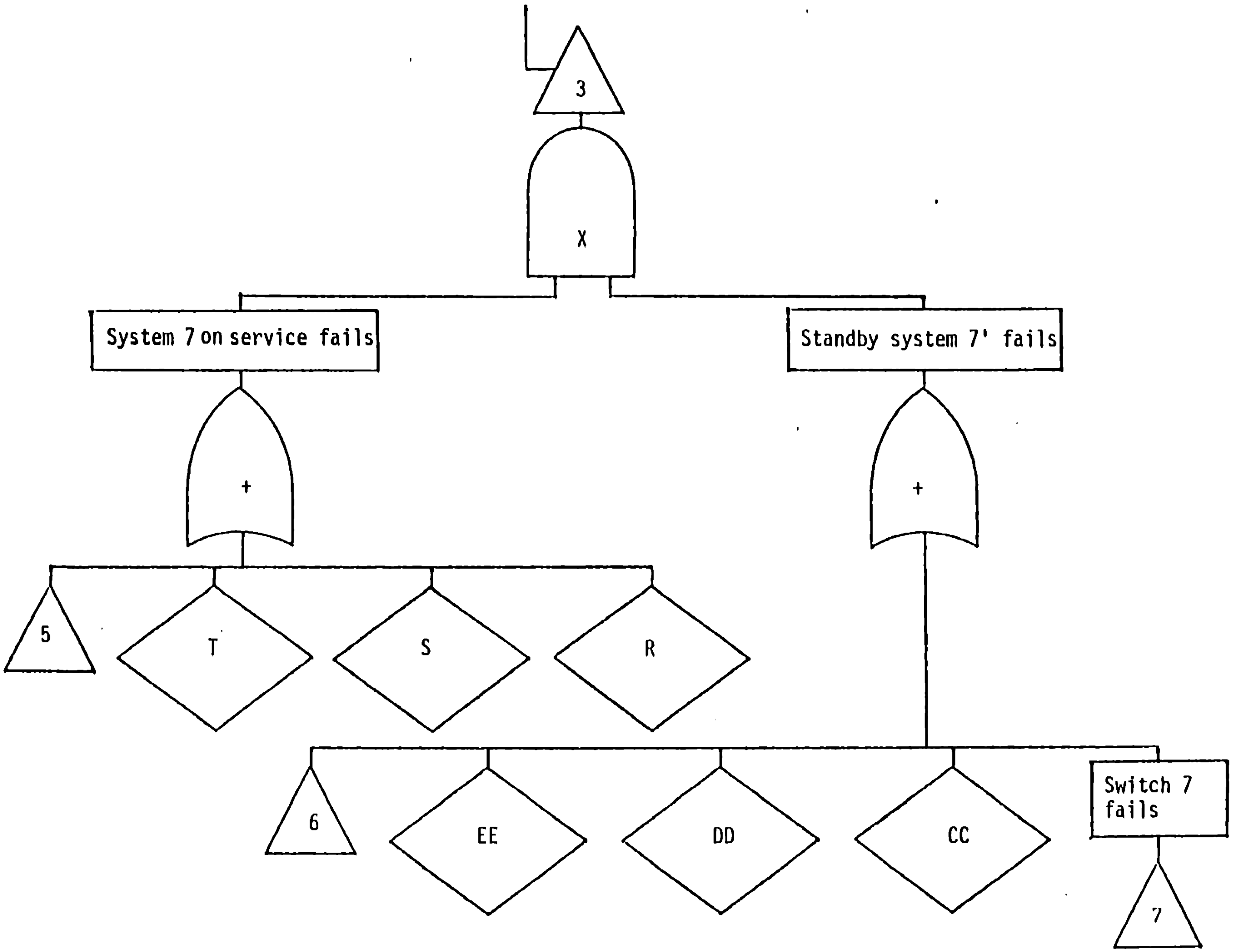


Figure D.11 (continued)

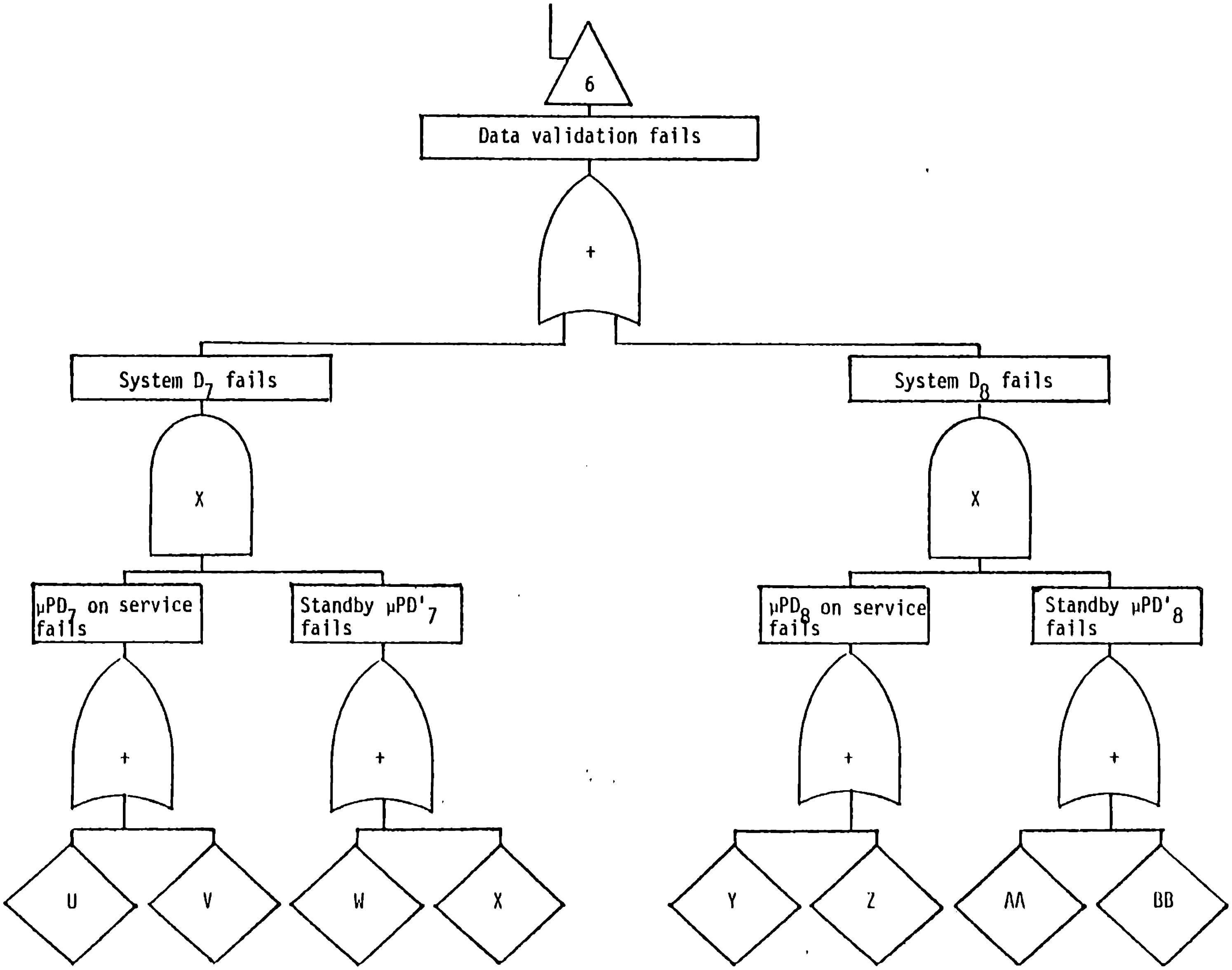

6
Data validation fails
+
System D_7 fails
System D_8 fails
X
X
μPD_7 on service fails
Standby $\mu PD'_7$ fails
μPD_8 on service fails
Standby $\mu PD'_8$ fails
+
+
+
+
U
V
W
X
Y
Z
AA
BB

Figure D.11 (continued)

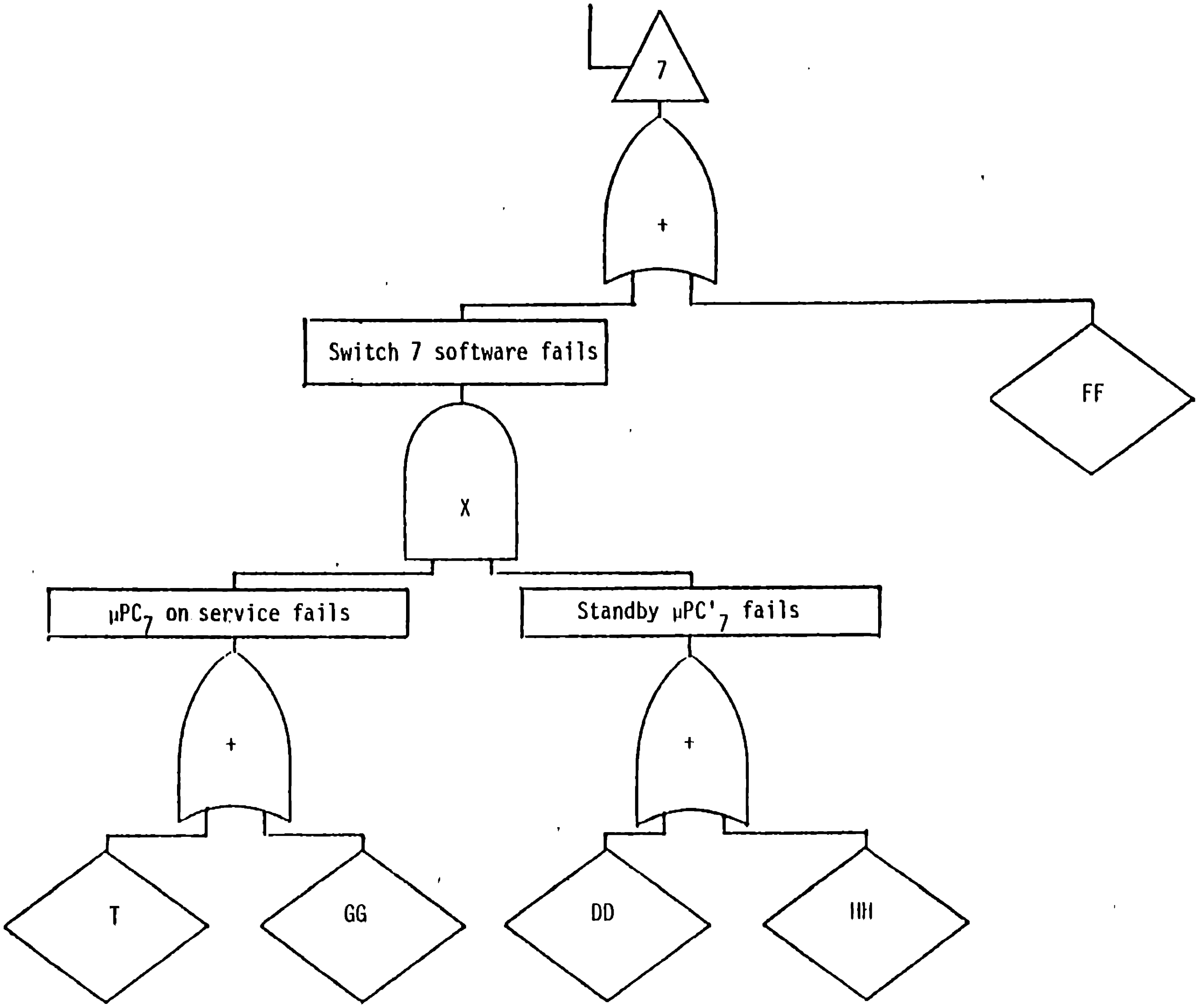


Figure D.11 (continued)

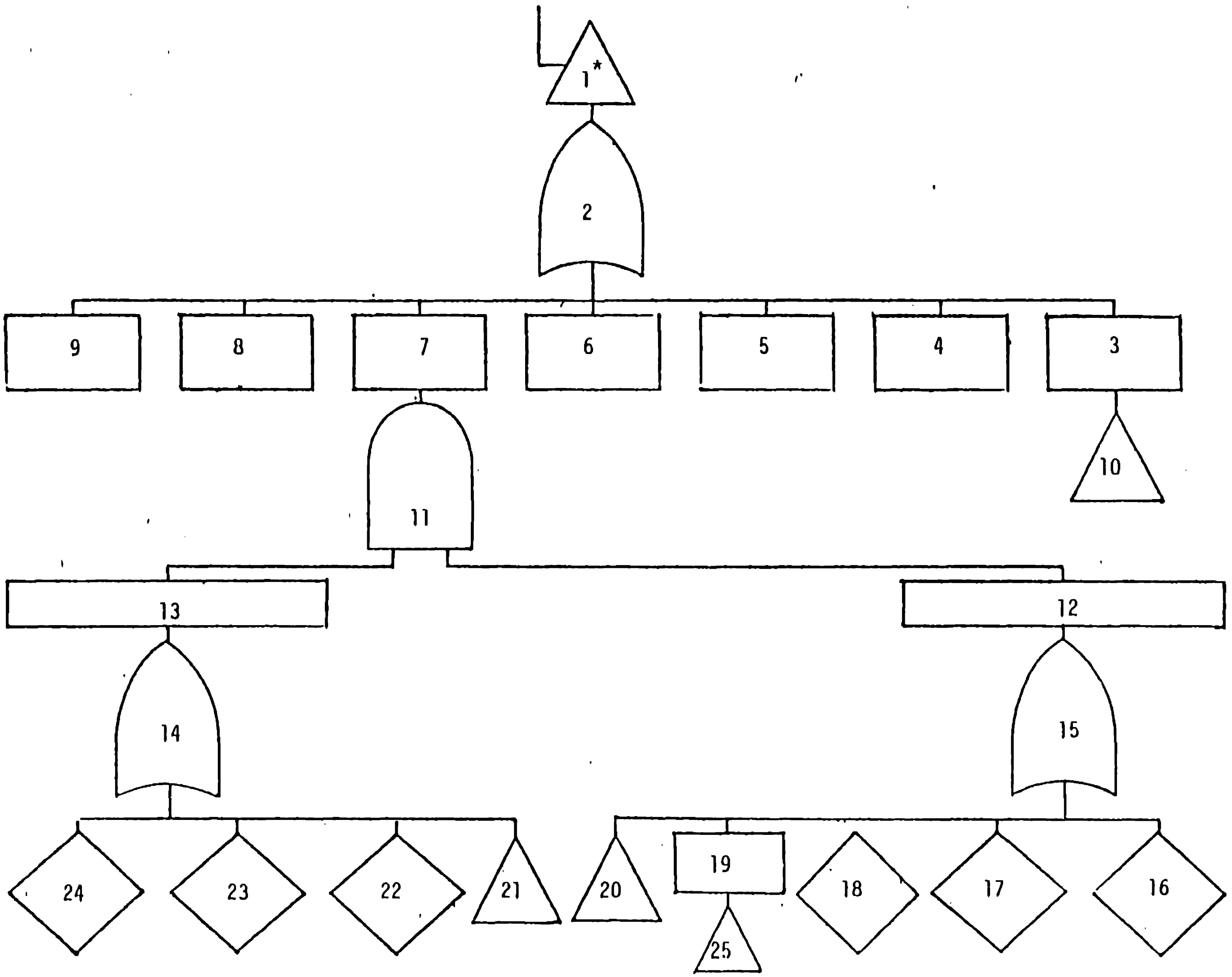


Figure D.11 (continued)
*See legend on next page.

1. 8
2. +
3. Distributed system 7 fails
4. Distributed system 6 fails
5. Distributed system 5 fails
6. Distributed system 4 fails
7. Distributed system 3 fails
8. Distributed system 2 fails
9. Distributed system 1 fails
10. 9
11. X
12. Standby system 3 fails
13. System 3 onservice fails
14. +
15. +
16. OO
17. M
18. N
19. Switch 3 fails
20. 4
21. 4
22. NN
23. F
24. G
25. 5

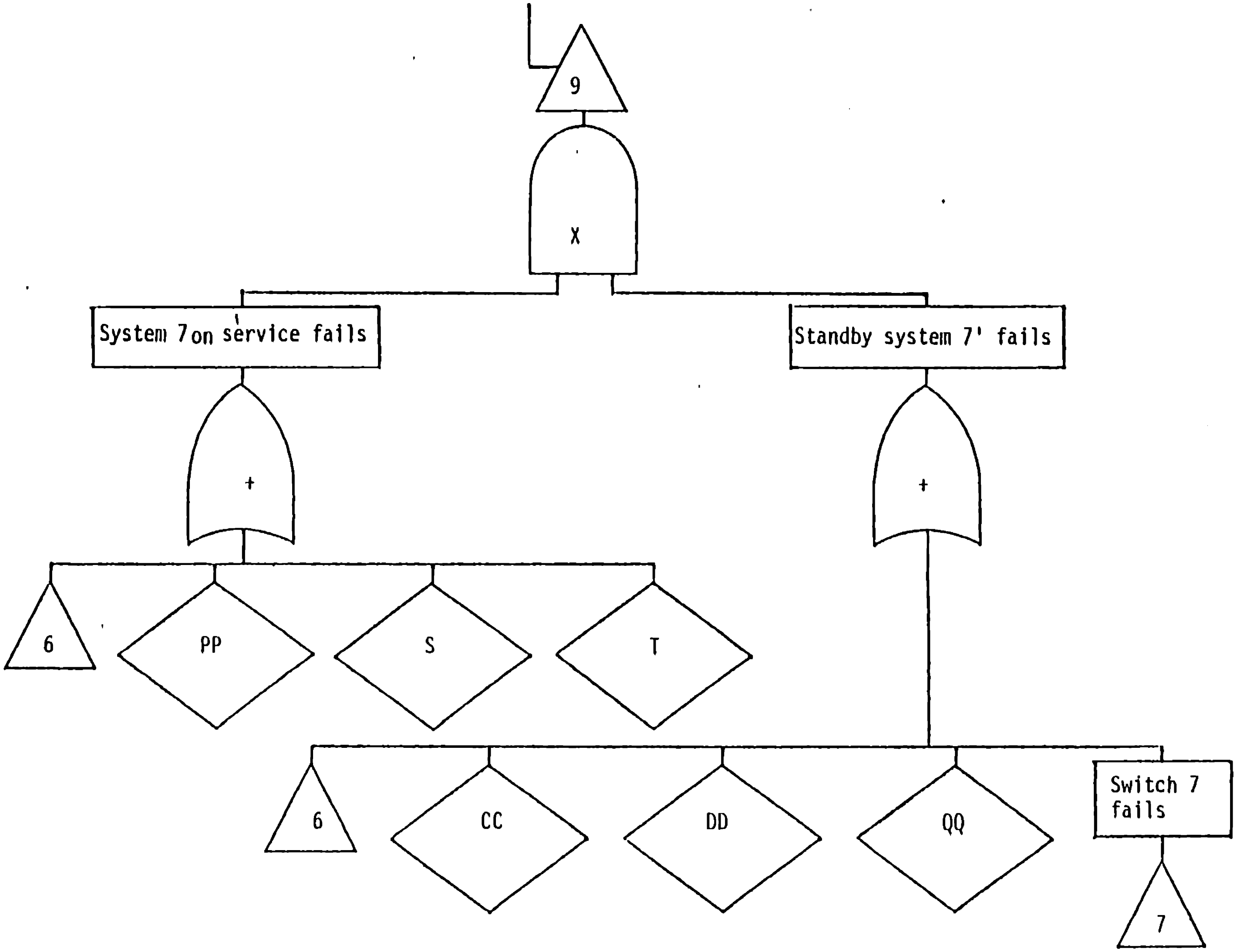


Figure D.11 (continued)

Table D.11

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (CONDITION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^{6}h)	π_Q	π_E	π_L	(F/10^{6}h)	
B	173.392	1.0	6.3	1.0	1.092x10^{3}	1.731x10^{-5}
C	352.6944	1.0	6.3	1.0	2.222x10^{3}	5.193x10^{-2}
D	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
E	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
F	110.503	1.0	6.3	1.0	696.169	1.657x10^{-2}
G	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
H	104.731	1.0	6.3	1.0	659.801	1.571x10^{-2}
I	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
J	104.731	1.0	6.3	1.0	659.801	1.571x10^{-2}
K	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
L	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
M	110.503	1.0	6.3	1.0	696.169	1.657x10^{-2}
N	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
O	.155	1.0	6.3	1.0	9.765x10^{-1}	1.8747x10^{-4}
P	67.6105	1.0	6.3	1.0	425.95	1.017x10^{-2}
Q	67.6105	1.0	6.3	1.0	425.95	1.017x10^{-2}
P	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
S	110.503	1.0	6.3	1.0	696.169	1.657x10^{-2}
T	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
U	104.731	1.0	6.3	1.0	659.8	1.571x10^{-2}

Table D.11 (continued)

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (CONDITION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
V	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
W	104.731	1.0	6.3	1.0	659.8	$1.571\text{x}10^{-2}$
X	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
Y	104.731	1.0	6.3	1.0	659.8	$1.571\text{x}10^{-2}$
Z	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
AA	104.731	1.0	6.3	1.0	659.8	$1.571\text{x}10^{-2}$
BB	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
CC	110.503	1.0	6.3	1.0	696.169	$1.657\text{x}10^{-2}$
DD	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
EE	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
FF	.155	1.0	6.3	1.0	.9765	$1.8747\text{x}10^{-4}$
GG	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
HH	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
II	173.392	1.0	6.3	1.0	1092.00	$1.731\text{x}10^{-5}$
JJ	352.6944	1.0	6.3	1.0	2222.00	$5.193\text{x}10^{-2}$
KK	352.6944	1.0	6.3	1.0	2222.00	$5.193\text{x}10^{-2}$
LL	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
MM	352.6944	1.0	6.3	1.0	2222.00	$5.193\text{x}10^{-2}$
NN	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$

Table D.11 (continued)

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (CONDITION ONE)

OO	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
PP	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
QQ	.06	3.0	1.0	1.0	.18	4.32x10^{-6}
RR						8.997x10^{-4}
SS					.18	8.997x10^{-4}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
B	MMI 1	MMI 1 system fails
C	MC 1 hardware	MC 1 hardware fails
D	MC 1 control software	MC 1 control software fails
E	Cable	C3-MC 1 line fails
F	μPC3 hardware	μPC3 hardware fails
G	μPC3 software	μPC3 software fails
H	μPD3 hardware	μPD3 hardware fails
I	μPD3 software	μPD3 software fails
J	μPD'3 hardware	μPD'3 hardware fails
K	μPD'3 software	μPD'3 software fails
L	Cable	C3-MC 1 line fails
M	μPC'3 hardware	μPC'3 hardware fails
N	μPC'3 software	μPC'3 software fails
O	Switch 3	Switch 3 hardware fails
P	μPC3 hardware (SR)	μPC3 hardware fails (SR)
Q	μPC'3 hardware (SR)	μPC'3 hardware fails (SR)
R	Cable	C7-MC line fails
S	μPC7 hardware	μPC7 hardware fails
T	μPC7 software	μPC7 software fails
U	μPD7 hardware	μPD7 hardware fails
V	μPD7 software	μPD7 software fails
W	μPD'7 hardware	μPD'7 hardware fails
X	μPD'7 software	μPD'7 software fails
Y	μPD8 hardware	μPD8 hardware fails
Z	μPD8 software	μPD8 software fails
AA	μPD'8 hardware	μPD'8 hardware fails
BB	μPD'8 software	μPD'8 software fails
CC	μPC'7 hardware	μPC'7 hardware fails
DD	μPC'7 software	μPC'7 software fails

Table D.11 (continued)

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (CONDITION ONE)

EE	Cable	C'7-MC 1 line fails
FF	Switch 7	Switch 7 hardware fails
GG	μPC7 hardware	μPC7 hardware (SR) fails
HH	μPC7 hardware	μPC7 hardware (SR) fails
II	MMI 2	MMI 2 system fails
JJ	MC 1 hardware	MC 1 hardware fails (SR)
KK	MC 2 hardware	MC 2 hardware fails (SR)
LL	MC 2 software	MC 2 software fails
MM	MC 2 hardware	MC 2 hardware fails
NN	Cable	MC2-C3 line fails
OO	Cable	MC2-C3' line fails
PP	Cable	MC2-C7 line fails
QQ	Cable	MC2-C7' line fails
RR	Secondary storage 1	Secondary storage 1 fails
SS	Secondary storage 2	Secondary storage 2 fails

DUAL STAR ARCHITECTURE

PROBABILISTIC EQUATIONS SERIAL TRANSMISSION ALTERNATIVE (SITUATION ONE)

From the corresponding fault tree:

$$TE = < B + C + D + RR + \{ E + F + G + [H + I] \times [J + K] \} \times \{ L + M + N + O$$

$$+ [G + P] \times (N + Q] + [H + J] \times [J + K] \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ \}$$

$$+ \{ R + S + T + [U + V] \times [W + X] + [Y + Z] \times [AA + BB] \} \times \{ CC +$$

$$+ DD + EE + FF + [T + GG] \times [DD + HH] + [U + V] \times [W + X] + [Y + Z]$$

$$\times [AA + BB] \} > \times < [D + JJ] \times [LL + KK] + II + MM + LL + SS +$$

$$+ \{ NN + F + G + [H + I] \times [J + K] \} \times \{ OO + M + N + O + [G + P] \times$$

$$\times [N + Q] + [H + I] \times [J + K] \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ \} + \{ PP +$$

$$+ S + T + [U + V] \times [W + X] + [Y + Z] \times [AA + BB] \} \times \{ CC + DD + QQ$$

$$+ FF + [T + GG] \times [DD + HH] + [U + V] \times [W + X] + [Y + Z] \times$$

$$+ [AA + BB] \} >$$

Reducing the equations by Boolean laws:

$$TE = < B + C + D + RR + \{ [H + I] \times [J + K] + [E + F + G] \times [L + M + N +$$

+ O + (G + P) x (N + Q)]} + { } + { } + { } + { } + { }
+ { [U + V] + [W + X] + [Y + Z] x [AA + BB] + [R + S + T] x [CC
+ DD + EE + FF + (T + GG) x (DD + HH)]}> + < [D + JJ] x [LL + KK]
+ II + MM + LL + SS + {[H + I] x [J + K] + [NN + F + G] + [OO +
+ M + N + O + (G + P) x (N + Q)]} + { } + { } + { } + { } + { } +
{[U + V] x [W + X] +[Y + Z] x [AA + BB] + [PP + S + T] x
[CC + DD + QQ + FF + (T + GG) x (DD + HH)]}>

Applying the probabilistic laws:

$TE = F_1$	$p(TE) = p(F_1)$
$F_1 = F_2 + F_3$	$p(F_1) = p(F_2) + p(F_3)$
$F_2 = F_{35} + F_6$	$p(F_2) = p(F_{35}) + p(F_6) - p(F_{35})p(F_6)$
$F_{35} = F_4 + F_5$	$p(F_{35}) = p(F_4) + p(F_5) - p(F_4)p(F_5)$
$F_4 = F_{33} + F_{34}$	$p(F_4) = p(F_{33}) + p(F_{34}) - p(F_{33})p(F_{34})$
$F_{33} = B + C$	$p(F_{33}) = p(B) + p(C) - p(B)p(C)$
$F_{34} = D + RR$	$p(F_{34}) = p(D) + p(RR)$
$F_5 = F_7 + F_7$	$p(F_5) = 2p(F_7) - p(F_7)^2$
$F_7 = F_8 + F_8 + F_8$	$p(F_7) = 3p(F_8) + p(F_8)^3 - 3p(F_8)^2$
$F_8 = F_{11} + F_{12}$	$p(F_8) = p(F_{11}) + p(F_{12}) - p(F_{11})p(F_{12})$
$F_{11} = [H + I] \times [J + K]$	$p(F_{11}) = [p(H) + p(I)] \times [p(J) + p(K)$
$F_{12} = (E + F + G) \times F_{13}$	$p(F_{12}) = [p(E)+p(F)+p(G)] \times p(F_{13})$
$F_{13} = F_{14} + F_{15}$	$p(F_{13}) = p(F_{14}) + p(F_{15}) - p(F_{14})p(F_{15})$
$F_{14} = L + M + N + 0$	$p(F_{14}) = p(L) + p(M) + p(M) + p(N) + p(0)$
$F_{15} = (G + P) \times (N + 0)$	$p(F_{15}) = p(G) + p(P)] \times [p(N) + p(0)]$
$F_6 = F_{16} + F_{17} + F_{18}$	$p(F_6) = p(F_{16}) + p(F_{17}) + p(F_{18})$

$$+ p(F_{16})p(F_{17})p(F_{18}) - p(F_{16})p(F_{17})$$
$$- p(F_{16})p(F_{18}) - p(F_{17})p(F_{18})$$

$F_{16} = (U + V) \times (W + X)$ $\qquad$ $p(F_{16}) = [p(U) + p(V)] + [p(W) + p(X)]$

$F_{17} = (Y + Z) \times (AA + BB)$ $\qquad$ $p(F_{17}) = [p(Y) + p(Z)] \times [p(AA) + p(BB)]$

$F_{18} = (R + S + T) + F_{19}$ $\qquad$ $p(F_{18}) = [p(R) + p(S) + p(T)] \times p(F_{19})$

$F_{19} = F_{20} + F_{21}$ $\qquad$ $p(F_{19}) = p(F_{20}) + p(F_{21}) - p(F_{20})p(F_{21})$

$F_{20} = CC + DD + EE + FF$ $\qquad$ $p(F_{20}) = p(CC) + p(DD) + p(EE) + p(FF)$

$F_{21} = (T + GG) \times (DD + HH)$ $\qquad$ $p(F_{21}) = [p(T) + p(GG)] \times [p(DD) + p(HH)]$

$F_3 = F_{22} + F_{23} + F_{24}$ $\qquad$ $p(F_3) = p(F_{22}) + p(F_{23}) + p(F_{24}) +$
$$p(F_{22})p(F_{23})p(F_{24}) - p(F_{22})p(F_{24})$$
$$- p(F_{22})p(F_{23}) - p(F_{23})p(F_{24})$$

$F_{22} = F_{25} + F_{26}$ $\qquad$ $p(F_{22}) = p(F_{25}) + p(F_{26}) - p(F_{25})p(F_{26})$

$F_{25} = (D + JJ) \times (LL + KK)$ $\qquad$ $p(F_{25}) = [p(D) + p(J) - p(D)p(J)]$
$$\times [p(LL) + p(KK) - p(LL)p(KK)]$$

$F_{26} = F_{33} + F_{34}$ $\qquad$ $p(F_{26}) = p(F_{33}) + p(F_{34}) - p(F_{33})p(F_{34})$

$F_{33} = II + MM$ $\qquad$ $p(F_{33}) = p(II) + p(MM) - p(II)p(MM)$

$F_{34} = LL + SS$ $\qquad$ $p(F_{34}) = p(LL) + p(SS) - p(LL)p(SS)$

$F_{23} = F_{27} + F_{27}$ $\qquad$ $p(F_{23}) = 2p(F_{27}) - p(F_{27})$

$F_{27} = F_{28} + F_{28} + F_{28}$ $\qquad$ $p(F_{27}) = 3p(F_{28}) + p(F_{28})^3 - 3p(F_{28})^2$

$F_{28} = F_{11} + F_{29}$ $\qquad$ $p(F_{28}) = p(F_{11}) + p(F_{29}) - p(F_{11})p(F_{29})$

$F_{29} = (NN + F + G) \times F_{30}$ $\qquad$ $p(F_{29}) = [p(NN) + p(F) + p(G)] \times p(F_{30})$

$F_{30} = F_{31} + F_{15}$ $\qquad$ $p(F_{30}) = p(F_{31}) + p(F_{15}) - p(F_{31})p(F_{15})$

$F_{31} = OO + M + N + O$ $\qquad$ $p(F_{31}) = p(OO) + p(M) + p(N) + p(O)$

$F_{24} = F_{16} + F_{17} + F_{32}$ $\qquad$ $p(F_{24}) = p(F_{16}) + p(F_{17}) + p(F_{32}) +$
$$p(F_{16})p(F_{17})p(F_{32}) - p(F_{16})p(F_{17}) -$$
$$p(F_{16})p(F_{32}) - p(F_{17})p(F_{32})$$

$F_{32} = (PP + S + T) \times F_{19}$ $\qquad$ $p(F_{32}) = [p(PP) + p(S) + p(T)] \times p(F_{19})$

Table D.12

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	($F/10^6h$)	π_Q	π_E	π_L	($F/10^6h$)	
B	173.392	1.0	6.3	1.0	1092.00	$1.731x10^{-5}$
II						$8.997x10^{-4}$
JJ						$8.997x10^{-4}$
VV	330.1464	1.0	6.3	1.0	2079.92	$4.869x10^{-2}$
RR	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
SS	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
MM	89.3502	1.0	6.3	1.0	562.906	$1.3149x10^{-2}$
NN	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
TT	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
PP	89.3502	1.0	6.3	1.0	562.906	$1.3149x10^{-2}$
QQ	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
UU	330.1464	1.0	6.3	1.0	2079.92	$4.869x10^{-2}$
KK	5.71	1.0	1.0	1.0	5.71	$1.3149x10^{-4}$
LL	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
OO	.06	3.0	1.0	1.0	.18	$4.32x10^{-6}$
FF	173.392	1.0	6.3	1.0	1092.00	$1.731x10^{-5}$

Table D.12 (continued)

DUAL STAR ARCHITECTURE SERIAL TRANSMISSION (CONDITION TWO)

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
B	MMI 1	MMI 1 system fails
II	Secondary storage 1	Secondary storage 1 fails
JJ	Secondary storage 2	Secondary storage 2 fails
VV	MC 2 hardware	MC 2 hardware fails
RR	MC 2 diagnosis software	MC 2 diagnosis software fails
SS	Cable	D3-MC 2 line fails
MM	μPD3 hardware	μPC3 hardware fails
NN	μPD3 software	μPC3 software fails
TT	Cable	D3-MC 2 cable fails
PP	μPD3' hardware	μPD3' hardware fails
QQ	μPD3' software	μPD3' software fails
UU	MC1 hardware	MC1 hardware fails (SR)
KK	MC1 hardware	MC1 hardware fails (SR)
LL	Cable	D3-MC 1 cable fails
FF	MMI 2	MMI 2 system fails

DUAL STAR ARCHITECTURE

PROBABILISTIC EQUATIONS SERIAL TRANSMISSION ALTERNATIVE (SITUATION TWO)

The fault tree and the equations are similar to the parallel transmission case; a few probabilities change. The values of the probabilities used in this case are given in Table D.10 and Table D.12.

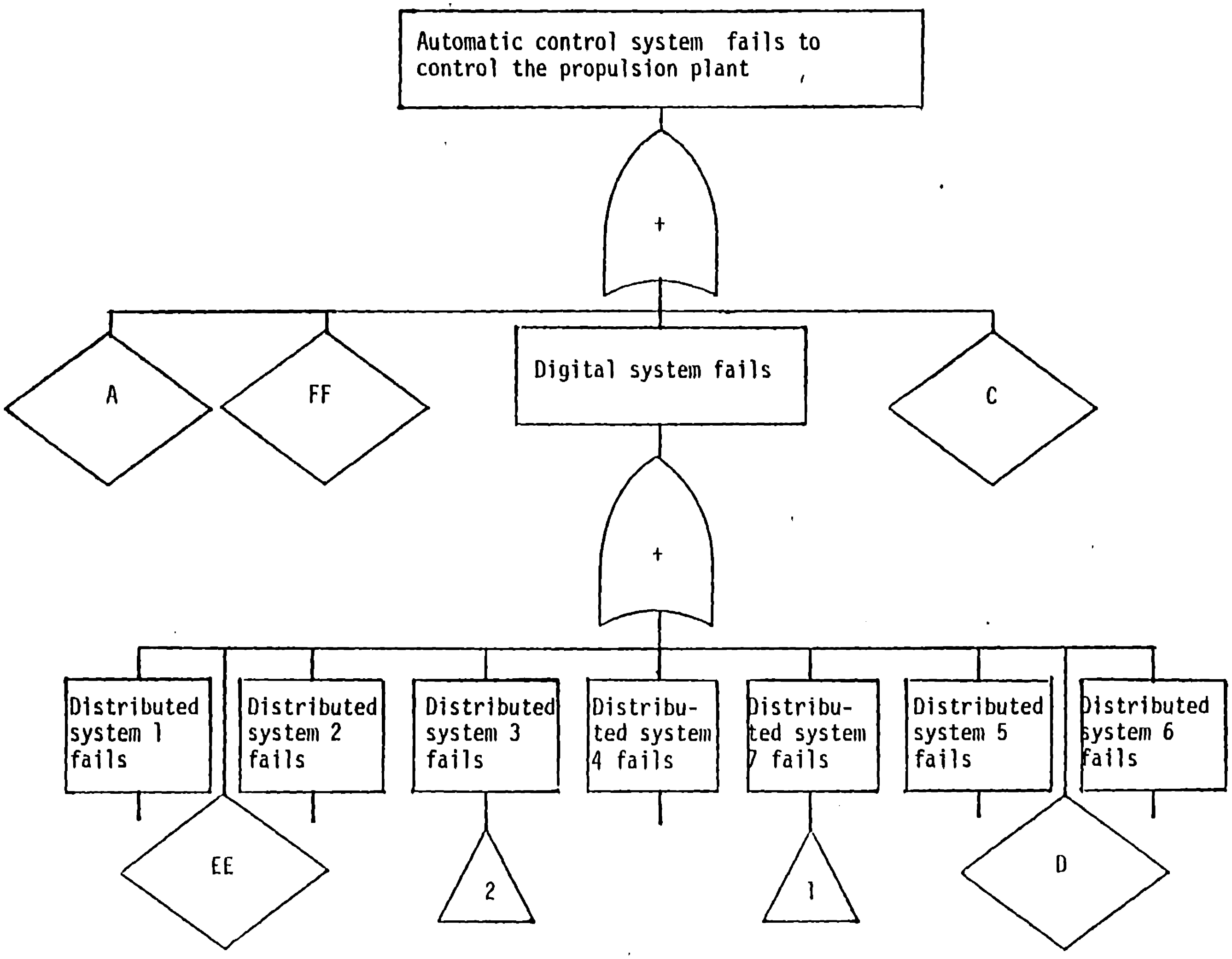

Automatic control system fails to control the propulsion plant
+
A
FF
Digital system fails
C
+
Distributed system 1 fails
Distributed system 2 fails
Distributed system 3 fails
Distributed system 4 fails
Distributed system 7 fails
Distributed system 5 fails
Distributed system 6 fails
EE
2
1
D

Figure D.13 Global bus architecture, situation one.

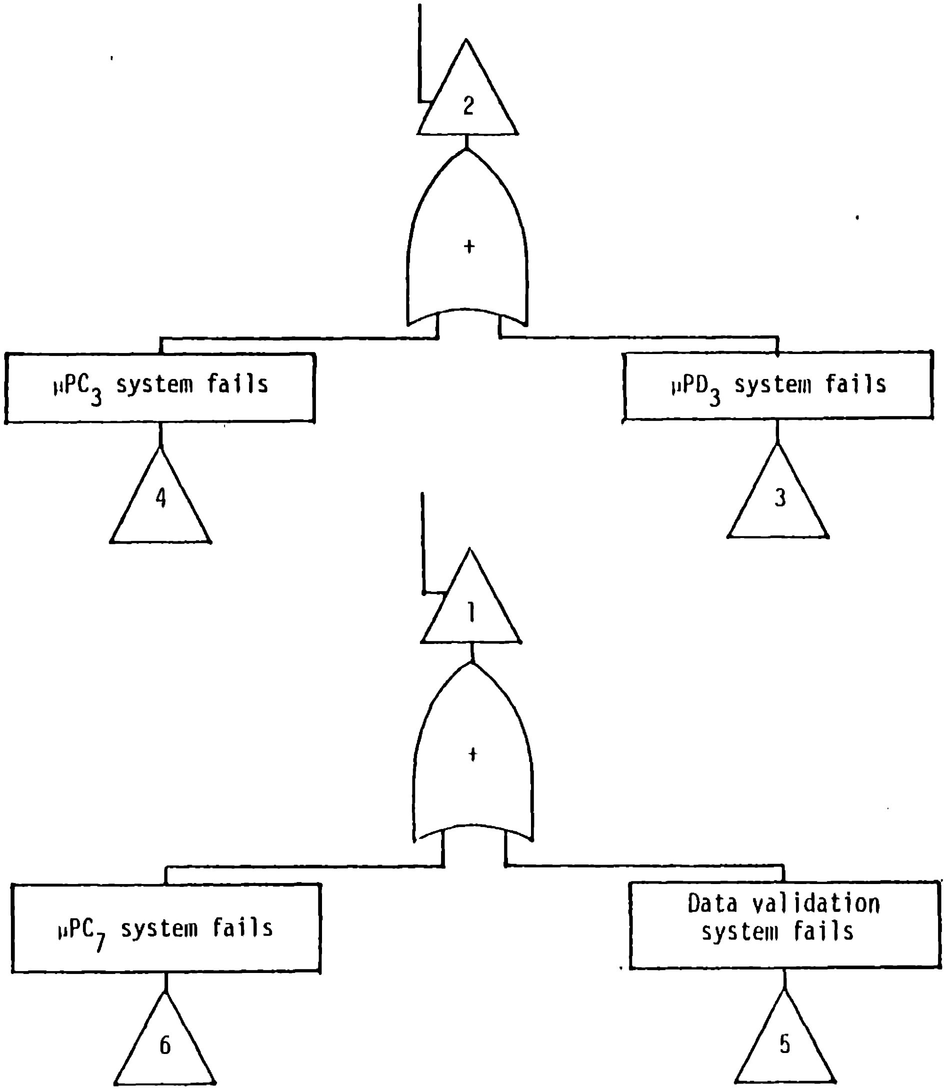


Figure D.13 (continued)

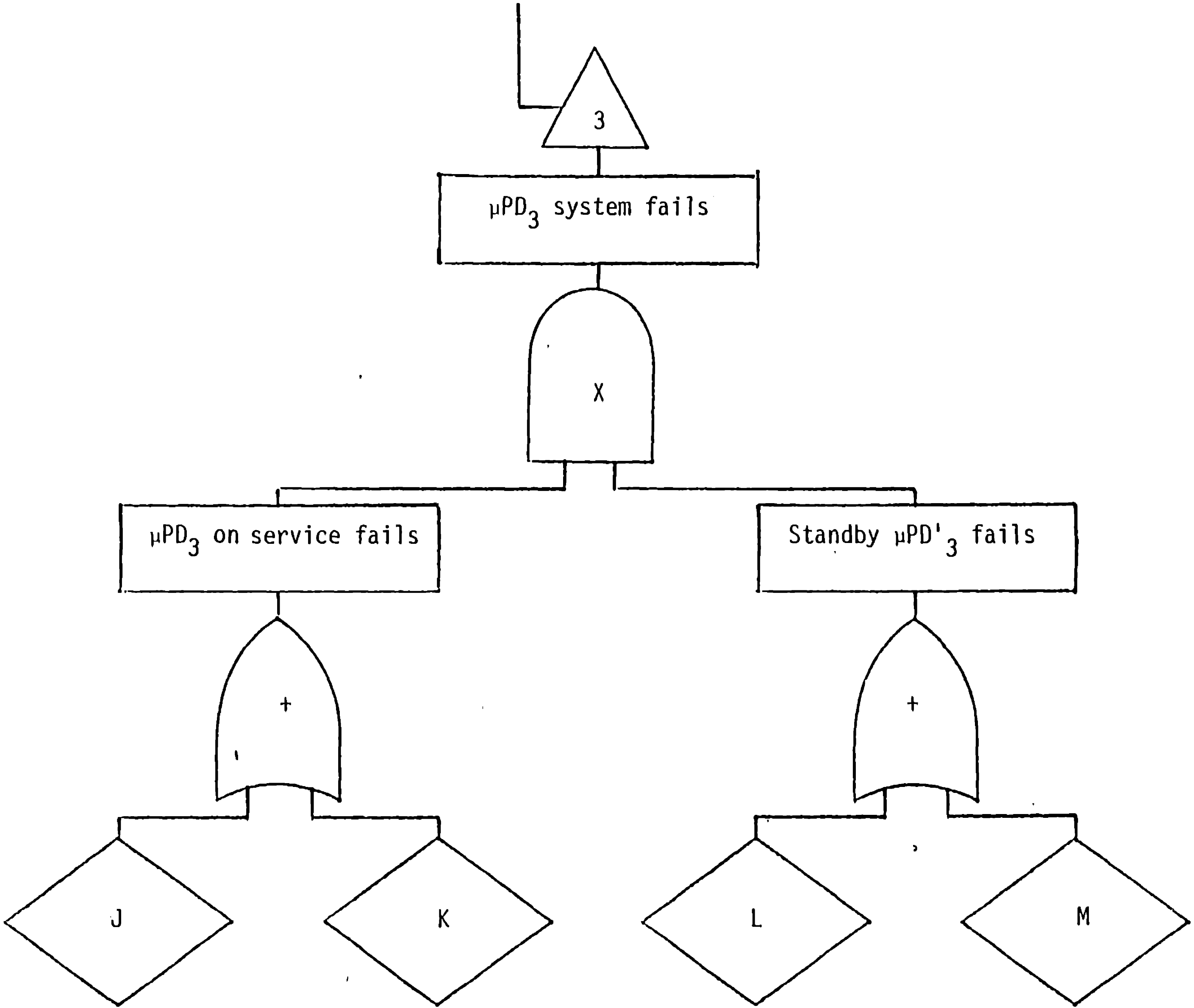


Figure D.13 (continued)

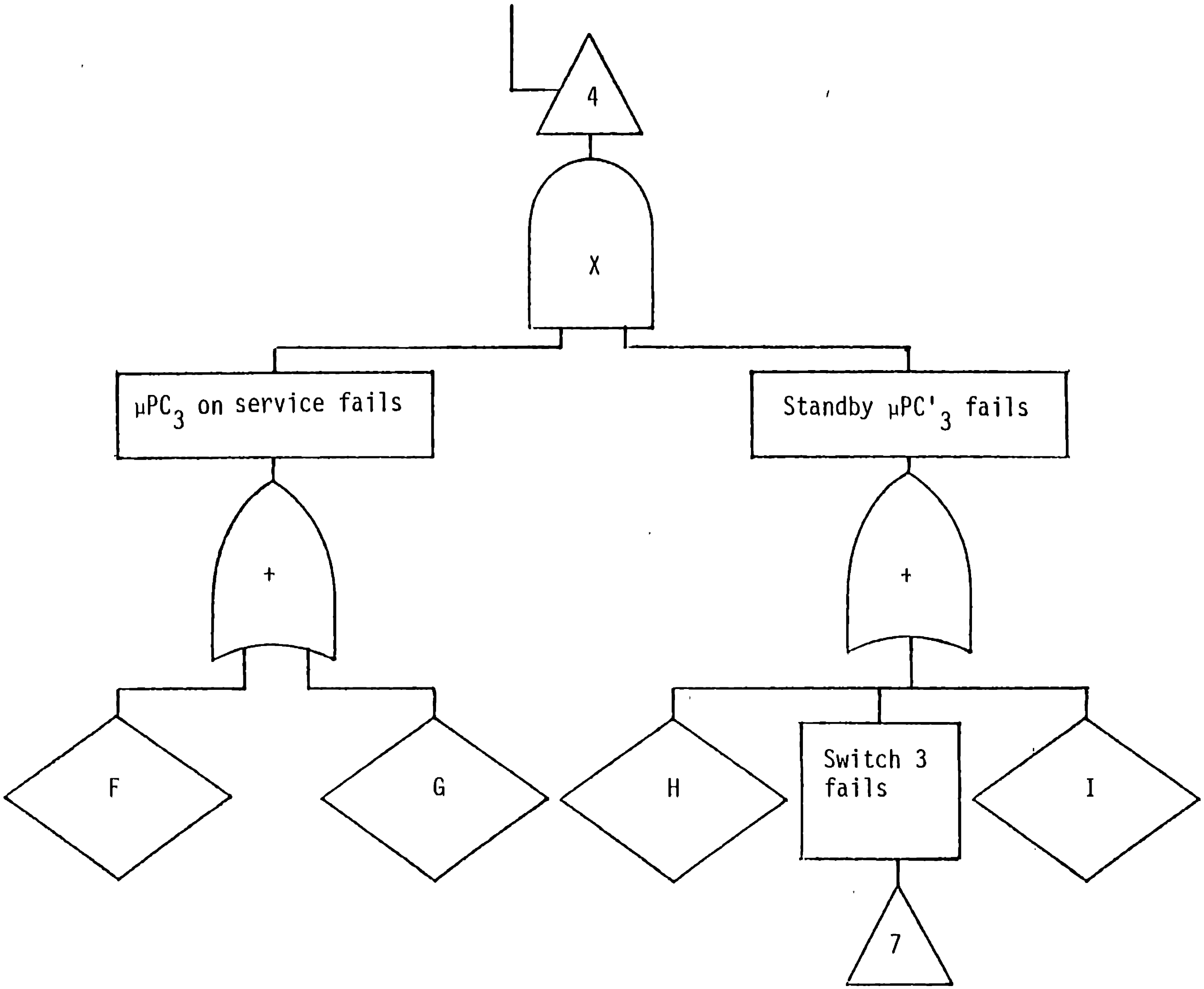


Figure D.13 (continued)

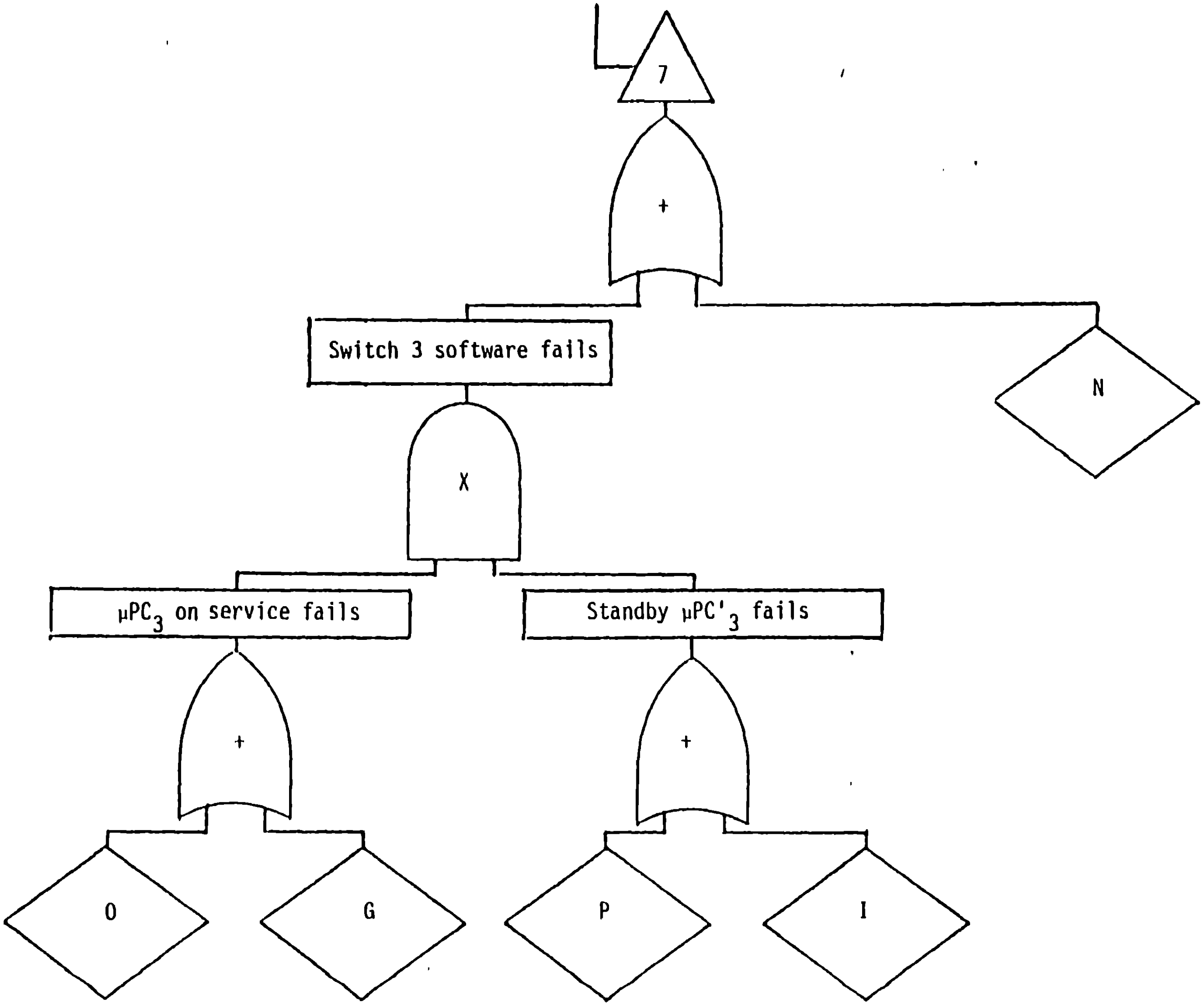


Figure D.13 (continued)

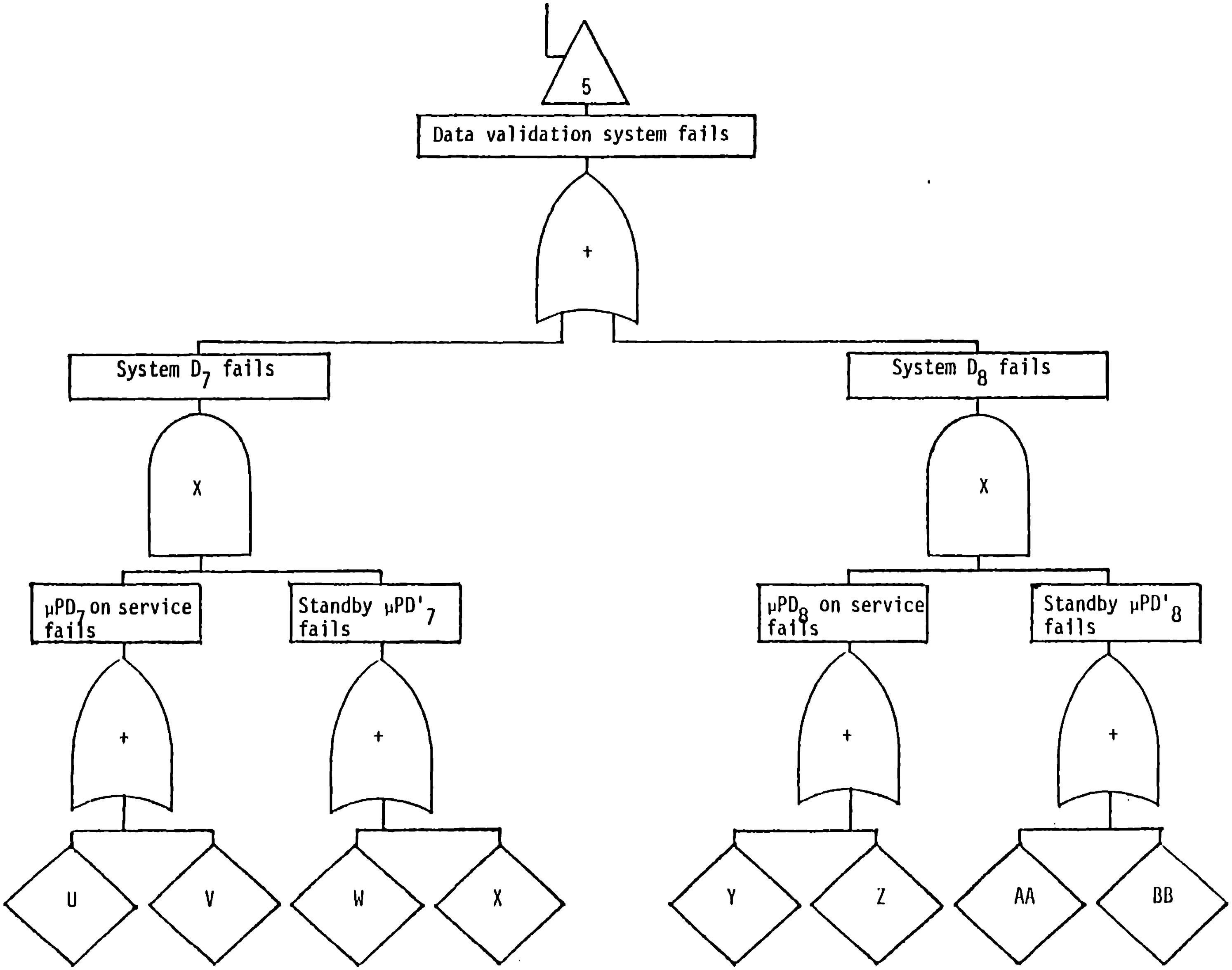


Figure D.13 (continued)

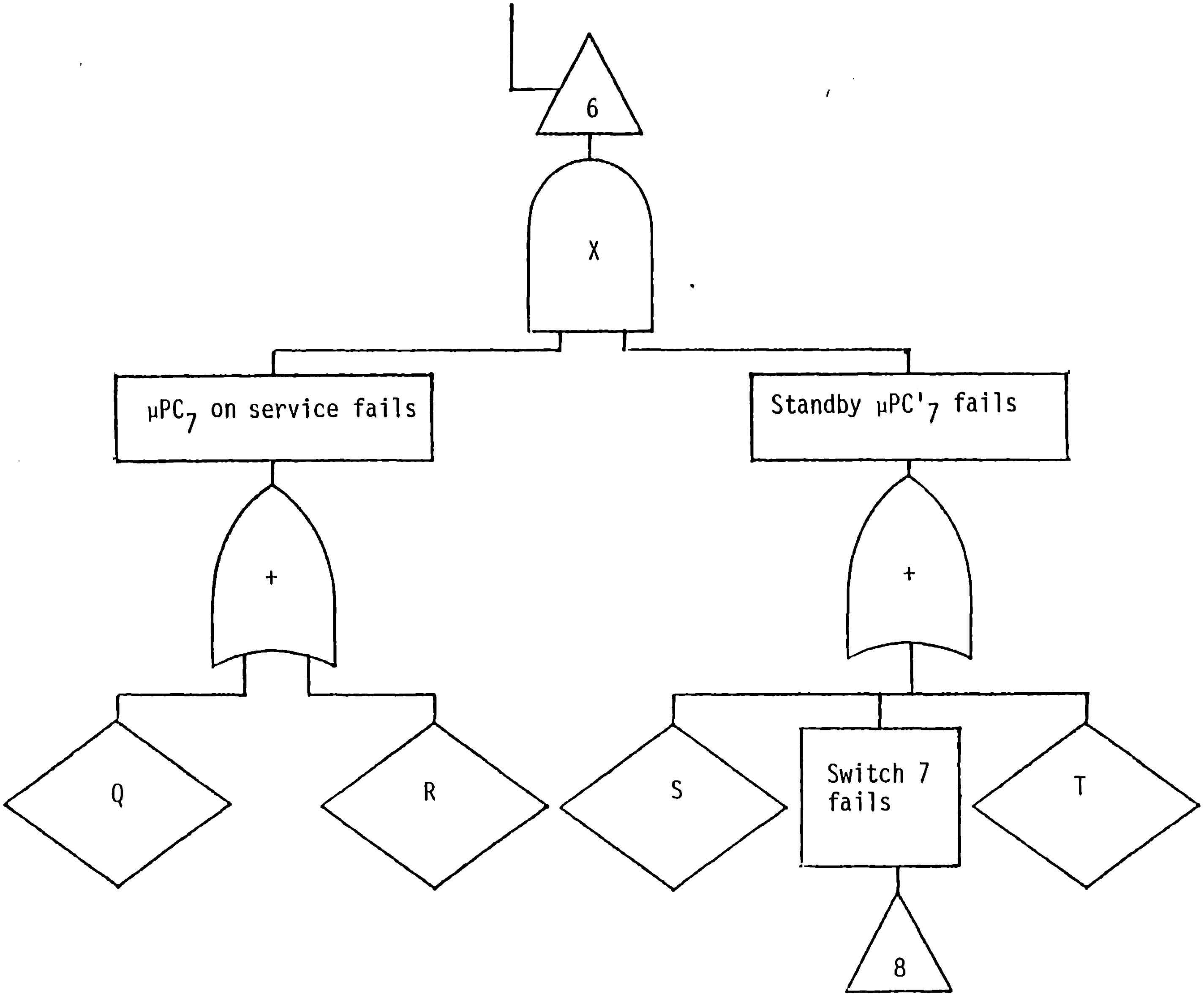


Figure D.13 (continued)

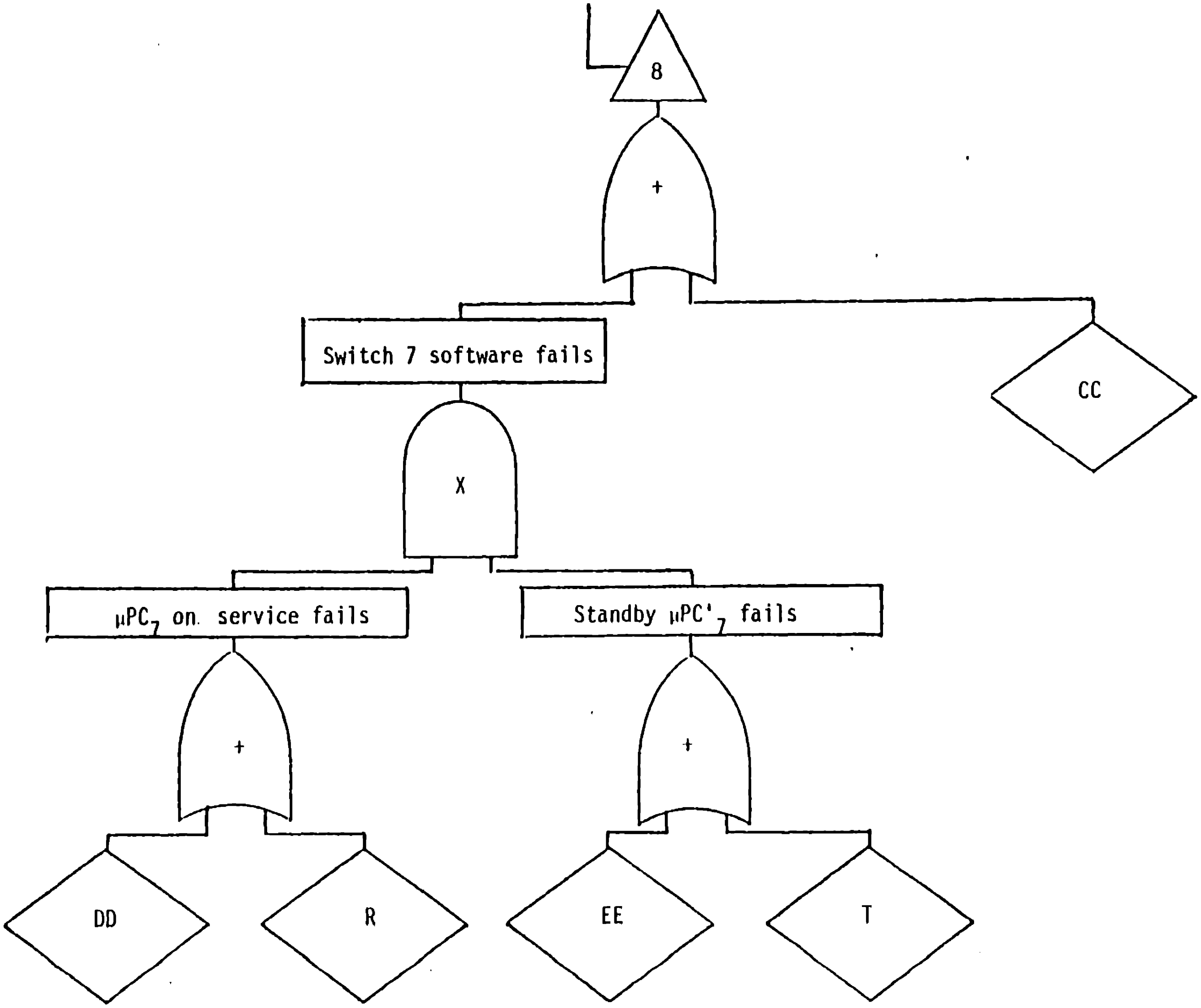


Figure D.13 (continued)

Table D.13

GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRON-MENTAL FACTOR	LEARN-ING FACTOR	FAILURE RATE (λ)	EVENT PROBA-BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
A	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
C	173.392	1.0	6.3	1.0	$1.092\text{x}10^{3}$	$1.731\text{x}10^{-5}$
D	223.84	1.0	6.3	1.0	1410.19	$3.328\text{x}10^{-2}$
E	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
F	102.517	1.0	6.3	1.0	646.046	$1.538\text{x}10^{-2}$
G	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
H	102.517	1.0	6.3	1.0	646.046	$1.538\text{x}10^{-2}$
I	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
J	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
K	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
L	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
M	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
N	.155	1.0	6.3	1.0	0.9765	$1.8747\text{x}10^{-4}$
O	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
P	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
Q	102.517	1.0	6.3	1.0	646.046	$1.538\text{x}10^{-2}$
R	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
S	102.517	1.0	6.3	1.0	646.046	$1.538\text{x}10^{-2}$
T	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
U	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$

Table D.13 (continued)

GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION ONE)

	GENERIC		ENVIRON-	LEARN-		EVENT
EVENT	FAILURE	QUALITY	MENTAL	ING	FAILURE	PROBA-
SYMBOL	RATE (λ_G)	FACTOR	FACTOR	FACTOR	RATE (λ)	BILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
V	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
W	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
X	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
Y	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
Z	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
AA	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
BB	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
CC	.155	1.0	6.3	1.0	.9765	$1.8747\text{x}10^{-4}$
DD	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
EE	67.6105	1.0	6.3	1.0	425.95	$1.017\text{x}10^{-2}$
FF						$8.997\text{x}10^{-4}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
A	Coaxial cable	Global bus fails
C	MMI	MMI system fails
D	MC hardware	MC hardware fails
E	MC control software	MC control software fails
F	μPC3 hardware	μPC3 hardware fails
G	μPC3 software	μPC3 software fails
H	μPC'3 hardware	μPC'3 hardware fails
I	μPC'3 software	μPC'3 software fails
J	μPD'3 hardware	μPD'3 hardware fails
K	μPD3 software	μPD3 software fails
L	μPD'3 hardware	μPD'3 hardware fails

Table D.13 (continued)

GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION ONE)

M	μPD3' software	μPD3' software fails
N	Switch 3	Switch 3 fails
O	μPC3 hardware	μPC3 hardware fails (SR)
P	μPC'3 software	μPC'3 software fails (SR)
Q	μPC7 hardware	μPC7 hardware fails
R	μPC7 software	μPC7 software fails
S	μPC'7 hardware	μPC'7 hardware fails
T	μPC'7 software	μPC'7 software fails
U	μPD7 hardware	μPD7 hardware fails
V	μPD7 software	μPD7 software fails
W	μPD'7 hardware	μPD'7 hardware fails
X	μPD'7 software	μPD'7 software fails
Y	μPD8 hardware	μPD8 hardware fails
Z	μPD8 software	μPD8 software fails
AA	μPD'8 hardware	μPD'8 hardware fails
BB	μPD'8 software	μPD'8 software fails
CC	Switch 7	Switch 7 fails
DD	μPC7 hardware	μPC7 hardware fails (SR)
EE	μPC'7 hardware	μPC'7 hardware fails (SR)
FF	Secondary storage	Secondary storage fails

GLOBAL BUS ARCHITECTURE

PROBABILISTIC EQUATIONS D.13 SITUATION ONE

From the fault tree:

$$\begin{aligned} TE = {} & A + \underline{C} + \underline{D} + E + \underline{FF} + \{ [\underline{F} + G] \times [\underline{H} + I + N + (\underline{O} + G) \times (\underline{P} + I)] \\ & + [\underline{J} + K] \times [\underline{L} + M] \} + \{ \quad \} + \{ \quad \} + \{ \quad \} + \{ \quad \} + \{ \quad \} + \{ [\underline{Q} + R] \\ & \times [\underline{S} + T + CC + (\underline{DD} + R) \times (\underline{EE} + T)] + [\underline{U} + V] \times [\underline{W} + X] + [\underline{Y} + Z] \\ & \times [AA + BB] \} \end{aligned}$$

Applying the probabilistics laws:

$TE = F_1 + F_2 + F_3$

$$\begin{aligned} p(TE) = {} & p(F_1) + p(F_2) + p(F_3) + p(F_1)p(F_2)p(F_3) \\ & - p(F_1)p(F_2) - p(F_1)p(F_3) - p(F_2)p(F_3) \end{aligned}$$

$F_1 = F_{17} + F_{18}$

$$p(F_1) = p(F_{17}) + p(F_{18}) - p(F_{17})p(F_{18})$$

$F_{17} = C$	$p(F_{17}) = p(C)$
$F_{18} = D + E + FF + A$	$p(F_{18}) = p(D) + p(E) + p(FF) - p(D)p(FF) + p(A)$
$F_2 = F_4 + F_4$	$p(F_2) = 2p(F_4) - p(F_4)^2$
$F_4 = F_5 + F_5 + F_5$	$p(F_4) = 3p(F_5) + p(F_5)^3 - 3p(F_5)^2$
$F_5 = F_6 + F_7$	$p(F_5) = p(F_6) + p(F_7) - p(F_6)p(F_7)$
$F_6 = (J + K) \times (L + M)$	$p(F_6) = [p(J) + P(K)] \times [p(L) + p(M)]$
$F_7 = (F + G) \times F_8$	$p(F_7) = [p(F) + p(G)] \times p(F_8)$
$F_8 = F_9 + F_{10}$	$p(F_8) = p(F_9) + p(F_{10}) - p(F_9)p(F_{10})$
$F_9 = H + I + N$	$p(F_9) = p(H) + p(I) + p(N)$
$F_{10} = (O + G) \times (P + I)$	$p(F_{10}) = [p(O) + p(G)] \times [p(P) \times p(I)]$
$F_3 = F_{11} + F_{12} + F_{13}$	$p(F_3) = p(F_{11}) + p(F_{12}) + p(F_{13}) +$ $p(F_{11})p(F_{12})p(F_{13}) - p(F_{11})p(F_{12}) -$ $p(F_{12})p(F_{13}) - p(F_{11})p(F_{13})$
$F_{11} = (U + V) \times (W + X)$	$p(F_{11}) = [p(U) + p(V)] \times [p(W) + p(X)]$
$F_{12} = (Y + Z) \times (AA + BB)$	$p(F_{12}) = [p(Y) + p(Z)] \times [p(AA) + p(BB)]$
$F_{13} = (Q + R) \times F_{14}$	$p(F_{12}) = [p(Q) + p(R)] \times p(F_{14})$
$F_{14} = F_{15} + F_{16}$	$p(F_{14}) = p(F_{15}) + p(F_{16}) - p(F_{15})p(F_{16})$
$F_{15} = S + T + CC$	$p(F_{15}) = [p(S) + p(T) + p(CC)$
$F_{16} = (DD + R) \times (EE + T)$	$p(F_{16}) = [p(DD) + p(R)] \times [p(EE) + p(T)]$

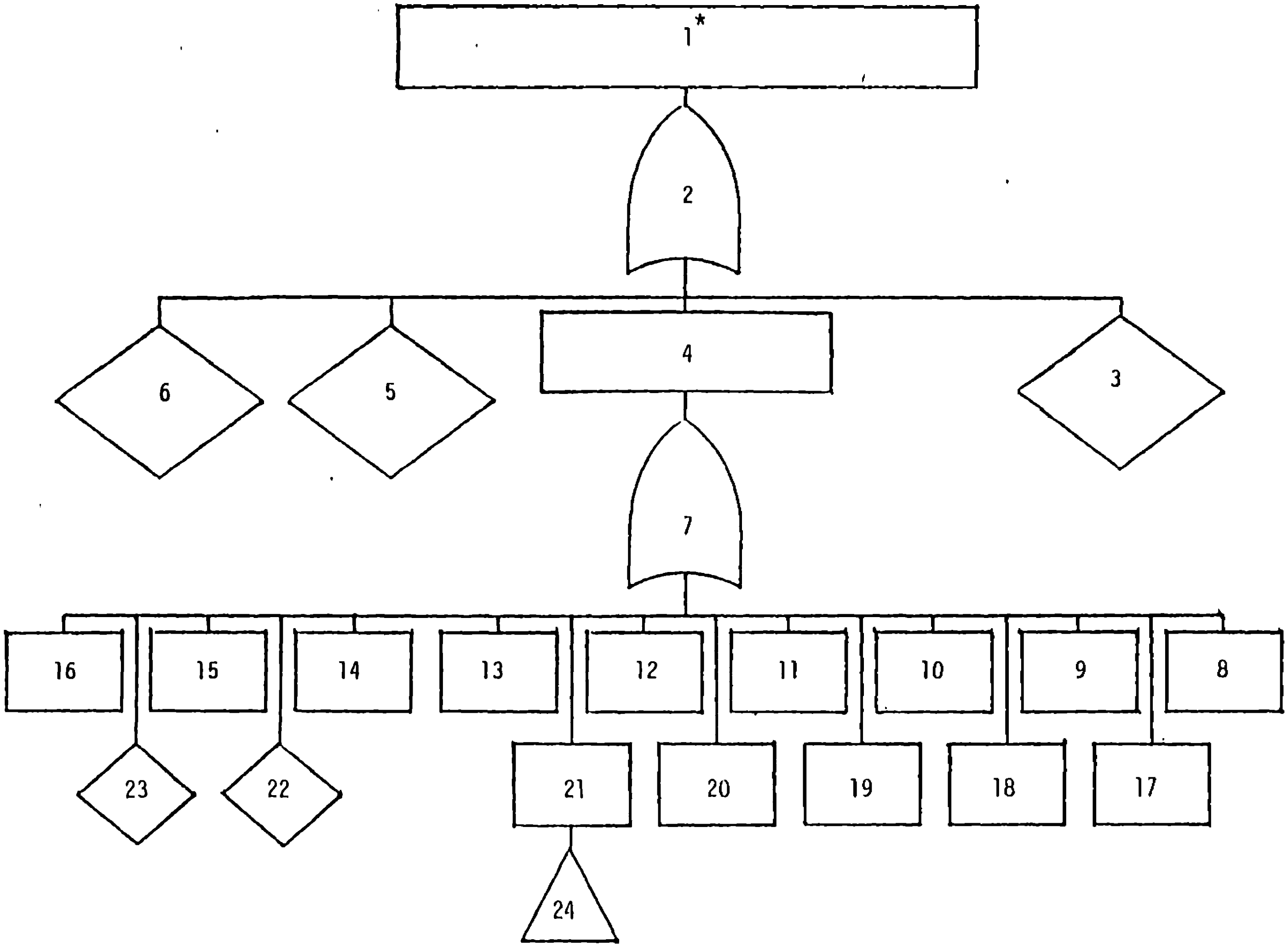


Figure D.14 Global bus architecture, situation two.
*See legend on next page.

1. Control system fails to diagnose and to advise the appropriate corrective measures
2. +
3. FF
4. Digital diagnosis system fails
5. A
6. C
7. +
8. Distributed system D_9 fails
9. Distributed system D_8 fails
10. Distributed system D_7 fails
11. Distributed system D_6 fails
12. Distributed system D_5 fails
13. Distributed system D_4 fails
14. Distributed system D_2 fails
15. Distributed system D_1 fails
16. Distributed system D_{14} fails
17. Distributed system D_{13} fails
18. Distributed system D_{12} fails
19. Distributed system D_{11} fails
20. Distributed system D_{10} fails
21. Distributed system D_3 fails
22. GG
23. HH
24. 1

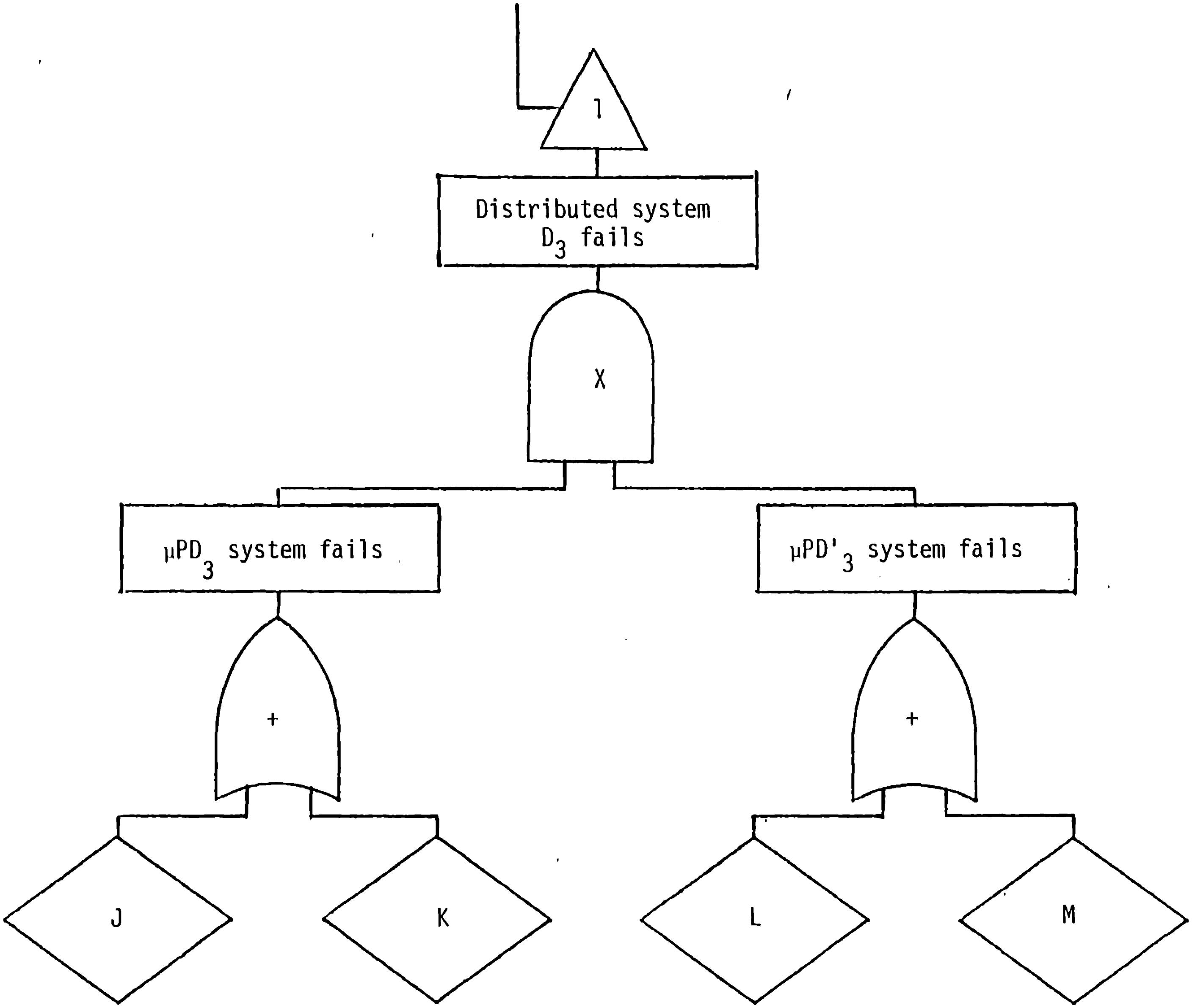


Figure D.14 (continued)

Table D.14

GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10 h^6)	
FF						$8.997\text{x}10^{-4}$
GG	223.84	1.0	6.3	1.0	1410.19	$3.328\text{x}10^{-2}$
HH	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
J	96.776	1.0	6.3	1.0	609.688	$1.452\text{x}10^{-2}$
K	5.71	1.0	1.0	1.0	5.71	1.314910^{-4}
L	97.776	1.0	6.3	1.0	609.608	$1.452\text{x}10^{-2}$
M	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
E	173.392	1.0	6.3	1.0	$1.092\text{x}10^{3}$	$1.731\text{x}10^{-5}$
A	0.06	3.0	1.0	1.0	0.18	$4.32\text{x}10^{-6}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
FF	Secondary storage	Secondary storage fails
GG	MC hardware	MC hardware fails
HH	MC diagnosis software	MC diagnosis software fails
J	μPD3 hardware	μPD3 hardware fails
K	μPD3 software	μPD3 software fails
L	μPD'3 hardware	μPD'3 hardware fails
M	μPD'3 software	μPD'3 software fails
E	MMI system	MMI system fails
A	Coaxial cable	Global bus fails

From the fault tree:

TE = FF + A + C + GG + HH + [J + K] x [L + M] + [ ] + [ ] + [ ] + [ ] +

+ [ ] + [ ] + [ ] + [ ] + [ ] + [ ] + [ ] + [ ] +[ ]

Applying the probabilistics laws:

$TE = F_1 + F_2$	$p(TE) = p(F_1) + p(F_2) - p(F_1)p(F_2)$
$F_1 = F_8 + F_9$	$p(F_1) = p(F_8) + p(F_9) - p(F_8)p(F_9)$
$F_8 = FF + GG$	$p(F_8) = p(FF) + p(GG) - p(FF)p(GG)$
$F_9 = A + C + HH$	$p(F_9) = p(A) + p(C) + p(HH)$
$F_2 = F_3 + F_3$	$p(F_2) = 2p(F_3) - p(F_3)^2$
$F_3 = F_4 + F_5$	$p(F_3) = p(F_4) + p(F_5) - p(F_4)p(F_5)$
$F_4 = F_6 + F_6$	$p(F_4) = 2p(F_6) - p(F_6)^2$
$F_6 = F_7 + F_7$	$p(F_6) = 2p(F_7) - p(F_7)^2$
$F_5 = F_7 + F_7 + F_7$	$p(F_5) = 3p(F_7) + p(F_7)^3 - 3p(F_7)^2$
$F_7 = (J+K) \times (L+M)$	$p(F\ ) = [p(J) + p(K)] \times [p(L) + p(M)]$

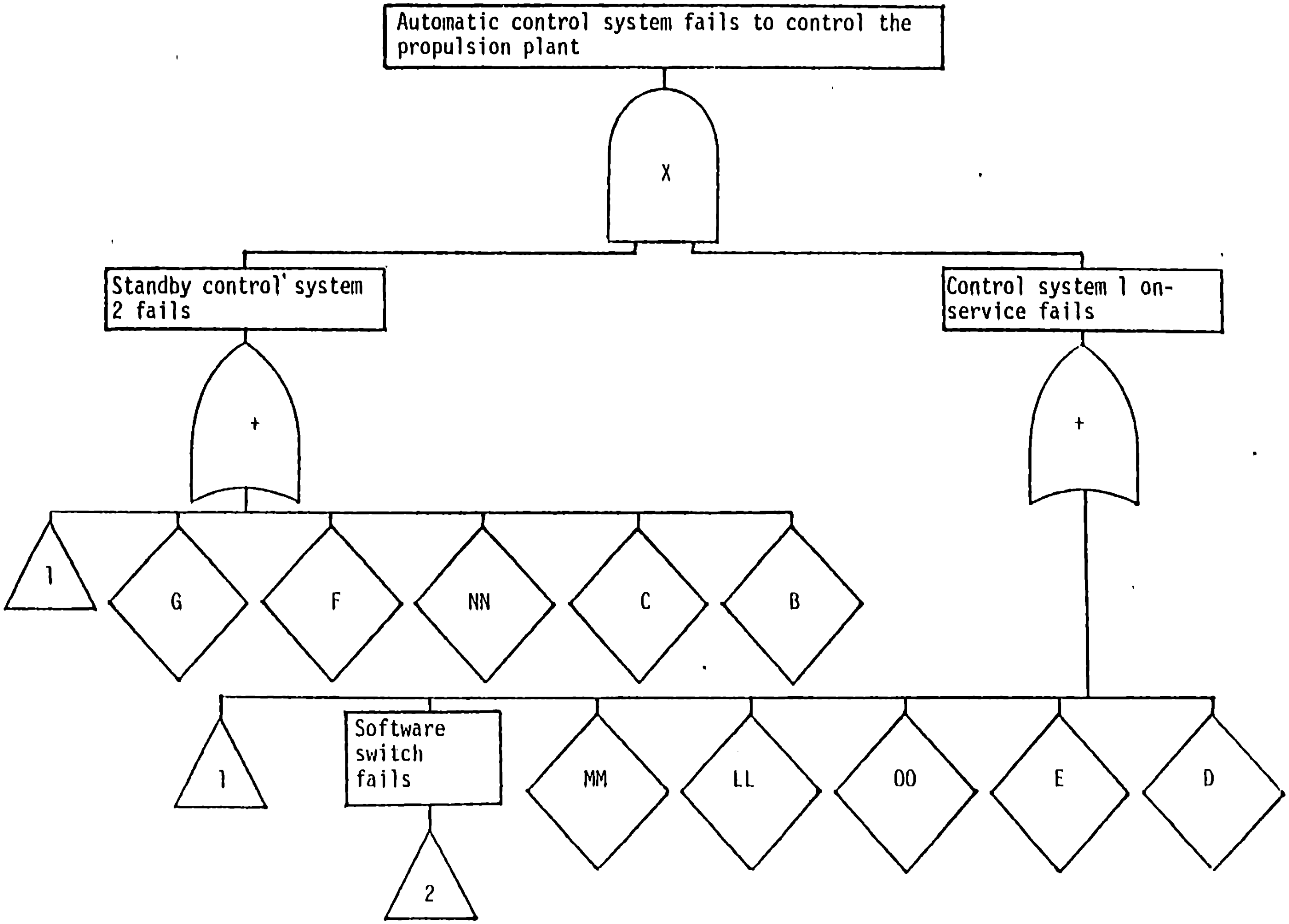

Automatic control system fails to control the propulsion plant
X
Standby control' system 2 fails
Control system 1 on-service fails
+
+
1
G
F
NN
C
B
1
Software switch fails
MM
LL
OO
E
D
2

Figure D.15 Dual global bus architecture, situation one.

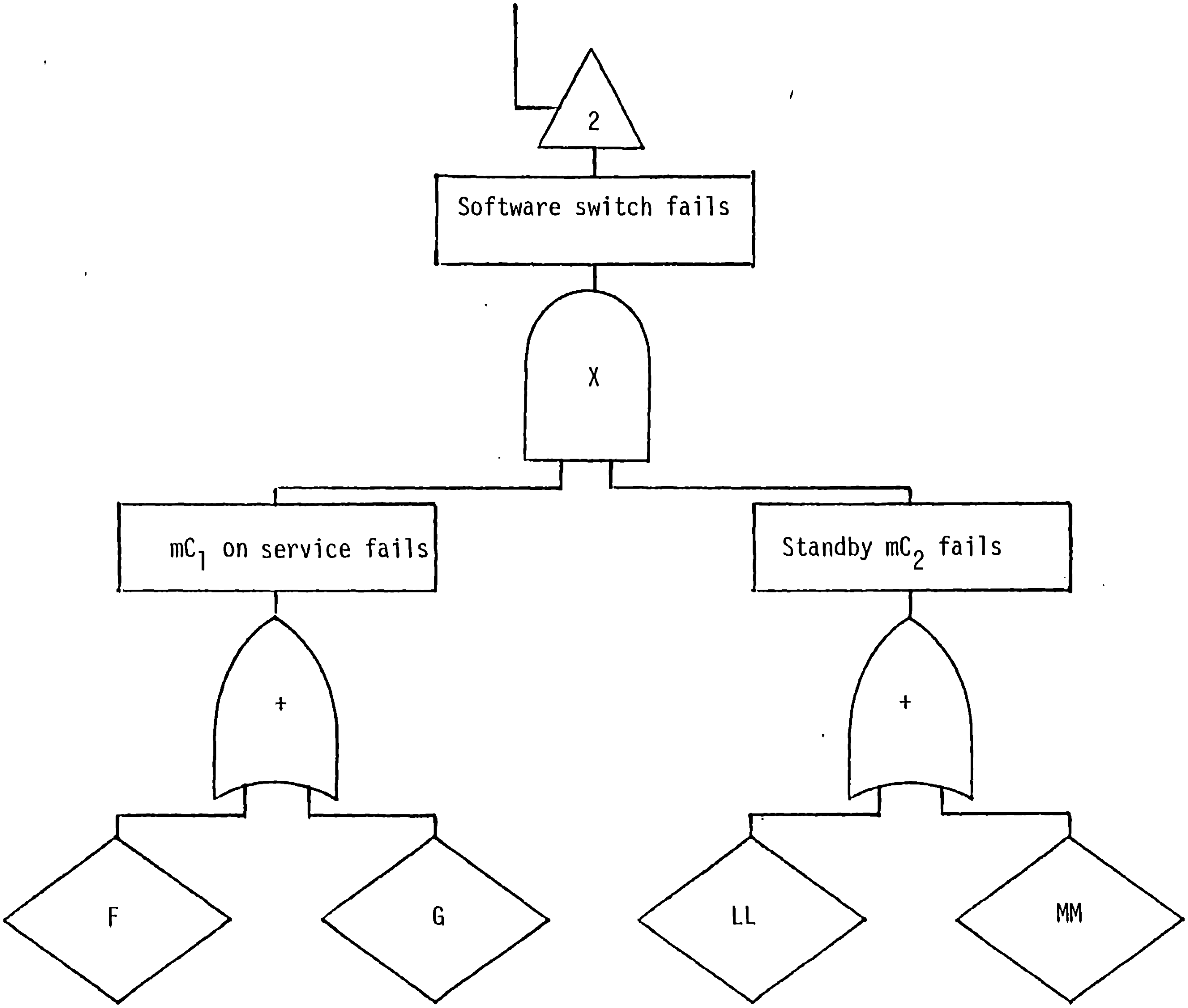


Figure D.15 (continued)

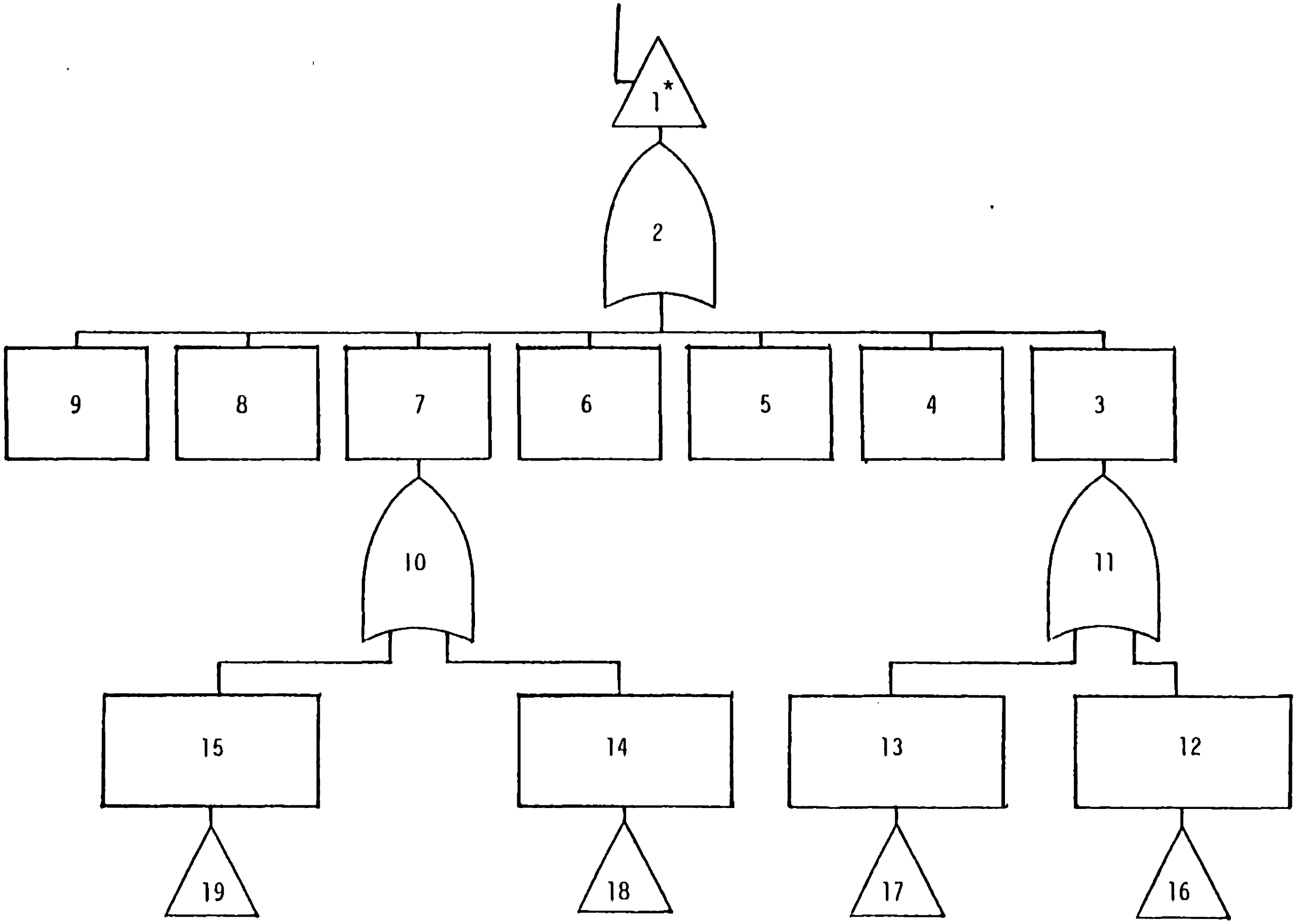


Figure D.15 (continued)

1. 1
2. +
3. Distributed system 7 fails
4. Distributed system 6 fails
5. Distributed system 5 fails
6. Distributed system 4 fails
7. Distributed system 3 fails
8. Distributed system 2 fails
9. Distributed system 1 fails
10. +
11. +
12. Data validation system fails
13. μPC_7 system fails
14. μPD_3 system fails
15. μPC_3 system fails
16. 3
17. 4
18. 5
19. 6

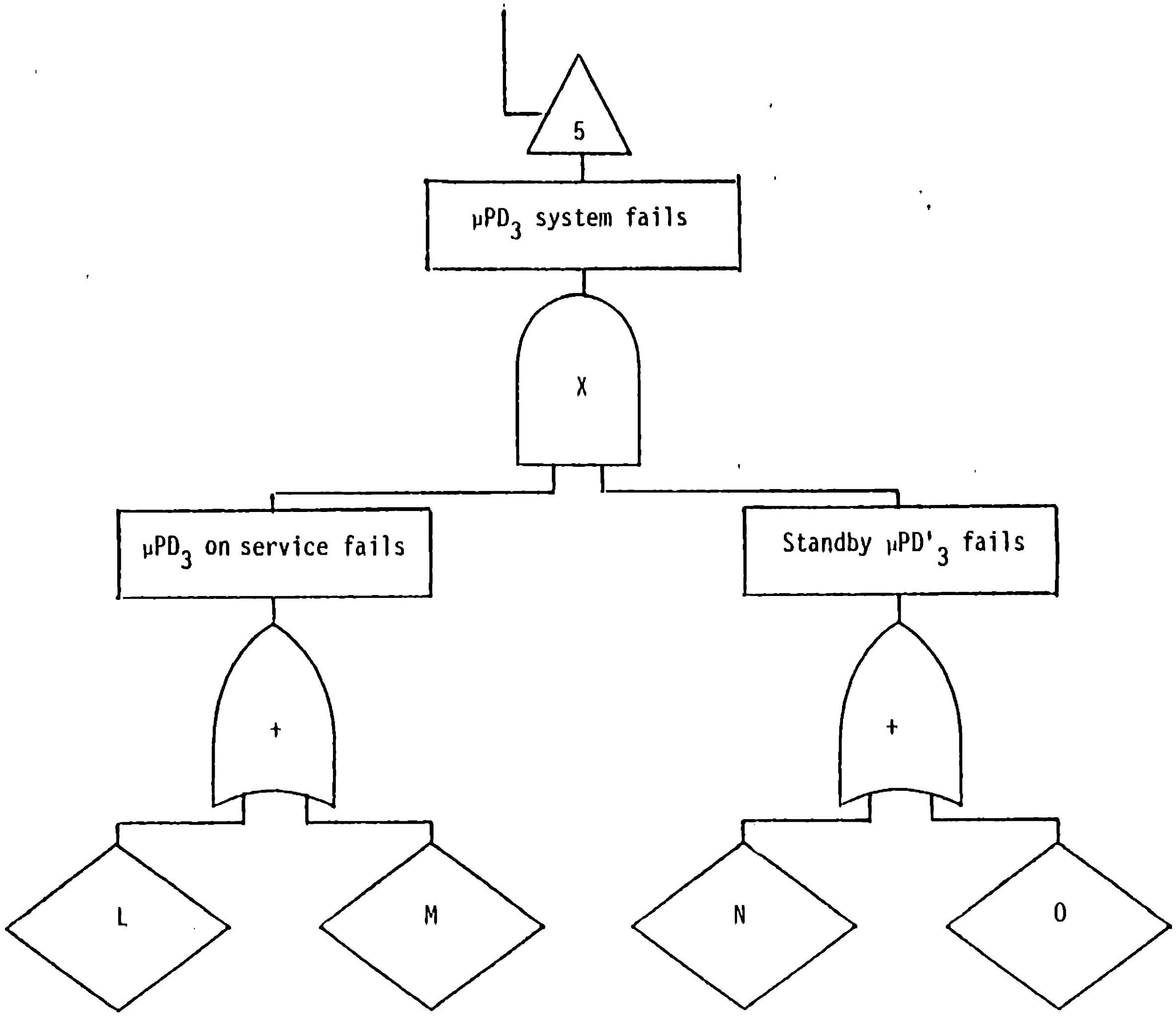


Figure D.15 (continued)

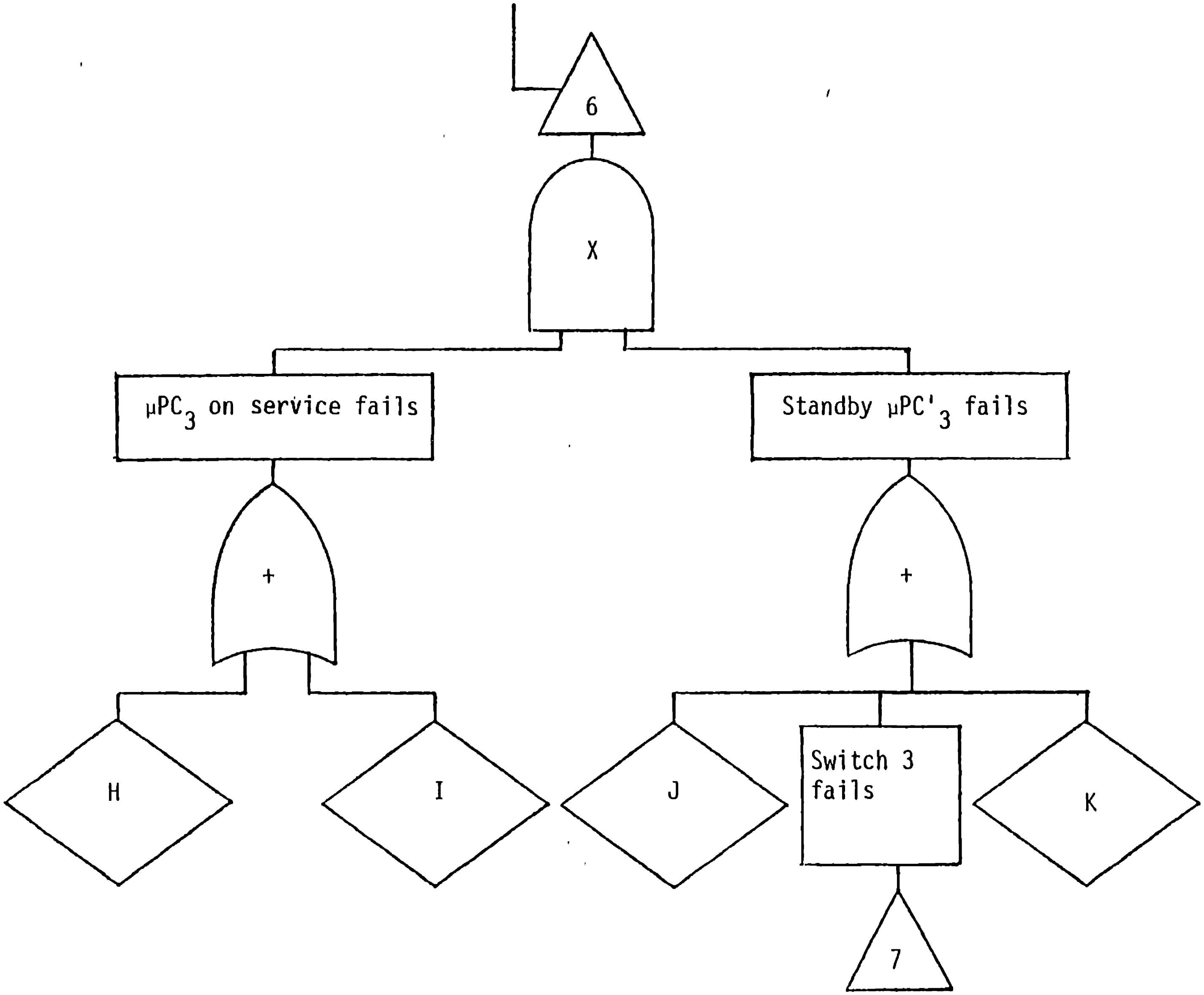


Figure D.15 (continued)

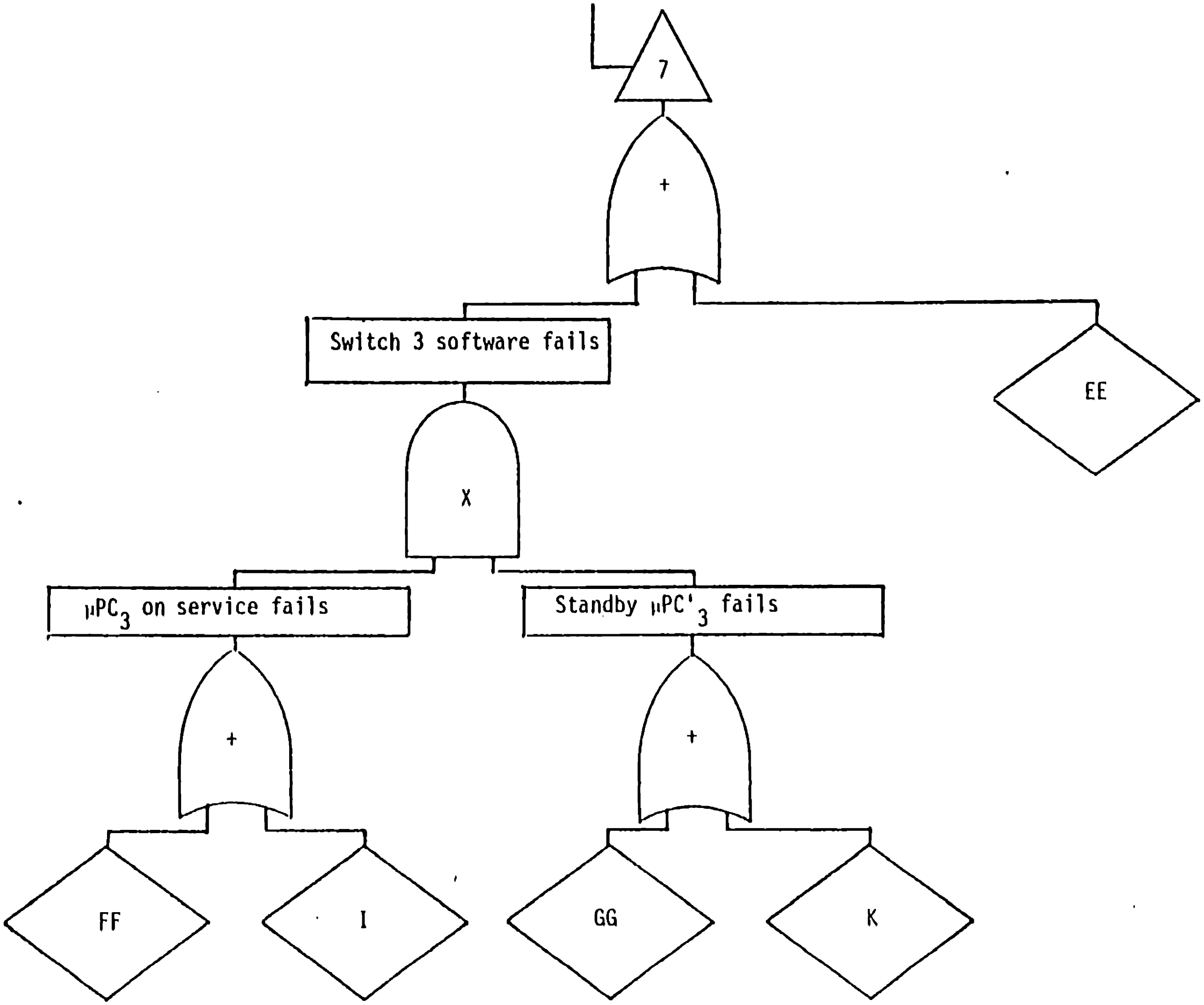


Figure D.15 (continued)

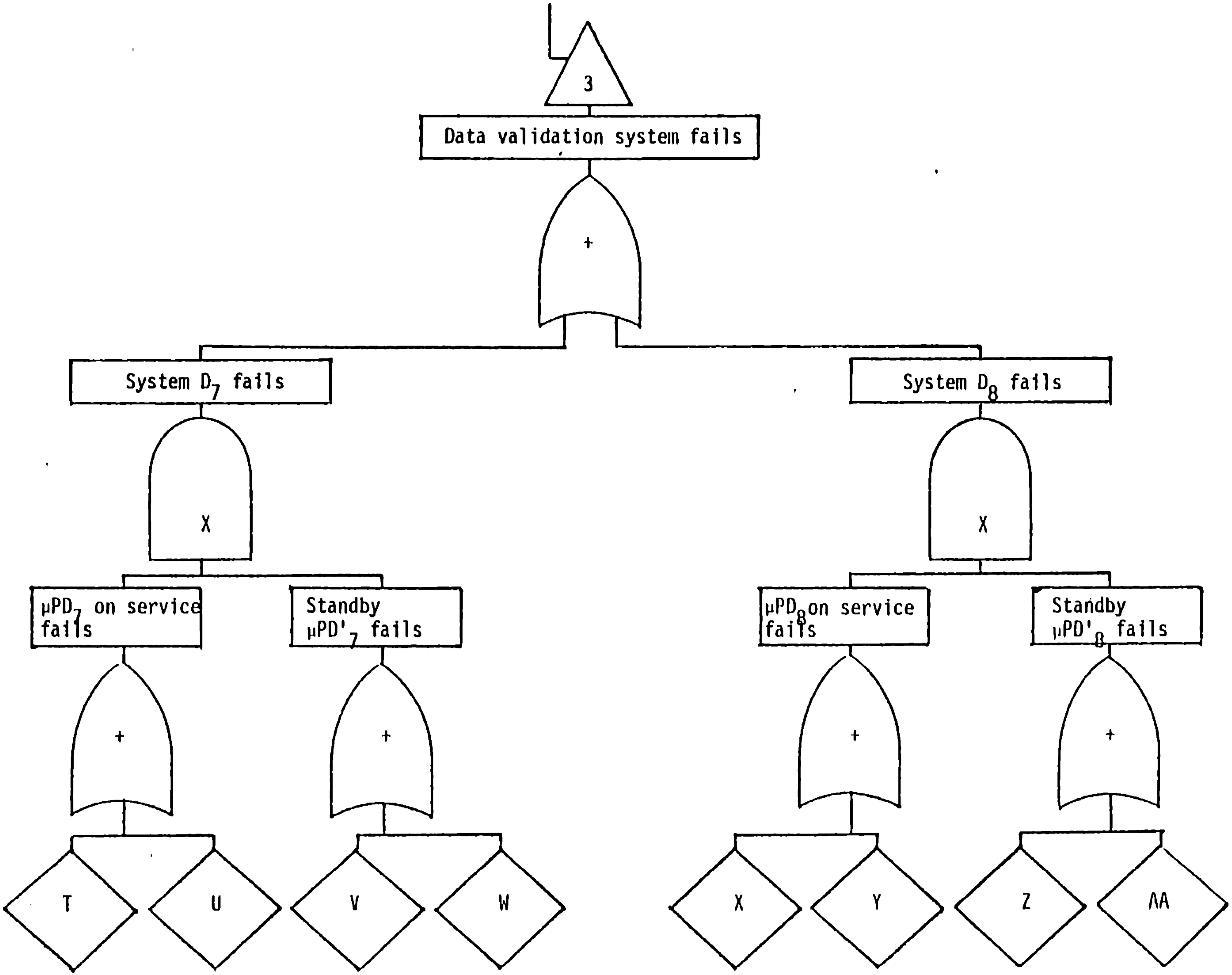

3
Data validation system fails
+
System D_7 fails
System D_8 fails
X
X
μPD_7 on service fails
Standby $\mu PD'_7$ fails
μPD_8 on service fails
Standby $\mu PD'_8$ fails
+
+
+
+
T
U
V
W
X
Y
Z
AA

Figure D.15 (continued)

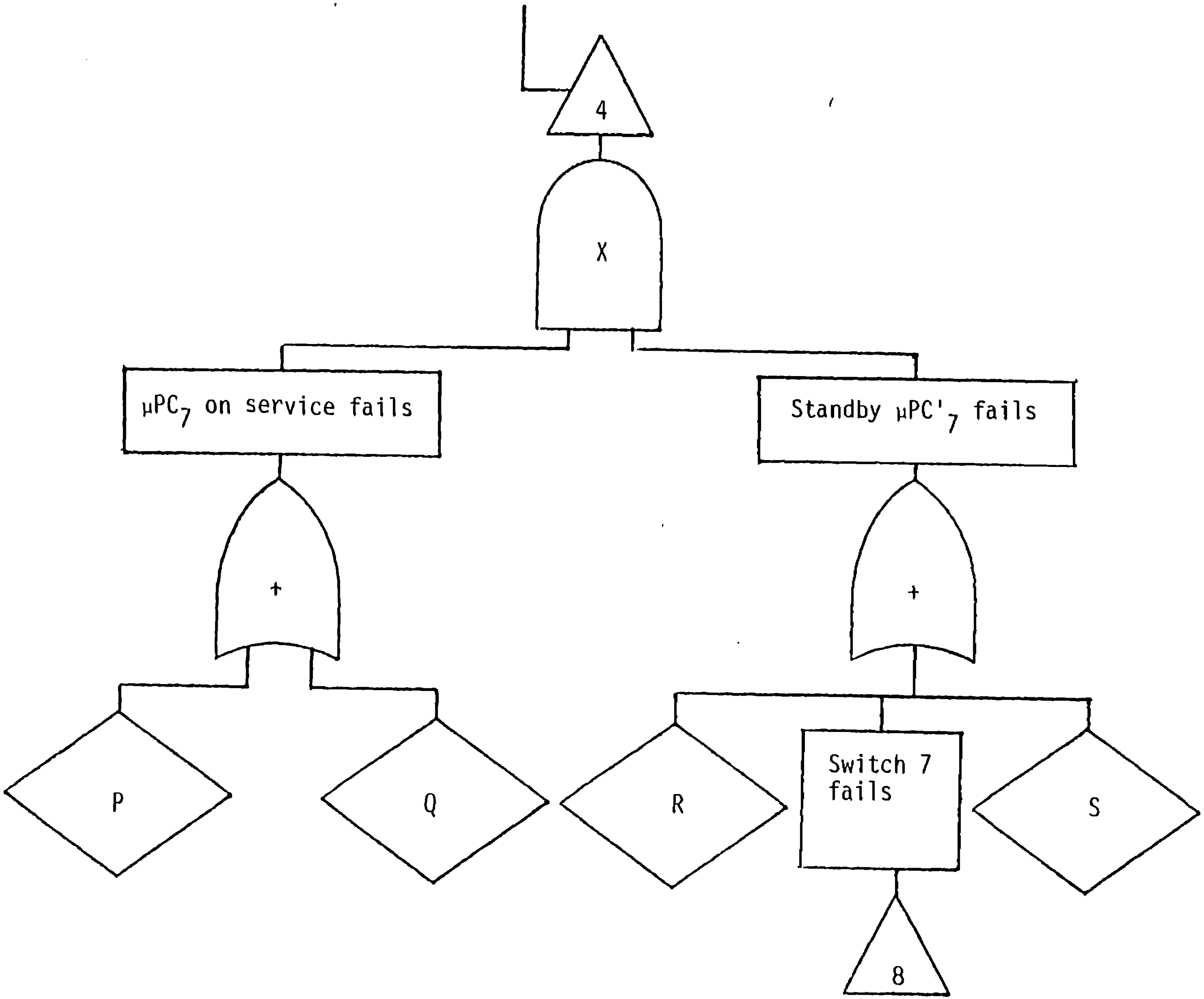


Figure D.15 (continued)

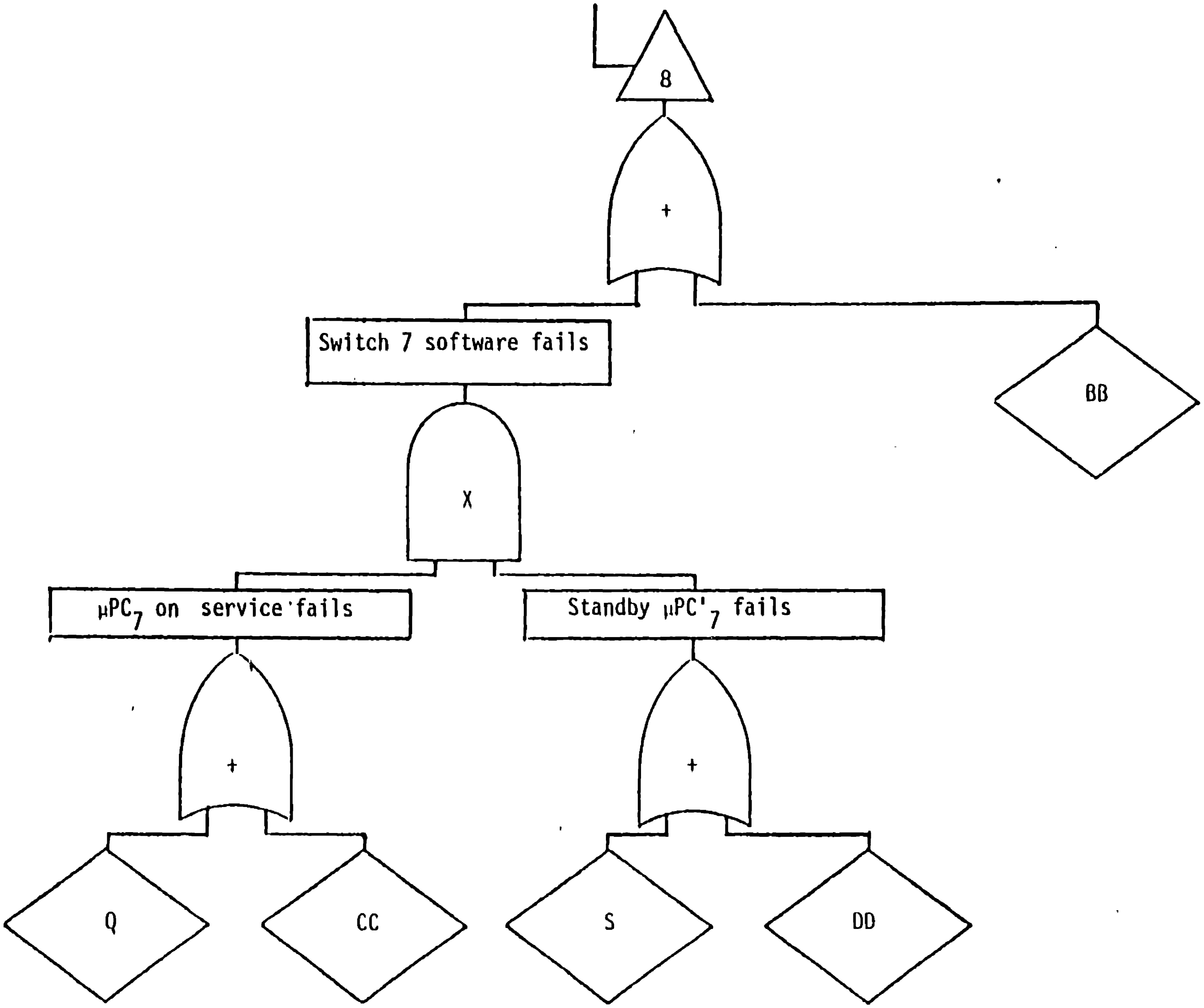


Figure D.15 (continued)

Table D.15

DUAL GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^6h)	π_Q	π_E	π_L	(F/10^6h)	
B	0.06	3.0	1.0	1.0	0.18	4.32×10^{-6}
C	173.392	1.0	6.3	1.0	1.092×10^{3}	1.731×10^{-5}
D	0.06	3.0	1.0	1.0	0.18	4.32×10^{-6}
E	173.392	1.0	6.3	1.0	1.092×10^{3}	1.731×10^{-5}
F	223.84	1.0	6.3	1.0	1410.19	3.328×10^{-2}
G	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
H	127.547	1.0	6.3	1.0	803.546	1.91×10^{-2}
I	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
J	127.547	1.0	6.3	1.0	803.546	1.91×10^{-2}
K	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
L	127.993	1.0	6.3	1.0	806.36	1.9166×10^{-2}
M	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
N	127.993	1.0	6.3	1.0	806.36	1.9166×10^{-2}
O	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
P	127.547	1.0	6.3	1.0	803.546	1.91×10^{-2}
Q	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
R	127.547	1.0	6.3	1.0	803.546	1.91×10^{-2}
S	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}
T	127.993	1.0	6.3	1.0	806.36	1.9166×10^{-2}
U	5.71	1.0	1.0	1.0	5.71	1.3149×10^{-4}

Table D.15 (continued)

DUAL GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION ONE)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^{6}h)	π_Q	π_E	π_L	(F/10^{6}h)	
V	127.993	1.0	6.3	1.0	806.36	1.9166x10^{-2}
W	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
X	127.993	1.0	6.3	1.0	806.36	1.9166x10^{-2}
Y	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
Z	127.993	1.0	6.3	1.0	806.36	1.9166x10^{-2}
AA	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
BB	.155	1.0	6.3	1.0	.9765	1.8747x10^{-4}
CC	67.6135	3.0	6.3	1.0	425.95	1.017x10^{-2}
DD	67.610	3.0	6.3	1.0	425.95	1.017x10^{-2}
EE	.155	1.0	6.3	1.0	.9765	1.8747x10^{-4}
FF	67.610	3.0	6.3	1.0	425.95	1.017x10^{-2}
GG	67.610	3.0	6.3	1.0	425.95	1.017x10^{-2}
LL	223.84	1.0	6.3	1.0	1410.10	3.328x10^{-2}
MM	5.71	1.0	1.0	1.0	5.71	1.3149x10^{-4}
NN						8.997x10^{-4}
NN						8.997x10^{-4}

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
B	Coaxial cable	Global bus 1 fails

C	MMI 1 system	MMI 1 system fails
D	Coaxial cable	Global bus 2 fails
E	MMI 2 system	MMI 2 system fails
F	MC 1 hardware	MC 1 hardware fails
G	MC 1 software	MC 1 software fails
H	µPC3 hardware	µPC3 hardware fails
I	µPC3 software	µPC3 software fails
J	µPC'3 hardware	µPC'3 hardware fails
K	µPC'3 software	µPC'3 software fails
L	µPD3 hardware	µPD3 hardware fails
M	µPD3 software	µPD3 software fails
N	µPD'3 hardware	µPD'3 hardware fails
O	µPD'3 software	µPD'3 software fails
P	µPC7 hardware	µPC7 hardware fails
Q	µPC7 software	µPC7 software fails
R	µPC'7 hardware	µPC'7 hardware fails
S	µPC'7 software	µPC'7 software fails
T	µPD7 hardware	µPD7 hardware fails
U	µPD7 software	µPD7 software fails
V	µPD'7 hardware	µPD'7 hardware fails
W	µPD'7 software	µPD'7 software fails
X	µPD8 hardware	µPD8 hardware fails
Y	µPD8 software	µPD8 software fails
Z	µPD'8 hardware	µPD'8 hardware fails
AA	µPD'8 software	µPD'8 software fails
BB	Switch 7	Switch 7 hardware fails
CC	µPC7 hardware	µPC7 hardware fails (SR)
DD	µPC'7 hardware	µPC'7 hardware fails (SR)
EE	Switch 3	Switch 3 hardware fails
FF	µPC3 hardware (SR)	µPC3 hardware fails (SR)
GG	µPC'3 hardware (SR)	µPC'3 hardware fails (SR)
LL	MC 2 hardware	MC 2 hardware fails
MM	MC 2 software	MC 2 control software fails
NN	Secondary storage 1	Secondary storage 1 fails
OO	Secondary storage 2	Secondary storage 2 fails

PROBABILISTIC EQUATIONS

From the fault tree:

$$\begin{aligned} TE = \; & < B + C + NN + F + G + \{ [H + I] + [J + K + EE + (FF + I) \times \\ & (GG + K)] + [L + M] \times [N + O] \} + \{ \; \} + \{ \; \} + \{ \; \} + \{ \; \} + \\ & \{ \; \} + [P + Q] \times [R + S + BB + (Q + CC) \times (S + DD)] + \\ & [T + U] \times [V + W] + [X + Y] \times [Z + AA] \} > \times < D + E + OO + \end{aligned}$$

$$[F + G] \times [LL + MM] + LL + MM + \Big\{[H + I] \times [J + K + EE + (FF + I) \times (GG + K)] + [L + M] \times [N + O]\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{[P + Q] \times [R + S + BB + (Q + CC) \times (S + DD)] + [T + U] \times [V + W] + [X + Y] \times [Z + AA]\Big\} >$$

By using the boolean laws the equation is reduced to:

$$TE = \Big\{[H + I] \times [J + K + EE + (FF + I) \times (GG + K)] + [L + M] \times [N + O]\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{\quad\Big\} + \Big\{[P + Q] \times [R + S + BB + (Q + CC) \times (S + DD)] + [T + U] \times [V + W] \times [X + Y] \times [Z + AA]\Big\} + [B + C + F + G + NN] \times [D + E + LL + MM + OO]$$

Applying the probabilistics laws:

$TE = F_1 + F_2 + F_3$	$p(TE) = p(F_1) + p(F_2) + p(F_3) - p(F_1)p(F_2)p(F_3) - p(F_1)p(F_2) - p(F_1)p(F_3) - p(F_2)p(F_3)$
$F_1 = F_4$	$p(F_1) = p(F_4)$
$F_4 = F_{18} \times F_{19}$	$p(F_4) = p(F_{18}) \times p(F_{19})$
$F_{18} = B + C + F + G + NN$	$p(F_{18}) = p(B) + p(C) + p(F) + p(G) + p(NN) + p(C)p(F)p(NN) - p(C)p(F) - p(C)p(NN) - p(F)p(NN)$
$F_{19} = D + E + LL + MM + OO$	$p(F_{19}) = p(D) + p(E) + p(LL) + p(MM) + p(OO) + p(E)p(LL)p(OO) - p(E)p(LL) - p(E)p(OO) - p(LL)p(OO)$
$F_2 = F_5 + F_5$	$p(F_2) = 2p(F_5) - p(F_5)^2$
$F_5 = F_6 + F_6 + F_6$	$p(F_5) = 3p(F_6) + p(F_6)^3 - 3p(F_6)^2$
$F_6 = F_7 + F_8$	$p(F_6) = p(F_7) + p(F_8) - p(F_7)p(F_8)$

$$F_7 = (L+M) \times (N+O) \qquad p(F_7) = [p(L) + p(M)] \times [p(N) + p(O)]$$

$$F_8 = (H+I) + F_9 \qquad p(F_8) = [p(H) + p(I)] \times p(F_9)]$$

$$F_9 = F_{10} + F_{11} \qquad p(F_9) = p(F_{10}) + p(F_{11}) - p(F_{10})p(F_{11})$$

$$F_{10} = J + K + E \qquad p(F_{10}) = p(J) + p(K) + p(E) - p(J)p(E)$$

$$F_{11} = (FF+I) \times (GG + K) \qquad p(F_{11}) = [p(FF) + p(I)] \times [p(GG) + p(K)]$$

$$F_3 = F_{12} + F_{13} + F_{14} \qquad p(F_3) = p(F_{12}) + p(F_{13}) + p(F_{13}) + p(F_{12})$$
$$p(F_{13})p(F_{14}) - p(F_{12})p(F_{14}) -$$
$$p(F_{12})p(F_{13}) - p(F_{13})p(F_{14})$$

$$F_{12} = (T+U) \times (V+W) \qquad p(F_{12}) = [p(T) + p(U)] \times [p(V) + p(W)]$$

$$F_{13} = (X+Y) \times (Z+AA) \qquad p(F_{13}) = [p(X) + p(Y)] \times [p(Z) + p(AA)]$$

$$F_{14} = (P+Q) + F_{15} \qquad p(F_{14}) = [p(P) + p(Q)] \times p(F_{15})$$

$$F_{15} = F_{16} + F_{17} \qquad p(F_{15}) = p(F_{16}) + p(F_{17}) - p(F_{16})p(F_{17})$$

$$F_{16} = R + S + BB \qquad p(F_{16}) = p(R) + p(S) + p(BB)$$

$$F_{17} = (Q+CC) \times (S + DD) \qquad p(F_{17}) = [p(Q) + p(CC)] \times [p(S) + p(DD)]$$

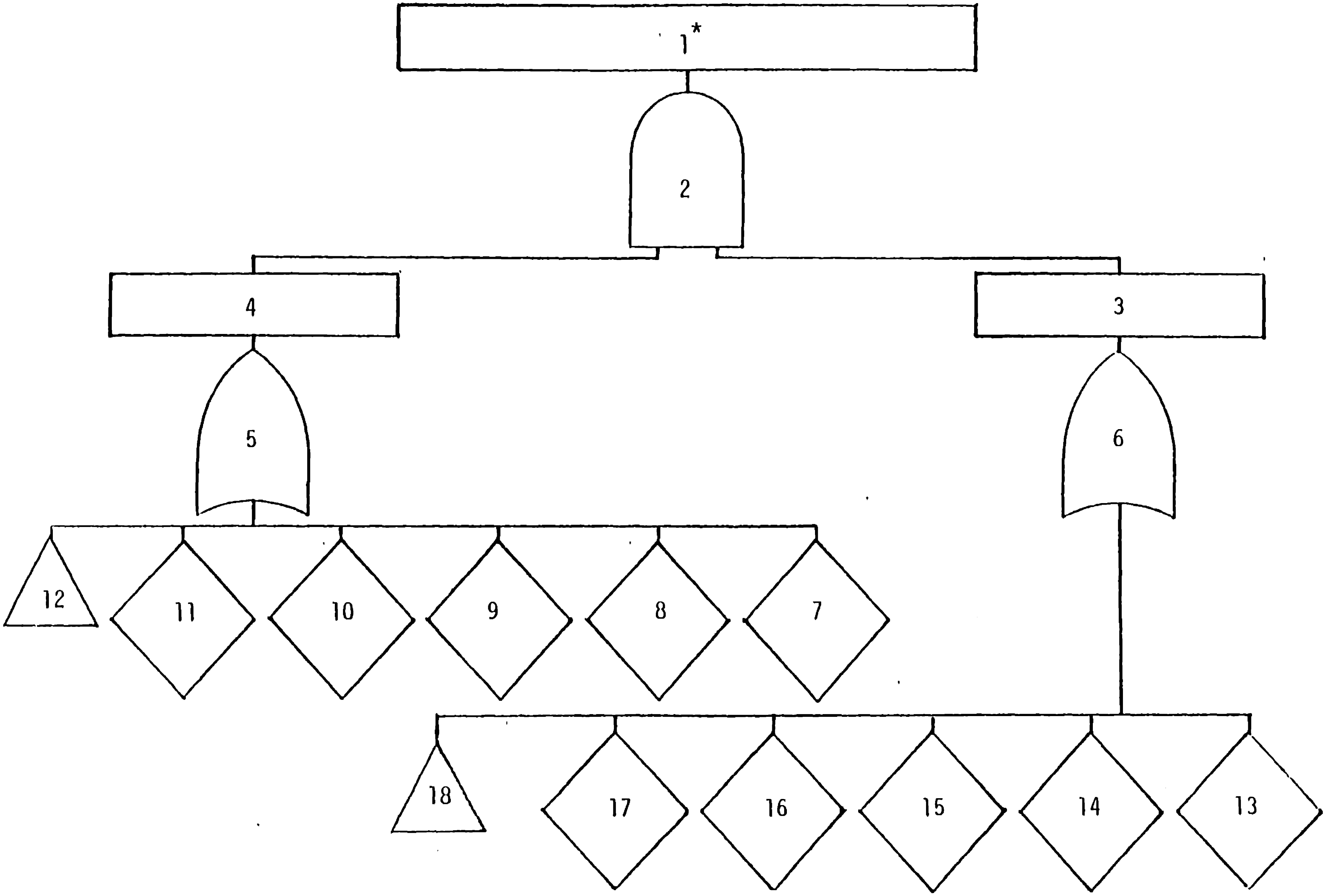


Figure D.16 Dual global bus architecture, situation two.
*See legena on next page.

1. Control system fails to diagnose and to advise the appropriate corrective measures
2. X
3. Standby diagnosis system No. 2 fails
4. Diagnosis system No. 1 on service fails
5. +
6. +
7. NN
8. C
9. B
10. F
11. PP
12. 1
13. OO
14. E
15. D
16. QQ
17. LL
18. 1

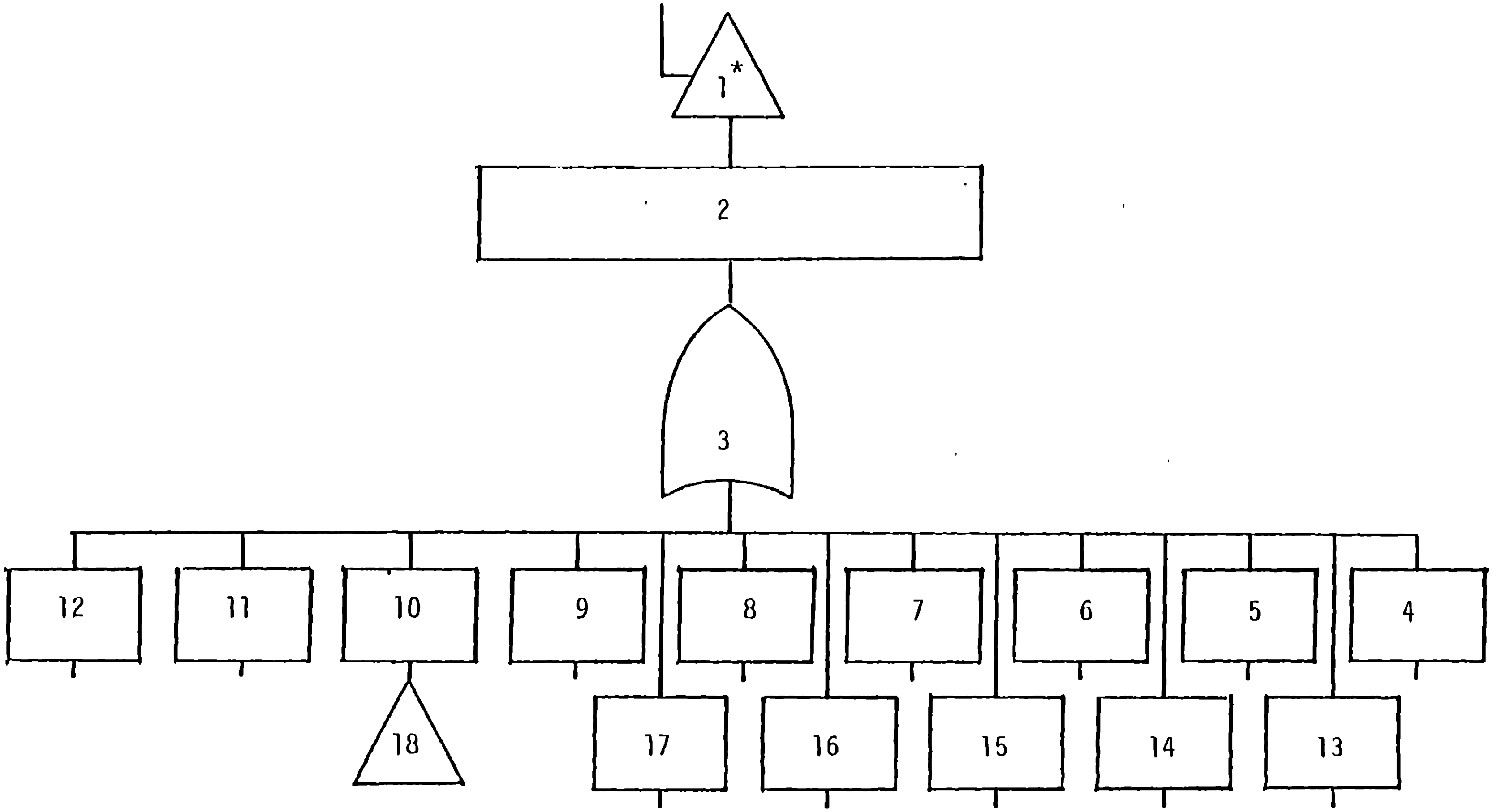


Figure D.16 (continued)

*See legend on next page.

1. 1
2. Distributed digital system fails
3. +
4. Distributed system D_9 fails
5. Distributed system D_8 fails
6. Distributed system D_7 fails
7. Distributed system D_6 fails
8. Distributed system D_5 fails
9. Distributed system D_4 fails
10. Distributed system D_3 fails
11. Distributed system D_2 fails
12. Distributed system D_1 fails
13. Distributed system D_{14} fails
14. Distributed system D_{13} fails
15. Distributed system D_{12} fails
16. Distributed system D_{11} fails
17. Distributed system D_{10} fails
18. 2

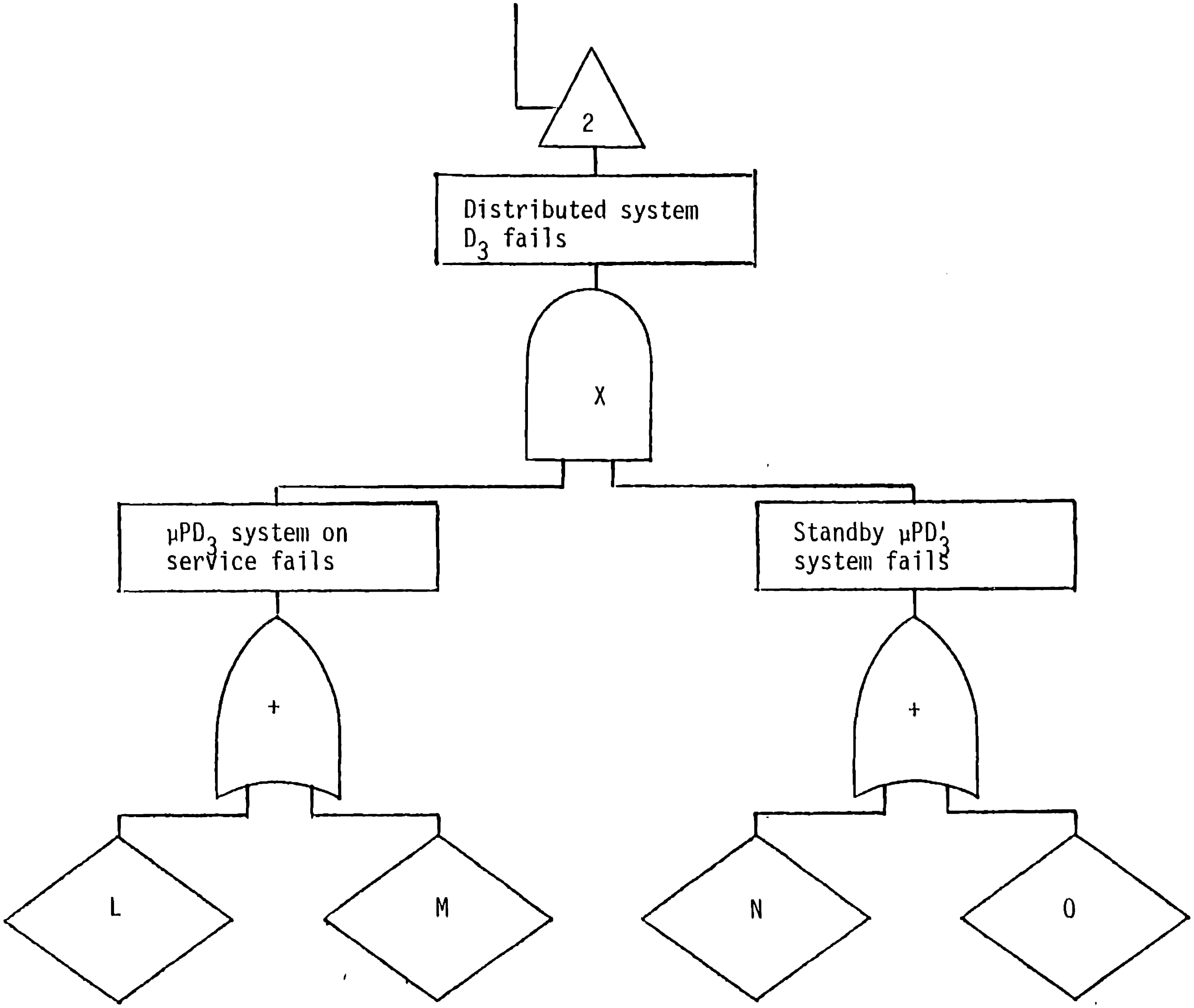

2
Distributed system D_3 fails
X
μPD_3 system on service fails
Standby $\mu PD'_3$ system fails
+
+
L
M
N
O

Figure D.16 (continued)

Table D.16

DUAL GLOBAL BUS ARCHITECTURE SERIAL TRANSMISSION (SITUATION TWO)

EVENT SYMBOL	GENERIC FAILURE RATE (λ_G)	QUALITY FACTOR	ENVIRONMENTAL FACTOR	LEARNING FACTOR	FAILURE RATE (λ)	EVENT PROBABILITY
	(F/10^{6}h)	π_Q	π_E	π_L	(F/10^{6}h)	
NN						$8.997\text{x}10^{-4}$
OO						$8.997\text{x}10^{-4}$
PP	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
QQ	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
LL	127.547	1.0	6.3	1.0	803.546	$1.91\text{x}10^{-2}$
M	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
N	127.547	1.0	6.3	1.0	803.546	$1.91\text{x}10^{-2}$
O	5.71	1.0	1.0	1.0	5.71	$1.3149\text{x}10^{-4}$
B	.06	3.0	1.0	1.0	.18	$4.32\text{x}10^{-6}$
C	173.392	1.0	6.3	1.0	1092	$1.731\text{x}10^{-5}$
F	223.84	1.0	6.3	1.0	1410.19	$3.328\text{x}10^{-2}$
E	173.392	1.0	6.3	1.0	1092	$1.731\text{x}10^{-5}$
LL	223.84	1.0	6.3	1.0	1410.19	$3.328\text{x}10^{-2}$

MEANING OF EVENT SYMBOLS:

EVENT SYMBOL	COMPONENT	EVENT
NN	Secondary storage 1	Secondary storage 1 fails
OO	Secondary storage 2	Secondary storage 2 fails
PP	MC 1 software	MC 1 software fails
QQ	MC 2 software	MC 2 software fails
L	μPD3 hardware	μPD3 hardware fails
M	μPD3 software	μPD3 software fails
N	μPD'3 hardware	μPD'3 hardware fails

O	μPD'3 software	μPD'3 software fails
B	Coaxial cable	Global bus 1 fails
C	MMI 1	MMI 1 system fails
F	MC 1 hardware	MC 1 hardware fails
D	Coaxial cable	Global bus 2 fails
E	MMI2	MMI 2 system fails
LL	MC 2 hardware	MC 2 hardware fails

PROBABILISTIC EQUATIONS

From the corresponding fault tree:

$$\begin{aligned} TE = \Big(&B + C + NN + \Big\{F + PP + [L + M] \times [N + O] + [\ ] + [\ ] + [\ ] + \\ &+ [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + \\ &+ [\ ] + [\ ]\Big\}\Big) \times \Big(D + E + OO + \Big\{LL + QQ + [L + M] \times \\ &[N + O] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + \\ &+ [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ]\Big\}\Big) \end{aligned}$$

Applying boolean laws the equation is reduced to:

$$\begin{aligned} TE = \ &[L + M] \times [N + O] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] \\ &+ [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + [\ ] + \\ &[D + E + OO + LL + QQ] \times [B + C + NN + F + PP] \end{aligned}$$

Applying the probabilistics laws:

$TE = F_1 + F_2$ $\quad$ $p(TE) = p(F_1) + p(F_2) - p(F_1)p(F_2)$

$F_1 = F_3 \times F_4$ $\quad$ $p(F_1) = p(F_3)p(F_4)$

$F_3 = B + C + NN + F + PP$ $\quad$ $p(F_3) = p(B) + p(C) + p(NN) + p(F) + p(PP) +$

$p(C)p(NN)p(F) - p(C)p(F) - p(C)p(NN)$

$- p(NN)p(F)$

$F_4 = D + E + OO + LL + QQ$ $\quad$ $p(F_4) = p(D) + p(E) + p(OO) + P(LL) + P(QQ)$

$p(E)p(OO)p(LL) - p(E)p(OO) - p(E)p(LL)$

$- p(OO)p(LL)$

$F_2 = F_5 + F_5$ $\quad$ $p(F_2) = 2p(F_5) - p(F_5)^2$

$F_5 = F_6 \text{ x } F_7$ $\quad$ $p(F_5) = p(F_6)p(F_7) -p(F_6)p(F_7)$

$F_6 = F_8 \text{ x } F_8$ $\quad$ $p(F_6) = 2p(F_8) - p(F_8)^2$

$F_8 = F_9 + F_9$ $\quad$ $p(F_8) = 2p(F_9) - p(F_9)^2$

$F_7 = F_9 + F_9 + F_9$ $\quad$ $p(F_7) = 3p(F_9) + p(F_9)^3 - 3p(F_9)^2$

$F_9 = (L + M) \text{ x } (N + O)$ $\quad$ $p(F_9) = [p(L) + p(M)] \text{ x } [p(N) + p(O)]$

APPENDIX E

DEBUGGING TIME CALCULATIONS

The theory behind the debugging time calculations has been stated in references E.1 and E.2. In those references it is proved that the expected number of software errors or failures detected at time t is a non-decreasing function of t. Also this expression is a function of the expected total number of errors to be detected until complete and perfect debugging. This expression has the following form:

$$m(t) = a(1 - e^{-bt}) \qquad (E.1)$$

where

$m(t)$ = expected number of errors detected at time t

a = total expected number of errors

b = software parameter characteristic of each program.

The theory has been developed aiming to predict the expected reliability of a program when it has not been completely debugged. In other words, the actual parameters for Eq. (E.1) come from direct observation during the debugging process.

Performing a time derivative on Eq. (E.1)::

$$\frac{dm(t)}{dt} = \hat{B}\ b\ e^{-bt} \qquad (E.2)$$

$a = \hat{B}$, the expected remaining bugs in the program.

$\frac{dm(t)}{dt}$ can be interpreted as the hazard function of the software.

The following step is to assume that the debugging process is done by running the code under study and looking for the errors buried in it. This assumption equates the time variable in Eq. (E.1) with the debugging time.

For a debugging time T_D

$$\left.\frac{dm(t)}{dt}\right]_{t=t_0} = \hat{B}\ b\ e^{-bT_D}$$

making the hazard function a fixed value (at designer will).

$$\left.\frac{dm(t)}{dt}\right]_{t=T_D} = C \qquad (E.3)$$

$$C = \hat{B}\ b\ e^{-bT_D}$$

Solving the equation

$$T_D = -\frac{1}{b}\ln\left(\frac{C}{\hat{B}\ b}\right) \qquad (E.4)$$

In our case the values for $\hat{B}$ come from Table B.2 where the estimated number of errors at the end of programming stage are calculated. The parameter C is fixed value by the designer. Only the parameter b offers difficulties to obtain it, because this is a value which can only be acquired after the real debugging process has been started. This point presents a problem that cannot be accurately solved at this stage of the analysis but from past experiences a general number for b can be assumed.

$b = 7.381 \times 10^{-4}\ [h^{-1}]$

More accurate calculations must wait until the real debugging process is started.

REFERENCES

E.1 A guide book for software reliability assessment. Alan Suckert, Amrit L. Goel. Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, CA, 1980.

E.2 Time dependent error detection rate model for software reliability and other performance measures. A.L. Goel and K. Okumato. IEEE Transactions on Reliability, vol. R-28, no. 3, August 1979, pp. 206-211.

APPENDIX F

SENSITIVITY ANALYSIS

The results of the sensitivity analysis are written in two tables, one for each situation. The first three options in each sitatuion have been chosen for the sensitivity analysis: dual start serial, dual global bus, and dual star parallel in situation one and central computer, global bus, and star serial in situation two.

The parameters (variables) analyzed are the following:

1. Situation One

   cost (C)

   payoff of success (POS)

   probability of μPC hardware failure (P(μPC))

   probability of μPD hardware failure (P(μPD))

   probability of mC hardware failure (P(mC))

   probability of line failure (P(lines))

   time between maintenance (T_{maint})

   probability of software failure (P(soft))

2. Situation One

   cost (C)

   probability of wrong operator intervention (P(OP))

   probability of μPD hardware failure (P(μPD))

   probability of mC hardware failure (P(mC))

   probability of line failure (P(line))

   time between maintenance (T_{maint})

   probability of software failure (P(soft))

The tables show the values of the variables, the corresponding probability of failure for the architecture, and the related EMV. All the numbers are graphically shown in Figures 2.10.1 through 2.10.15.

Table F.1: Sensitivity Analysis: Situation One

	Dual Star Serial			Dual Global Bus		
	Variable	P_f(ACT)	EMVx10^6	Variable	P_f(ACT)	EMVx10^6
Cost	$10.9\text{x}10^6$	.0035	55.865	$10.9\text{x}10^6$	.0068	55.646
	$11.21\text{x}10^6$	.0035	55.553	$11.26\text{x}10^6$	.0068	55.282
	$11.5\text{x}10^6$	.0035	55.265	$11.5\text{x}10^6$	.0068	55.047
P(μPC)	$1.0\text{x}10^6$	.0033	55.566	$1.0\text{x}10^{-2}$	.0049	55.408
	$1.66\text{x}10^{-2}$	.0035	55.553	$1.91\text{x}10^{-2}$	.0068	55.282
	$3.0\text{x}10^{-2}$	.0042	55.507	$3.0\text{x}10^{-2}$	.0107	55.020
P(μPD)	$1.0\text{x}10^{-2}$	.0034	55.567	$1.0\text{x}10^{-2}$	.0046	55.426
	$1.57\text{x}10^{-2}$	.0035	55.553	$1.92\text{x}10^{-2}$	.0067	55.282
	$3.0\text{x}10^{-2}$	.0041	55.512	$3.01\text{x}10^{-2}$	.0011	54.998
P(mC)	$1.0\text{x}10^{-2}$	.0003	55.770	$1.0\text{x}10^{-2}$	.0057	55.352
	$5.10\text{x}10^{-2}$	.0035	55.553	$3.33\text{x}10^{-2}$	.0068	55.282
	$7.0\text{x}10^{-2}$	.006-	55.379	$7.0\text{x}10^{-2}$	.0106	55.025
P(soft)	$1.0\text{x}10^{-5}$	.0034	55.499	$1.0\text{x}10^{-5}$	.0068	55.222
	$1.37\text{x}10^{-4}$	.0035	55.553	$1.37\text{x}10^{-4}$	.0068	55.282
	$1.0\text{x}10^{-3}$	.0035	55.605	$1.0\text{x}10^{-3}$	.0073	55.295
POS	$33.5\text{x}10^6$	.0035	22.171	$33.5\text{x}10^6$	.0067	22.01
	$67\text{x}10^6$	.0003	55.553	$67\text{x}10^6$	.0068	55.282
	$1.0\text{x}10^8$	.0035	88.438	$1\text{x}10^8$	.0068	88.059
P(lines)	0	.0035	55.553	0	.0068	55.282
	$4.32\text{x}10^{-6}$	.0035	55.555	$4.32\text{x}10^{-6}$	.0068	55.282
	$1.0\text{x}10^{-5}$	.0035	55.553	$1.0\text{x}10^{-5}$	.0068	55.282
T(tests)	24(h)	.0035	55.553	24(h)	.0068	55.282
	72(h)	.0037	53.295	72(h)	.0058	51.846
	120(h)	.1136	48.174	120(h)	.1500	45.677

Table F.1: Sensitivity Analysis: Situation One (continued)

Dual Star Parallel

	Variable	P_f(ACT)	EMVx10^6
Cost	10.9×10^6	.0095	55.461
	11.39×10^6	.0095	54.967
	11.5×10^6	.0095	54.861
P(μPC)	1.0×10^{-2}	.0084	55.041
	1.60×10^{-2}	.0095	54.967
	3.0×10^{-2}	.0142	54.654
P(μPD)	1.0×10^{-2}	.0082	55.056
	1.63×10^{-2}	.0095	54.967
	3.0×10^{-2}	.0146	54.679
P(mC)	1.0×10^{-2}	.0044	55.313
	6.37×10^{-2}	.0095	54.967
	9.0×10^{-2}	.0147	54.623
P(soft)	1.0×10^{-5}	.0095	54.906
	1.37×10^{-4}	.0095	55.967
	1.0×10^{-3}	.01	54.987
POS	33.5×10^6	.0095	21.786
	67×10^6	.0095	54.967
	1.0×10^8	.0095	87.652
P(lines)	0	.0095	54.967
	4.32×10^{-6}	.0095	54.967
	1.0×10^{-5}	.0095	54.967
T(tests)	24(h)	.0095	54.967
	72(h)	.0079	50.341
	120(h)	.1944	42.579

Table F.2: Sensitivity Analysis: Situation Two

	Central			Global Bus		
	Variable	P_f(ACT)	EMVx10^6	Variable	P_f(ACT)	EMVx10^6
Cost	10.8x10^6	.177	-10.93	10.8x10^6	.0037	-10.83
	10.91x10^6	.177	-11.05	11.04x10^6	.0037-	-11.07
	11.3x10^6	.177	-11.43	11.3x10^6	.0037	-11.33
P(op)	0.01	.177	-10.95	0.01	.0037	-11.05
	0.039	.177	-11.05	0.039	.0037	-11.07
	0.1	.177	-11.25	0.1	.0037	-11.11
P(µPD)				1.0x10^{-2}	.0036	-11.067
				1.45x10^{-2}		-11.068
				3.0x10^{-2}	.0465	-11.075
P(mC)	0.1	.105	-10.99	1.0x10^{-2}	.014	-11.051
	0.172	.177	-11.05	3.33x10^{-2}	.037	-11.068
	0.3	.304	-11.14	7.0x10^{-2}	.073	-11.095
P(lines)	5.0x10^{-4}	.173	-11.04	0	.037	-11.068
	4.69x10^{-3}	.177	-11.05	4.32x10^{-6}	.037	-11.068
	5.0x10^{-2}	.2141	-11.07	1.0x10^{-5}	.037	-11.068
P(soft)	1.0x10^{-5}	.176	-11.11	1.0x10^{-5}	.0370	-11.134
	1.31x10^{-4}	.177	-11.05	1.31x10^{-4}	.0372	-11.018
	1.0x10^{-3}	.177	-10.99	1.0x10^{-3}	.0383	-11.068
T(tests)	24(h)	.177	-11.05	24(h)	.0372	-11.068
	72(h)	.445	-11.24	72(h)	.1274	-11.135
	120(h)	.628	-11.38	120(h)	.2313	-11.212

Table F.2: Sensitivity Analysis: Situation One (continued)

Star Serial

	Variable	P_f(ACT)	EMVx10^6
Cost	10.	.0514	-10.84
	11.07	.0514	-11.11
	11.3x10^6	.0514	-11.34
P(op)	0.01	.0514	-11.08
	0.039	.0514	-11.11
	0.1	.0514	-11.16
P(μPD)	1.0x10^{-2}	.0506	-11.06
	1.26x10^{-2}	.0514	-11.06
	3.0x10^{-2}	.0613	-11.114
P(mC)	1.0x10^{-2}	.0133	-11.078
	4.8x10^{-2}	.0514	-11.107
	7.0x10^{-2}	.073	-11.123
P(lines)	0	.0514	-11.107
	4.32x10^{-6}	.0514	-11.107
	1.0x10^{-5}	.0514	-11.107
P(soft)	1.0x10^{-5}	.051	-11.172
	1.31x10^{-4}		-11.107
	1.0x10^{-3}	.052	-11.056
T(test)	24(h)	.0514	-11.107
	72(h)	.162	-11.189
	120(h)	.277	-11.273

APPENDIX G

STATE EQUATIONS FOR THE QUASI STEADY STATE CONDITION

The basic equations to start the process of obtaining the state equations are:

$$\dot{M}_s = w_{fl} - w_c \qquad (3.3.11)$$

$$\dot{M}_w = w_{sp} + w_c + w_{su} - w_{fl} \qquad (3.3.12)$$

$$\dot{U}_s = w_{fl}\ h_{fl} - w_c h_s - P\dot{V}_s \qquad (3.3.13)$$

$$\dot{U}_w = w_{su} h_{su} \overset{+}{c} w_c h_c + w_{sp} h_c - w_{fl} h_{fl} + Q_h - P\dot{V}_w \qquad (3.3.23)$$

$$w_{sp} h_{sp} + w_c h_s = w_c h_c + w_{sp} h_c \qquad (3.3.19)$$

$$\dot{V}_w + \dot{V}_s = 0 \qquad (3.3.17)$$

By definition

$$\dot{U}_w = \dot{H}_s - P\dot{V}_s - \dot{P}V_s$$

Substituting (3.3.13) into the defnition

$$\dot{H}_s - P\dot{V}_s - \dot{P}V_s = w_{fl} h_{fl} - w_c h_s - \dot{P}V_s$$

cancelling equal terms

$$\dot{H}_s = w_{fl} h_{fl} - w_c h_s + P\dot{V}_s \qquad (G.1)$$

Also by definition

$$\dot{H}_s = \dot{M}_s h_s + M_s \dot{h}_s$$

Substituting the definition into (G.1)

$$\dot{M}_s h_s + M_s \dot{h}_s = w_{fl} h_{fl} - w_c h_s + \dot{P} V_s$$

Substituting (3.3.11) into the former equation

$$(w_{fl} - w_c) h_s + M_s \dot{h}_s = w_{fl} h_{fl} - w_c h_s + \dot{P} V_s$$

$$M_s \dot{h}_s = w_{fl} h_{fl} - w_c h_s + w_c h_s - w_{fl} h_s + \dot{P} V_s$$

$$M_s \dot{h}_s = w_{fl}(h_{fl} - h_s) + \dot{P} M_s v_s \tag{G.2}$$

Also by definition

$$\dot{U}_w = \dot{H}_w - P\dot{V}_w - \dot{P} V_w$$

Substituting the definition into (G.1)

$$\dot{H}_w - P\dot{V}_w - \dot{P} V_w = w_{su} h_{su} + w_c h_c + w_{sp} h_c - w_{fl} h_{fl} + Q_h - P\dot{V}_w$$

$$\dot{H}_w = w_{su} h_{su} + (w_c + w_{sp}) h_c + Q_h - w_{fl} h_{gl} + \dot{P} V_w \tag{G.3}$$

By definition

$$\dot{H}_w = \dot{M}_w h_w + M_w \dot{h}_w$$

Substituting the definition into (G.3)

$$\dot{M}_w h_w + M_w \dot{h}_w = w_{su} h_{su} + (w_{sp} + w_c) h_c + Q_h - w_{fl} h_{fl} + \dot{P} V_w$$

Substituting (3.3.12) into the former equation

$$h_w (w_{sp} + w_c + w_{su} - w_{fl}) + M_w \dot{h}_w =$$

$$w_{su} h_{su} + (w_{sp} + w_c) h_c + Q\ _h - w_{fl} h_{fl} + \dot{P} V_w$$

$$M_w \dot{h}_w = w_{su} h_{su} + (w_{sp} + w_c) h_c + Q_h - w_{fl} h_{fl} + \dot{P} V_w$$

$$- (w_{sp} + w_c + w_{su} - w_{fl}) h_w \qquad \text{(G.4)}$$

Taking equation (3.3.17) and developing it:

$$M_s \dot{v}_s + \dot{M}_s v_s + M_w \dot{v}_w + \dot{M}_w v_w$$

Substituting (3.3.11) and (3.3.12) into the former equation

$$M_s \dot{v}_s + \dot{M}_w v_w + (w_{fl} - w_c) v_s + (w_{sp} + w_c + w_{su} - w_{fl}) v_w = 0 \qquad \text{(G.5)}$$

The general case is:

$$v_s = v_s(h_s, P)$$

$$v_w = v_w(h_w, P)$$

Taking the derivative of the expressions

$$\dot{v}_s = \frac{\partial v_s}{\partial h_s} \dot{h}_s + \frac{\partial v_s}{\partial P} \dot{P}$$

$$\dot{v}_w = \frac{\partial v_w}{\partial h_w} \dot{h}_s + \frac{\partial v_w}{\partial P} \dot{P}$$

Substituting the former derivatives into (G.5)

$$M_s[\frac{\partial v_s}{\partial h_s}\dot{h}_s + \frac{\partial v_s}{\partial P}\dot{P}] + M_w[\frac{\partial v_w}{\partial h_w}\dot{h}_w + \frac{\partial v_w}{\partial P}\dot{P}] =$$

$$- (w_{f1} - w_c)v_s - (w_{sp} - w_c + w_{su} - w_{f1})v_w \qquad (G.6)$$

Substituting (G.2) and (G.4) into (G.6)

$$\frac{\partial v_s}{\partial h_s}[w_{f1}(h_{f1} - h_s) + \dot{P}M_s v_s] + M_s\frac{\partial v_s}{\partial P}\dot{P} + v_w\frac{\partial v_w}{\partial P}\dot{P} +$$

$$\frac{\partial v_s}{\partial h_w}[w_{su}h_{su} + (w_{sp} + w_c)h_c + Q_h - w_{f1}h_{f1} + \dot{P}V_w$$

$$- (w_{sp} + w_c + w_{su} - w_{f1})h_w] = - (w_{f1} - w_c)v_s$$

$$- (w_{sp} + w_c + w_{su} - w_{f1})v_w$$

At this point the quasi steady state assumptions are applied.

$h_s \simeq h_{f1} \simeq h_g(P)$

$h_c \simeq h_w \simeq h_f(P) \qquad\qquad w_{f1} \simeq Q_h/h_{fg}$

$$\dot{P}\frac{\partial v_s}{\partial h_g}M_{-g}v_g + M_g\frac{\partial v_g}{\partial P}\dot{P} + M_f\frac{\partial v_f}{\partial P}\dot{P} + \frac{\partial v_f}{\partial h_f}[w_{su}h_{su} + (w_{sp} + w_c)h_f$$

$$+ \dot{P}V_w - (w_{sp} + w_c + w_{su} - w_{f1})h_f + Q_h - w_{f1}h_g] =$$

$$- (w_{f1} - w_c)v_g - w_{sp} + w_c + w_{su} - w_{f1})v_f$$

$$\dot{P}[M_g(\frac{\partial v_g}{\partial h_g}v_g + \frac{\partial v_g}{\partial P}) + M_f(\frac{\partial v_f}{\partial h_f}V_f + \frac{\partial v_f}{\partial P})]$$

$$- (w_{f1} - w_c)v_g - (w_{sp} + w_c + w_{su} - w_{f1})v_f -$$

$$- \frac{\partial v_f}{\partial h_f} [w_{su}(h_{su} - h_f) + w_{fl} h_f - w_{fl} h_g + Q_h]$$

Noting that

$$- w_{fl} h_f - w_{fl} h_g = w_{fl}(h_f - h_g) = - w_{fl} h_{fg}$$

the final equation is

$$\dot{P} = \frac{-(w_{fl}-w_c)v_g-(w_{sp}+w_c+w_{su}-w_{fl})v_f - \frac{\partial v_f}{\partial h_f} w_{su}(h_{su}-h_f)}{M_g(\frac{\partial v_g}{\partial h_g} v_g + \frac{\partial v_g}{\partial P}) + M_f(\frac{\partial v_f}{\partial h_f} v_f + \frac{\partial v_f}{\partial P})} \qquad (G.7)$$

Equation (G.7) is the quasi steady state model for the pressure in the pressurizer.

APPENDIX H

CONTROL SYSTEM SIMULATION PROGRAM

The code simulates the behavior of the pressure and level in the N.S. Savannah pressurizer. Although only the pressure and the level appear in the print sequence, with minor changes it is possible to call a different couple of variables and print them. The code has been writtein in AOS, which is the appropriate language for T5-58 and T5-59 programmable calculators. This code only fits in the T5-59 calculator.

The inputs to the code are divided into two groups:

1. Inputs directly to memory registers
2. Inputs directly to program locations. The meaning of each input and its location is given in Table H.1.

Also the code uses 30 numerical registers, leaving the remaining as program memory locations. This means that the memory partition is 719.29.

Because of the code size, no automatic stop feature has been added, that is, the code has to be started and stopped by hand. The most practical way to stop the code is to press the R/S key immediately after the print sequence has finished. If the code has to be restarted press GTO 478, R/S.

Every set point for the pressurizer control system can be changed at the programmer's will. Table H.2 shows the set points and their locations. Table H.3 has the step-by-step sequence for using the code; and finally Table H.4 displays the code listings.

Table H.1

INPUTS TO THE PROGRAM

Inputs to Memory Registers

Variable	Register Number	Value
$P(k)$	10	11.93
$M_f(k)$	11	1152.992
$M_g(k)$	12	180.7521
$L(k-1)$	14	0.69
$h_w(k)$	17	1489.13
$P(k-1)$	21	11.93

Note: Every other register is initiated with 0 value.

Inputs to Code Locations

Variable	Value	Code Locations
K_{let}	14.0	076; 077
K_{mak}	18.0	098; 099
w_p		118; 119; 120; 121
K_Q	76	211; 212
K_{sp}	12	270; 271; 272
h_{sp}	1134	327; 328; 329; 330
$\tau x \ w_{su}(\text{max})$	78	370; 371
h_{su}	1184	444; 445; 446; 447
K_1	1.	688; 689
K_2	0.	699; 700
K_3	10	668; 669

Table H.1 (continued)

INPUTS TO THE PROGRAM

Note: As far as the code concerns (see notation, Chapter 3)

$$K_{let} = K^m \times K_{let}$$
$$K_{mak} = K^m \times K_{mak}$$
$$K_Q = K^m \times K_Q$$
$$K_{sp} = K^m \times K_{sp}$$

Table H.2

SET POINTS LOCATIONS

Variable	Value	Program Location
$E_L(k)_{ref}$	4.3608	013;014;015;016;017;018
$E_p(k)_{ref}$	8.864	148;149;150;151;152
$e_p(k)_{ref}$(sprays)	.13	164;165;166;167
$E_c(o)$(sprays)	.032	178;179;180;181
$E_p(Q_h)$max	8.96	231;232;233;234
$E_p(Q_h)$min	8.8	241;242;243
$L_{ref}/1.48$	.4992	419;420;421;422;423

Note: Because of the calculator low memory capacity the back-up heaters have been lumped in one group, starting its action at $E_p(Q_h)$min, and stopping its action at $E_p(Q_h)$max.

Table H.3

USERS MANUAL

	Comments	Key Sequence
1.	Turn calculator and printer on	
2.	Input memory partition	3, 2nd OP 17
3.	Load program (either by hand or using magnetic cards)	
4.	Input initial data (Tables H.1, H.2)	
5.	Start program	RST; R/S
6.	Stop program	R/S
7.	Restart program	GTO 478, R/S

Note: If the user wants to change a value during execution, he should wait until next print sequence is done and stop it by pressing R/S. Then he can change to the desired value and restart the program.

Table H.4

Control System Simulation Code

```
000  00   0
001  42  STO
002  22   22
003  32  X:T
004  02   2
005  42  STO
006  26   26
007  03   3
008  42  STO
009  27   27
010  04   4
011  42  STO
012  28   28
013  04   4
014  93   .
015  03   3
016  06   6
017  00   0
018  08   8
019  75   -
020  06   6
021  93   .
022  03   3
023  02   2
024  65   x
025  43  RCL
026  14   14
027  95   =
028  71  SBR
029  33  X²
030  43  RCL
031  02   02
032  77   GE
033  00   00
034  56   56
035  43  RCL
036  29   29
037  44  SUM
038  09   09
039  43  RCL
040  08   08
041  32  X:T
042  77   GE
043  00   00
044  51   51
045  43  RCL
046  29   29
047  44  SUM
048  08   08
049  61  GTO
050  23  LNX
051  00   0
052  42  STO
053  08   08
054  61  GTO
055  23  LNX
056  43  RCL
057  29   29
058  44  SUM
059  08   08
060  43  RCL
061  09   09
062  77   GE
063  00   00
064  71   71
065  43  RCL
066  29   29
067  44  SUM
068  09   09
069  61  GTO
070  23  LNX
071  00   0
072  42  STO
073  09   09
074  76  LBL
075  23  LNX
076  00   0
077  00   0
078  65   x
079  43  RCL
080  09   09
081  95   =
082  94  +/-
083  42  STO
084  26   26
085  09   9
086  42  STO
087  13   13
088  01   1
089  93   .
090  03   3
091  71  SBR
092  34  √X
093  43  RCL
094  26   26
095  94  +/-
096  42  STO
097  20   20
098  01   1
099  08   8
100  65   x
101  43  RCL
102  08   08
103  95   =
104  42  STO
105  26   26
106  08   8
107  42  STO
108  13   13
109  03   3
110  93   .
111  09   9
112  71  SBR
113  34  √X
114  43  RCL
115  26   26
116  44  SUM
117  20   20
118  00   0
119  00   0
120  00   0
121  00   0
122  44  SUM
123  20   20
124  01   1
125  42  STO
126  22   22
127  05   5
128  42  STO
129  26   26
130  06   6
131  42  STO
132  27   27
133  07   7
134  42  STO
135  28   28
136  93   .
137  07   7
138  04   4
139  03   3
140  65   x
```

Table H.4 (continued)

```
141   43  RCL
142   21   21
143   95   =
144   42  STO
145   14   14
146   94  +/-
147   85   +
148   08   8
149   93   .
150   08   8
151   06   6
152   04   4
153   95   =
154   71  SBR
155   33  X²
156   00   0
157   32  X:T
158   43  RCL
159   05   05
160   77   GE
161   02   02
162   01   01
163   32  X:T
164   93   .
165   01   1
166   03   3
167   94  +/-
168   77   GE
169   01   01
170   78   78
171   00   0
172   32  X:T
173   43  RCL
174   19   19
175   77   GE
176   01   01
177   91   91
178   93   .
179   00   0
180   03   3
181   02   2
182   44  SUM
183   29   29
184   43  RCL
185   29   29
186   44  SUM
187   19   19
188   61  GTO
189   01   01
190   94   94
191   00   L
192   42  STL
193   19   19
194   00   0
195   32  X:T
196   43  RCL
197   18   18
198   77   GE
199   02   02
200   08   08
201   43  RCL
202   29   29
203   44  SUM
204   18   18
205   61  GTO
206   02   02
207   11   11
208   00   0
209   42  STO
210   18   18
211   07   7
212   06   6
213   65   ×
214   43  RCL
215   18   18
216   95   =
217   42  STO
218   26   26
219   01   1
220   08   8
221   42  STO
222   13   13
223   01   1
224   07   7
225   71  SBR
226   34  √X
227   43  RCL
228   26   26
229   42  STO
230   21   21
231   08   8
232   93   .
233   09   9
234   06   6
235   32  X:T
236   43  RCL
237   14   14
238   77   GE
239   02   02
240   59   59
241   08   8
242   93   .
243   08   8
244   01   1
245   32  X:T
246   43  RCL
247   14   14
248   77   GE
249   02   02
250   62   62
251   02   2
252   00   0
253   06   6
254   42  STO
255   16   16
256   61  GTO
257   02   02
258   62   62
259   00   0
260   42  STO
261   16   16
262   43  RCL
263   16   16
264   44  SUM
265   21   21
266   43  RCL
267   21   21
268   42  STO
269   15   15
270   01   1
271   02   2
272   93   .
273   65   ×
274   43  RCL
275   19   19
276   95   =
277   94  +/-
278   42  STO
279   26   26
280   01   1
281   09   9
```

Table H.4 (continued)

282	42	STO
283	13	13
284	02	2
285	93	.
286	06	6
287	71	SBR
288	34	√X
289	43	RCL
290	26	26
291	42	STO
292	13	13
293	01	1
294	52	EE
295	03	3
296	85	+
297	04	4
298	01	1
299	65	×
300	43	RCL
301	10	10
302	95	=
303	42	STO
304	29	29
305	01	1
306	09	9
307	04	4
308	00	0
309	75	-
310	06	6
311	02	2
312	65	×
313	43	RCL
314	10	10
315	95	=
316	35	1/X
317	42	STO
318	28	28
319	65	×
320	43	RCL
321	13	13
322	65	×
323	53	(
324	43	RCL
325	29	29
326	75	-
327	01	1
328	01	1
329	03	3
330	04	4
331	54	)
332	95	=
333	42	STO
334	23	23
335	00	0
336	42	STO
337	25	25
338	43	RCL
339	17	17
340	75	-
341	43	RCL
342	29	29
343	95	=
344	50	I×I
345	42	STO
346	27	27
347	32	X⇌T
348	02	2
349	77	GE
350	03	03
351	81	81
352	43	RCL
353	17	17
354	32	X⇌T
355	43	RCL
356	29	29
357	77	GE
358	03	03
359	91	91
360	00	0
361	32	X⇌T
362	43	RCL
363	20	20
364	77	GE
365	03	03
366	91	91
367	94	+/-
368	65	×
369	43	RCL
370	27	27
371	65	×
372	43	RCL
373	11	11
374	55	÷
375	07	7
376	08	8
377	95	=
378	61	GTO
379	03	03
380	83	83
381	43	RCL
382	21	21
383	22	INV
384	44	SUM
385	15	15
386	65	×
387	43	RCL
388	28	28
389	95	=
390	42	STO
391	25	25
392	53	(
393	01	1
394	00	0
395	06	6
396	85	+
397	03	3
398	93	.
399	09	9
400	01	1
401	65	×
402	43	RCL
403	10	10
404	42	STO
405	21	21
406	54	)
407	65	×
408	01	1
409	52	EE
410	05	5
411	94	+/-
412	95	=
413	42	STO
414	26	26
415	65	×
416	43	RCL
417	11	11
418	55	÷
419	01	1
420	93	.
421	04	4
422	08	8

Table H.4 (continued)

```
423  75   -
424  93   .
425  04   4
426  09   9
427  09   9
428  02   2
429  95   =
430  42  STO
431  14   14
432  43  RCL
433  20   20
434  44  SUM
435  13   13
436  77   GE
437  04   04
438  44   44
439  43  RCL
440  29   29
441  61  GTO
442  04   04
443  48   48
444  01   1
445  01   1
446  08   8
447  04   4
448  75   -
449  43  RCL
450  29   29
451  95   =
452  65   ×
453  43  RCL
454  20   20
455  95   =
456  42  STO
457  20   20
458  44  SUM
459  15   15
460  43  RCL
461  24   24
462  32  X:T
463  43  RCL
464  24   24
465  59  INT
466  22  INV
467  67   EQ
468  04   04
469  78   78
470  43  RCL
471  10   10
472  99  PRT
473  43  RCL
474  14   14
475  99  PRT
476  32  X:T
477  99  PRT
478  53   (
479  53   (
480  43  RCL
481  23   23
482  75   -
483  43  RCL
484  25   25
485  54   )
486  65   ×
487  53   (
488  03   3
489  03   3
490  05   5
491  75   -
492  01   1
493  06   6
494  65   ×
495  43  RCL
496  10   10
497  54   )
498  65   ×
499  01   1
500  52  EE
501  02   2
502  75   -
503  53   (
504  43  RCL
505  13   13
506  85   +
507  43  RCL
508  23   23
509  75   -
510  43  RCL
511  25   25
512  54   )
513  65   ×
514  43  RCL
515  26   26
516  65   ×
517  01   1
518  52  EE
519  06   6
520  75   -
521  53   (
522  01   1
523  00   0
524  05   5
525  65   ×
526  43  RCL
527  10   10
528  75   -
529  01   1
530  05   5
531  07   7
532  54   )
533  65   ×
534  43  RCL
535  20   20
536  65   ×
537  01   1
538  52  EE
539  03   3
540  94  +/-
541  54   )
542  55   ÷
543  53   (
544  43  RCL
545  12   12
546  65   ×
547  53   (
548  02   2
549  93   .
550  04   4
551  08   8
552  65   ×
553  43  RCL
554  10   10
555  33  X²
556  85   +
557  01   1
558  01   1
559  02   2
560  65   ×
561  43  RCL
562  10   10
563  75   -
```

Table H.4 (continued)

564	02	2
565	07	7
566	08	8
567	00	0
568	54	)
569	85	+
570	43	RCL
571	11	11
572	22	INV
573	49	PRD
574	15	15
575	65	×
576	53	(
577	43	RCL
578	10	10
579	33	X²
580	55	÷
581	02	2
582	04	4
583	04	4
584	75	-
585	93	.
586	07	7
587	02	2
588	05	5
589	65	×
590	43	RCL
591	10	10
592	85	+
593	04	4
594	93	.
595	00	0
596	08	8
597	54	)
598	54	)
599	95	=
600	55	÷
601	04	4
602	95	=
603	44	SUM
604	10	10
605	43	RCL
606	15	15
607	55	÷
608	04	4
609	95	=
610	44	SUM
611	17	17
612	43	RCL
613	25	25
614	75	-
615	43	RCL
616	23	23
617	95	=
618	55	÷
619	04	4
620	95	=
621	44	SUM
622	12	12
623	94	+/-
624	85	+
625	43	RCL
626	13	13
627	95	=
628	55	÷
629	04	4
630	95	=
631	44	SUM
632	11	11
633	93	.
634	02	2
635	05	5
636	44	SUM
637	24	24
638	81	RST
639	76	LBL
640	34	ΓX
641	42	STO
642	25	25
643	32	X:T
644	43	RCL
645	26	26
646	77	GE
647	06	06
648	52	52
649	61	GTO
650	06	06
651	61	61
652	43	RCL
653	25	25
654	42	STO
655	26	26
656	43	RCL
657	29	29
658	94	+/-
659	74	SM*
660	13	13
661	92	RTN
662	76	LBL
663	33	X²
664	42	STO
665	25	25
666	04	4
667	65	×
668	01	1
669	00	0
670	65	×
671	53	(
672	73	RC*
673	27	27
674	72	ST*
675	28	28
676	75	-
677	73	RC*
678	26	26
679	72	ST*
680	27	27
681	65	×
682	02	2
683	85	+
684	43	RCL
685	25	25
686	54	)
687	85	+
688	01	1
689	93	.
690	65	×
691	53	(
692	43	RCL
693	25	25
694	75	-
695	73	RC*
696	27	27
697	54	)
698	85	+
699	00	0
700	00	0
701	55	÷
702	04	4
703	65	×
704	43	RCL

Table H.4 (continued)

```
705   25   25
706   72  ST*
707   26   26
708   95   =
709   74  SM*
710   22   22
711   73  RC*
712   22   22
713   55   ÷
714   04   4
715   95   =
716   42  STO
717   29   29
718   92  RTN
719   00   0
```

APPENDIX I

DETAILED DESCRIPTION OF THE N.S. SAVANNAH PRESSURIZER

VESSEL

The pressurizer (Fig. J-1) is a vertical, cylindrical vessel with hemispherical heads at both ends.

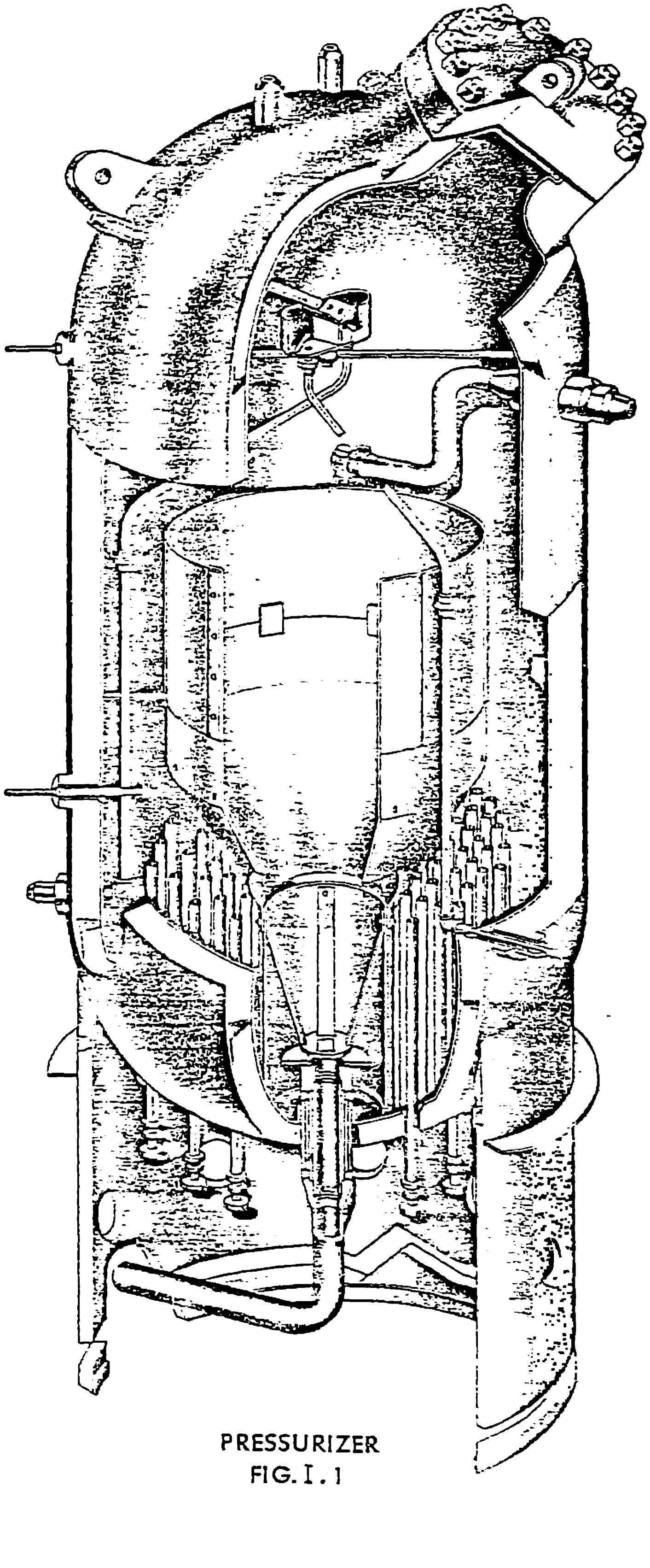
The base material is Type SA-212, Grade B carbon steel and clad with .109" thick SA-240, Grade S Stainless Steel.

The upper head is a 4'-6" I.D. hemispherical head and contains a 15" opening for the manway, two 2" penetrations for safety valve connections, a 1" penetration for the pressure transmitted connection and a 1" penetration for the vent connection. Welded to the outside of this upper head also are three 2" thick lifting lugs, material U.S.C.G. 51.04, Grade D carbon steel.

The cylindrical section is a 4 I.D. vessel with 3-5/8" thick SA-212 Grade B carbon steel walls and a .109" thick SA-240 Grade S stainless steel cladding. Welded internally also are four platform support lugs, material SA-240, Grade S. There are welded interally three stabilizer support bars, material SA-240, Grade for supporting the surge chamber.

There are two 1-1/2" penetrations in this section for the temperature sensing wells, two 1" penetrations for water level indicator connections and a 2" penetration for the spray nozzle.

The lower head is also a 4'6" I.D. hemispherical head, material Type SA-212, Grade B, carbon steel, 2-7/8" thick SA-240, Grade S, stainless steel cladding. This lower head contains 160 penetratons, 1.295" I.D. on



PRESSURIZER
FIG. I. 1

3" triangular pitch. There is also a 6-3/4" I.D. penetration in the lower head for the 4" insurge-outsurge nozzle.

INTERNALS

The vessel internals consist of the in-spray piping, in-spray nozzle, upper surge chamber, lower surge chamber, in-surge, out-surge baffle plate stand pipe assembly and 160 heater wells containing the electric heaters.

IN-SURGE, OUT-SURGE

This nozzle serves the dual function of both and in-surge and out-surge connection and is fitted with a thermal sleeve, with slots cut in the sleeve for drainage. In addition a baffle plate is welded to the end of the surge nozzle inside the vessel. Primary water enters and leaves this nozzle vertically and the flow is directed by means of the control surge chamber.

STAND PIPE ASSEMBLY

The function of this assumption is to aid in measuring the pressurizer water level. This assembly provides the constant reference level from which changes in pressurizer water level are measured and recorded. This assembly consists of 1" Schedule 40 SA-312 pipe connected to the trasmitter nozzle in the upper head, terminating with an open end above the reservoir cup. This reservoir cup is connected by means of two 3/8" schedule 80 SA-212 pipes to the two level indicator connections in the cylindrical section. The cup is supported by the spider, consisting of four 3/4" schedule 40, SA-312 pipes.

IN-SPRAY

Primary water also enters the spray nozzle located in the upper shell section and flows through the stainless steel 1-1/4" Schedule 160 spray piping to the spray distribution nozzle located in the center of the upper part of the vessel. This spray distribution nozzle has a spray angle of 45° designed so that the spray will not impinge on the vessel walls at normal water level or operating conditions. The spray distribution nozzle is screwed to the spray line.

The spray distribution nozzle is of the cone, hollow type with pipe threads and locking clip welded to the nozzle and pipe to prevent rotation. The spray distribution nozzle directs the water in such a manner as to condense the steam in the upper portion of the vessel. The spray nozzle is fitted with a thermal sleeve designed to protect the vessel from temperature fluctuations of the incoming fluid. The spray internal piping is welded to the spray nozzle.

SURGE CHAMBER

The surge chamber is essentially a cone-shaped baffle made up of an upper and lower section with an internal volume of 26 cubic feet. The surge chamber is supported at the top by three stabilizer bars. These stabilizer bars are made of stainless steel, SA-24-, Grade S, welded to the inside of the vessel shell and bolted to the upper section of the surge chamber. The upper part of the upper section is cylindrical, 36" O.D., material SA-240, Grade S, 1-1/4" thick plate. There are three 3/8" x 5/8" slotted holes, 120° apart for bolting to the stabilizer bars and twelve 1" diameter drilled holes. The lower part of this upper section is conical with a 14-1/32" I.D. at the bottom. The lower section is cylindrical and is bolted to the upper section with four stainless steel nuts and bolts. The lower section terminates on and is supported by means of four support angles, located 90° apart, material SA-240 Grade S which are welded to the bottom head.

PLATFORM SUPPORTS

Welded to the cylindrical section of the vessel are four platform supports for maintenance, repair and inspection. These supports are located 90° apart and are made of SA-240 Grade S, 2-1/2" x 1" x 3".

ELECTRIC HEATERS

The cartridge type, electric heating elements are designed for vertical insertion into the walls provided in the pressurizer lower head wall. The electric heaters are provided with electrical terminals for connection to a power source that equals the heating rating.

The tubular pressurizer heaters will operate at 110 volts and are connected four in series across a 440 volt supply. Each heater is rated at 40 watts per square inch of heated sheath surface and have an outside diameter of 0.553" with an effective heating length of 20 inches. The heaters are enclosed by heater wells which extend vertically into the lower part of the vessel by means of stainless steel transition sleeves. The heaters are held within the heater walls by means of mechanical pressure seals which also serve as back-up well closures in the event of heater well failure. They are mounted on a 3" triangular pitch in order to provide for attachment of heater terminal box assemblies to the vessel.

The heater wells totally enclose the replaceable electric heaters. The internal end of the heater wells are sealed by means of a welded plug and externally by means of a mechanical pressure seal welded to the end.

The heater wells have an I.D. of 0.570" and are designed for 2015 psia external pressure and 900°F. The transition sleeve for the heater well is welded to the heater well externally and to the vessel internally.

Heater well mechanical seals consisting of a nut and ferrule are provided for each heater. They provide a high pressure seal between the heater and the heater well on the external end of the well. The seal retains the heater in position and prevents leakage in the event of well failure from 637°F and 2015 psia.

NOZZLES

The pressurizer vessel is fitted with a total of ten nozzles.

The following nozzles are located in the upper hemispherical head:

- One 15" I.D. manway nozzle forging, carbon steel, U.S.C.G. 51.46, F-105-II.
- One 1" vent nozzle, carbon steel nozzles, U.S.C.G. 51.34, P-106-B, SA-213, TP-302, stainless steel cladding.
- Two 2" safety valve carbon steel nozzles, U.S.C.G. 51.34,

P-106-B, SA-213, TP-302, stainless steel cladding. One nozzle feeds a line containing a safety relief valve. The second nozzle feeds a line containing a safety diaphragm operated valve which is pressure activated.

- One 1" pressure transmitter nozzle, carbon steel, U.S.C.G. 51.34, P-106-B, SA-213, TP-304 with stainless steel cladding.

The following nozzles are located in the cylindrical section:

- Two 1" water level indicator nozzles, carbon steel, U.S.C.G. 51.34, P-106-B, SA-213, TP-304 with stainless steel cladding.
- One 2" in-spray carbon steel nozzle, U.S.C.G. 51.34, P-106-B, SA-213, TP-304 with stainless steel thermal sleeve and stainless steel cladding.
- Two 1-1/2" stainless steel temperature sensing wells. Both are located in the cylindrical section. Each well is 1-1/2" O.D. x 10.34" in length with 6" extending into the vessel and a 9" screwed nipple on the external end. One well is located in the steam space and one in the water space on the aft end of the vessel approximately 15° starboard of the fore-aft centerline so as to clear the level indicating device and remain water covered after a 10 cubic foot outsurge and under design conditions of pitch and roll.

On the center of the lower hemispherical head is located the 4" in-surge and out-surge carbon steel nozzle, U.S.C.G. 51.34, P-106-B, SA-213, TP-304, with stainless steel thermal sleeve and stainless steel cladding.

MANWAY AND SUPPORTS

The 15" I.D. manway located in the upper elliptical head, serves as the only access to the pressurizer. The manway is sealed by a welded diaphragm and bolted cover plat, 29" O.D. by 5-1/4" thick with sixteen 2-3/8" diameter holes equally spaced to receive the 2-1/4" dia. x 11-5/8" long studs. Two lifting lugs are provided on the manway cover. The manway can also be sealed by means of a flexitallic gasket on a temporary basis if no welding facilities are available.

The pressurizer will be vertically mounted on a cylindrical support ring and skirt attached to the bottom hemispherical head. Access holes are provided in this support skirt for removing the replacable electric heaters.

INSULATION

The pressurizer is fitted with a support ring for insulation. This ring is located on the pressurizer support skirt. There will be a 4" thickness of insulation on the entire vessel including the lower head inside the supporting skirt.