NASA Contractor Report 178067

EVALUATION OF RELIABILITY MODELING TOOLS FOR ADVANCED FAULT TOLERANT SYSTEMS

(NASA-CR-178067) EVALUATION OF RELIABILITY MODELING TOOLS FOR ADVANCED FAULT TOLERANT SYSTEMS Final Report (Research Triangle Inst.) 159 p CSCL 14D

N87-16559

Unclas
G3/65 43230

Robert Baker and Charlotte Scheper

Center for Digital Systems Research
Research Triangle Institute
Research Triangle Park, North Carolina 27709

Contract NAS1-16489
Task Assignment No. 16
October 1986

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23665

NASA Contract Report 178067

EVALUATION OF RELIABILITY MODELING TOOLS FOR ADVANCED FAULT TOLERANT SYSTEMS

NASA Contract # NAS1-16489
Task 16

October 1986

Robert Baker
Charlotte Scheper

Center for Digital Systems Research
Research Triangle Institute
Research Triangle Park, North Carolina 27709

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

This report documents the results from an evaluation of the CARE III and ARIES 82 reliability tools for application to advanced fault-tolerant aerospace systems. The results of this investigation are expected to provide guidance for planning future reliability modeling research and development.

To determine reliability modeling requirements, the evaluation focuses on the Charles Stark Draper Laboratories' Advanced Information Processing System (AIPS) architecture as an example architecture for fault tolerant aerospace systems. A number of simple reliability problems were formulated and analyzed using CARE III and ARIES 82. From these test problems and from the reliability modeling requirements of AIPS, advantages and limitations were identified for CARE III and ARIES 82.

CARE III, which was designed primarily for analyzing ultrareliable flight control systems, was found to have many desirable features. Among these were the capability of handling large systems, a somewhat flexible fault handling model, nonconstant failure rates in the fault occurrence model, the provision for near coincident double faults, the computational accuracy required for analyzing ultrareliable systems, and the user interface, although not fully interactive, which provides for simple and flexible system definition.

Examination of the reliability modeling requirement for the AIPS architecture, particularly for the long mission times in space applications, revealed several current limitations of CARE III. System scenarios which were difficult to model or could not be modeled with CARE III were

- Systems with unpowered spare modules,
- Systems where equipment maintenance must be considered,
- Systems where failure depends on the sequence in which faults occurred,[1] and
- Systems where multiple faults greater than a double near coincident fault must be considered.[2]

[1] Appendix B.2 of the CARE III Users Guide describes a method to analyze time sequence dependent faults. This method essentially establishes bounds for reliability. Under appropriate conditions, usually mission times which are short relative to the time between failures, these bounds should be close to the actual reliability. For longer mission times, such as space applications, where exhaustion of components and techniques such as function migration are factors, it is not clear that the suggested method will be sufficiently accurate.

[2] The need to consider near coincident faults of order greater than two arises from configurations such as the quintuplex. With short fault recovery intervals and improved component reliability, triplex configurations may meet the needs of future systems and hence the need to analyze higher order, near coincident faults would not arise. It should be noted, however, that short fault recovery intervals may be difficult to achieve particularly with respect to software components. It should be further noted that CARE III's inability to handle third order, near coincident faults does not arise because it fails to evaluate the failure probability due to

Also, the computational accuracy of CARE III is limited outside the ultrareliable regime.

The ARIES 82 program, whose primary use has been to support university research and teaching, was found to have a number of desirable features. Among these were the interactive nature of the program, the ability to handle a wide range of system scenarios such as systems with and without maintenance and systems with powered or unpowered spares, the flexibility of user-defined state transition matrices, and the computation of performance measures other than reliability such as a mean time to failure, life cycle measures, and improvement factors. The primary limitations identified for ARIES were

- The use of instantaneous coverage,
- The use of constant transition rates,
- The limitations on the size of systems that can be modeled,
- Lack of formal validation,
- Several programming errors, which were apparent from analyzing sample problems,
- Limited computation accuracy, especially for ultrareliability requirements of commercial air transport, and
- ARIES is an unsupported product.

Both CARE III and ARIES were not suited to determine the reliability of complex nodal networks of the type used to interconnect processing sites in the AIPS architecture. In fact, this particular reliability analysis problem is not addressed by existing modeling tools and will require the development of new techniques.

It was concluded that ARIES was not suitable for modeling advanced fault tolerant systems. It was further concluded that, subject to the limitations cited above, CARE III is best suited for evaluating the reliability of advanced fault tolerant systems for air transport.

critical triples. The probability of critical triples often are quite small. The limitation is because CARE III cannot exclude from the reliability calculation those near coincident double faults which would not lead to system failure in systems such as the quintuplex.

1.0 Introduction and Scope

Digital flight control systems for spacecraft and aircraft perform life or missions critical functions. Extremely high reliability requirements must be established and demonstrated for these systems. To meet the reliability requirements, systems become large and complex. Size, complexity, and demanding requirements combine to make the prediction and validation of reliability difficult.

During the system design phase, reliability predictions must be obtained to support design tradeoffs between potential system architectures. After such a fault tolerant system has been built, experimental techniques for establishing reliability, such as life testing and simulation, are often precluded or are of limited value due to high costs. Consequently, sophisticated reliability modeling tools based on analytic models are needed to predict and validate reliability for both the design and development phases of fault tolerant systems.

This report details the results of an evaluation of CARE III and ARIES 82, two reliability modeling tools for application to fault tolerant system architectures. The evaluation was performed under NASA Contract NAS1-16489.

CARE III (Computer Aided Reliability Estimation) is the latest in a series of reliability assessment tools co-developed by NASA-LaRC and Raytheon. It was primarily designed for analyzing ultrareliable flight control systems. ARIES 82 (Automated Reliability Interactive Estimation System) is based on a unified model for reliability estimation developed by Ng and Avizienis at the University of California, Los Angeles. Its primary use has been to support university research and teaching.

The objective of this evaluation was to perform a comparative analysis and assessment of CARE III and ARIES 82 for application to advanced fault tolerant flight control systems such as the Advanced Information Processing System (AIPS) being developed by Charles Stark Draper Laboratories. Specifically, the following tasks were performed:

1. The AIPS architecture information was obtained and reviewed. The suitability of CARE III and ARIES 82 for AIPS analysis was determined.

2. A comparative analysis of CARE III and ARIES 82 was carried out.

3. CARE III and ARIES 82 were applied to problems of varying complexity.

4. The limitations of CARE III and ARIES 82, with respect to application to advanced fault tolerant architectures, were determined.

The fault tolerant features of the AIPS architecture are reviewed in Section 2.0 of this report. Section 3.0 provides an overview of the CARE III and ARIES 82 fault models. In Section 4.0, test cases that were analyzed using CARE III and ARIES 82 are described and the results are given. In Section 5.0, CARE III and ARIES 82 are compared and the limitations of each are identified.

2.0 Advanced Information Processing System (AIPS)

2.1 Objectives and Requirements [1]

The Advanced Information Processing System (AIPS) is a fault and damage tolerant system architecture which satisfies real-time data processing requirements for aerospace applications. The specific requirements for seven aerospace applications were established by Draper Laboratories and are given in Figure 2.1. As can be seen, a wide range in each resource requirement or performance parameter is covered by these applications.

Attributes of the AIPS architecture are

- Growth and Change Tolerance,
- Accepts Technology Upgrades,
- Graceful Degradation,
- System Complexity is Transparent to the User,
- Graded Redundancy, and
- Damage Tolerance.

2.2 AIPS Architectural Features and Building Blocks [1]

The elements for the AIPS architecture are the Fault Tolerant Multiprocessor (FTMP), the Fault Tolerant Processor (FTP), a fault and damage tolerant Intercomputer Network (IC), a fault and damage tolerant Input/Output Network (I/O), a fault tolerant mass memory, a fault tolerant power distribution system, and a network operating system which allows the elements to operate together.

Figure 2.2 shows the proof-of-concept model of the AIPS architecture. AIPS consists of processing sites, either FTMP or FTP, which are distributed as necessary

	Mission	Failure Probability	Thruput	Memory	Mass Memory	I/O Rates
COMMERCIAL AIRCRAFT	10 hrs	10^{-9}	5.5 MIPS	2 MB	15 MB	750 Kb/s
TACTICAL MILITARY AIRCRAFT	4 hrs	10^{-7}	6 MIPS	1 MB	100 MB	1 Mb/s
UNMANNED SPACE PLATFORM	5 yrs	10^{-2}	2 MIPS	750 KB	750 KB	150 Kb/s
UNMANNED SPACE VEHICLE	1 wk	10^{-6}	.5 MIPS	300 KB	300 KB	1.5 Mb/s
DEEP SPACE PROBE	5 yrs	10^{-2}	.5 MIPS	300 KB	1 MB	
MANNED SPACE PLATFORM	20 yrs	10^{-2}	15 MIPS	20 MB	400 MB	15 M/bs
MANNED SPACE VEHICLE	10 days	10^{-7}	1.5 MIPS	3 MB	3 MB	1 Mb/s
RATIO MAX/MIN	40K	10^7	30	60	1000	100

Figure 2.1. AIPS Application Requirements

throughout the vehicle. They are linked by a layered damage and fault tolerant IC network. Input/Output buses provide access to Input/Output devices. Processing sites and I/O buses may have a global, regional, or local extent. For example, most or all processing sites would have access to I/O devices that are connected via a global I/O bus , e.g., an I/O bus that is connected to each processing site. A local I/O bus could connect I/O devices to one processing site. Similarly, software operating systems for AIPS can have global, regional, or local control. Access to a fault tolerant mass memory is provided via a dedicated mass memory bus.

Resources within the distributed system are usually assigned to a fixed set of functions. Under certain conditions, such as a change in mission phase or a hardware failure, the computing resources can be reassigned to other functions. This capability allows for limited distributed processing and is called semi-dynamic function migration. Function migration is expected to be used to reconfigure system resources in order to achieve higher reliability for critical functions or to meet the resource or power requirement due to changes in a mission phase.

Hardware redundancy is implemented at the processor, memory, and bus level. Redundancy provides for fault detection and for continued operation of the system following a component failure. Redundant elements are operated in tight synchronism resulting in improved fault coverage and latency. Fault detection and masking functions are implemented in hardware. Tight synchronism requires that these functions be invoked frequently. By implementing these functions directly in hardware, the need for additional computational resources required by a software implementation is avoided.

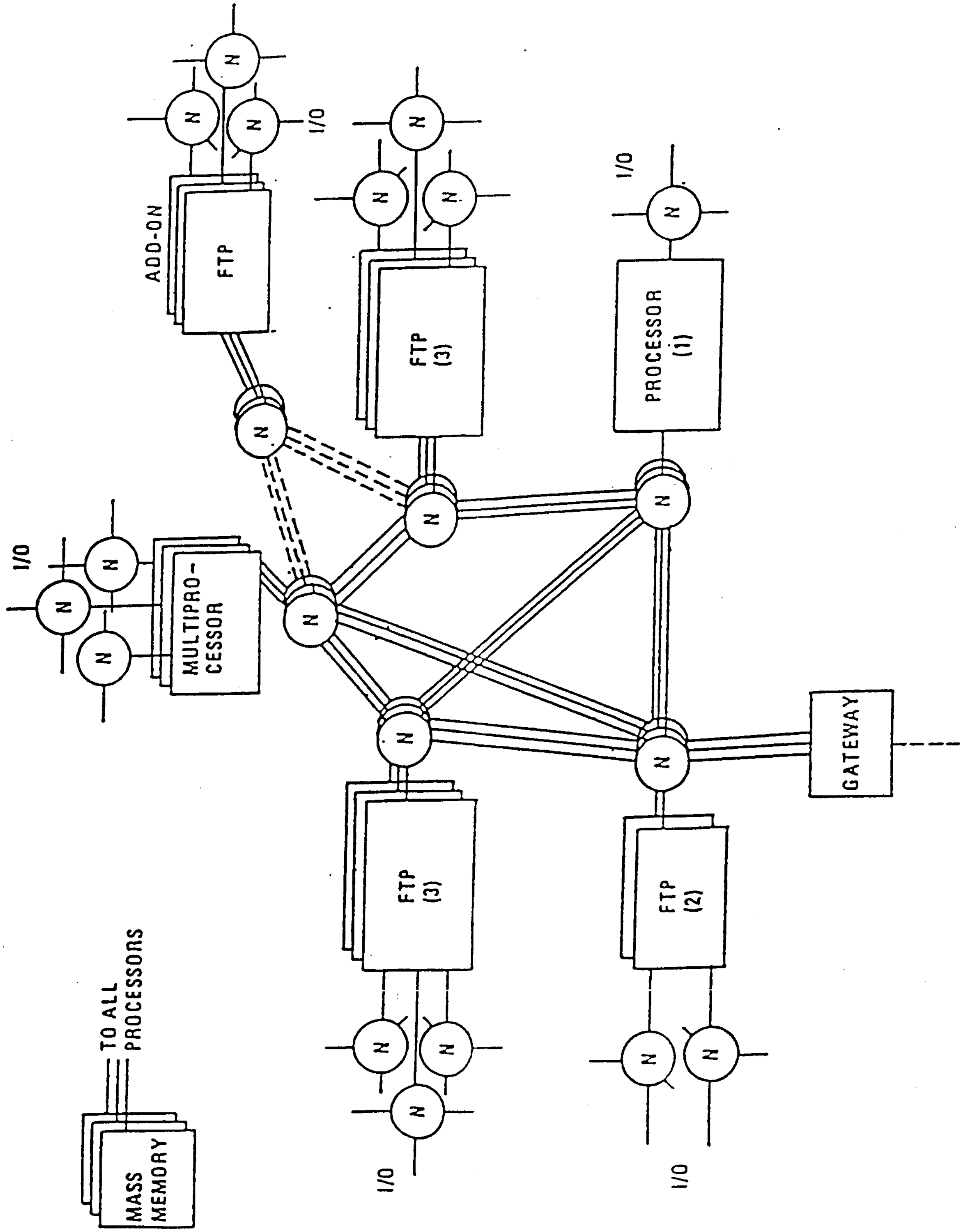


Figure 2.2. AIPS Proof-of-Concept System

Figure 2.2

The less frequently invoked fault isolation and reconfiguration functions are implemented in software.

The successful distribution of data from a simplex source to redundant processors is necessary to avoid single point failures. The processors must exchange their copies of the simplex data to assure that the same data values are being used by each processor. The process of establishing source congruency is supported and made efficient in the AIPS architecture by use of software and special hardware features.

A triplex FTP architecture is shown in Figure 2.3. The FTP can be configured in simplex, duplex, or triplex processor form. Each FTP channel has an Input/Output processor (IOP) and a computational processor (CP). These processors have separate memories, clocks, and timers. The IOP has interfaces to the I/O and IC buses. The processors have access to a shared memory, interfaces to the mass memory, and to data exchange hardware. The data exchange hardware is used to exchange data between redundant channels, to detect faults, and to mask faults. Redundant channels are tightly synchronized using a fault tolerant clock.

The IOP interfaces to a redundant IC network. It receives from each layer of the IC network and detects and masks faults. However, it can only transmit on one layer of the network. The other layers in the network are reserved for the remaining redundant channels in the FTP. With respect to a single channel, the receive interface is cross-strapped and the transmit interface is not.

The FTMP shown in Figure 2.4 is composed of a number of computational processors (processors with local memory) all interconnected via a redundant, fully cross-

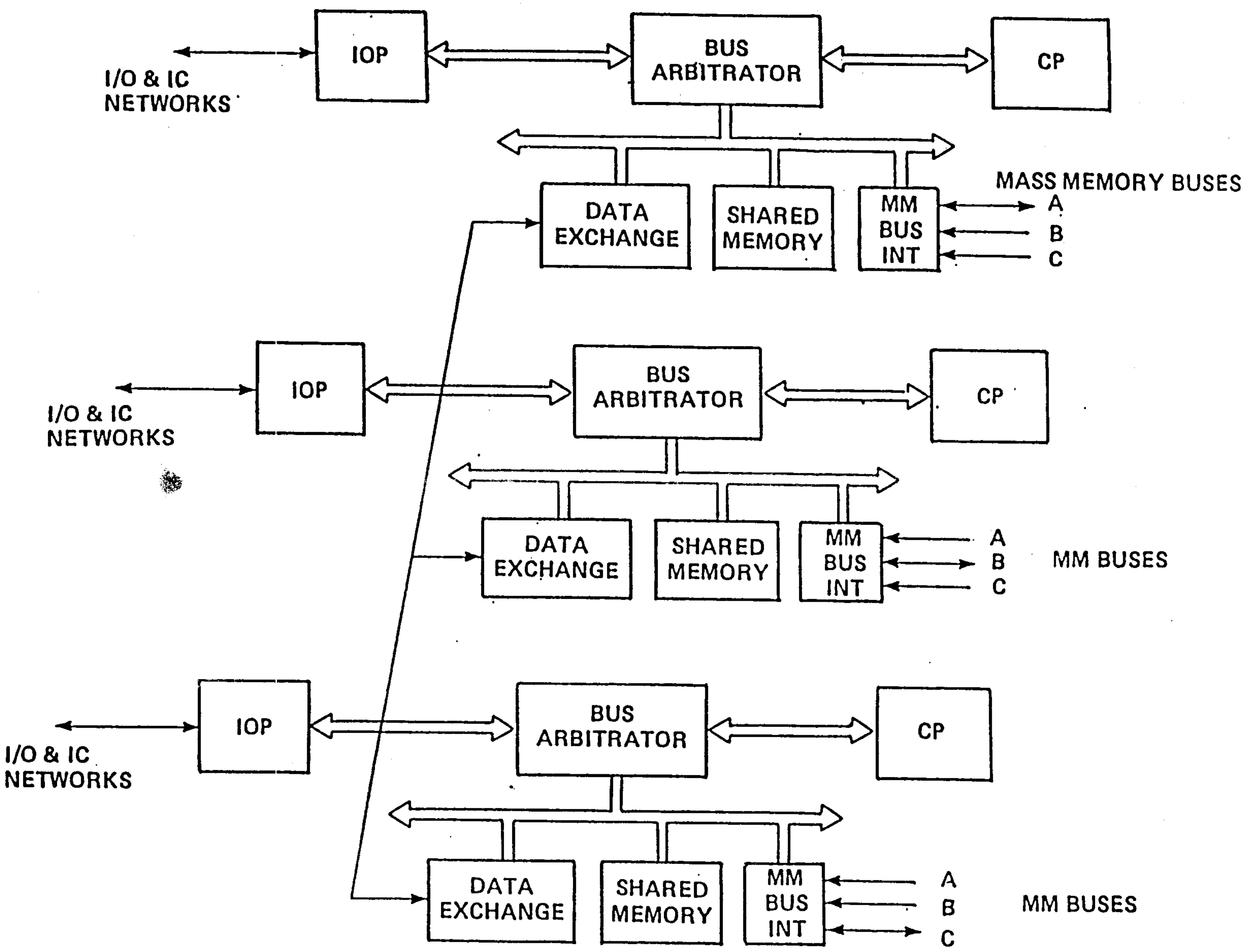


Figure 2.3. Fault Tolerant Processor (FTP) Architecture

strapped multiprocessor bus. A shared memory can be accessed via the multiprocessor bus. FTMP configurations could consist of triads of CP's interfaced to the I/O bus, to the IC network, or the mass memory bus. Some triads could be connected only via the multiprocessor bus.

The FTMP fault tolerance features such as synchronism, clocking, and redundancy are similar to those of FTP.

The intercomputer network (IC) consists of three identical, independent layers. Each layer consists of a number of multiported, circuit switched nodes interconnected by communication links. Nodes are generally associated with specific processing sites. Communication between any two processing sites can be established by selecting a suitable combination of nodes and links. If a link fails, communications between two sites can be reestablished by using another combination of nodes and links.

The I/O network is similar to the IC network except that only one layer is implemented.

In summary, some of the key fault tolerant features are

- FTMP and FTP Concepts,
- Hardware Redundancy,
- Redundant Elements in Tight Synchronism,
- Fault detection and masking implemented in hardware,
- Fault isolation and reconfiguration implemented in software,
- A layered nodal intercomputer communications network with reconfiguration features,
- A nodal I/O communications network with reconfiguration features,
- Features to support and efficiently implement the process to establish source congruency, and

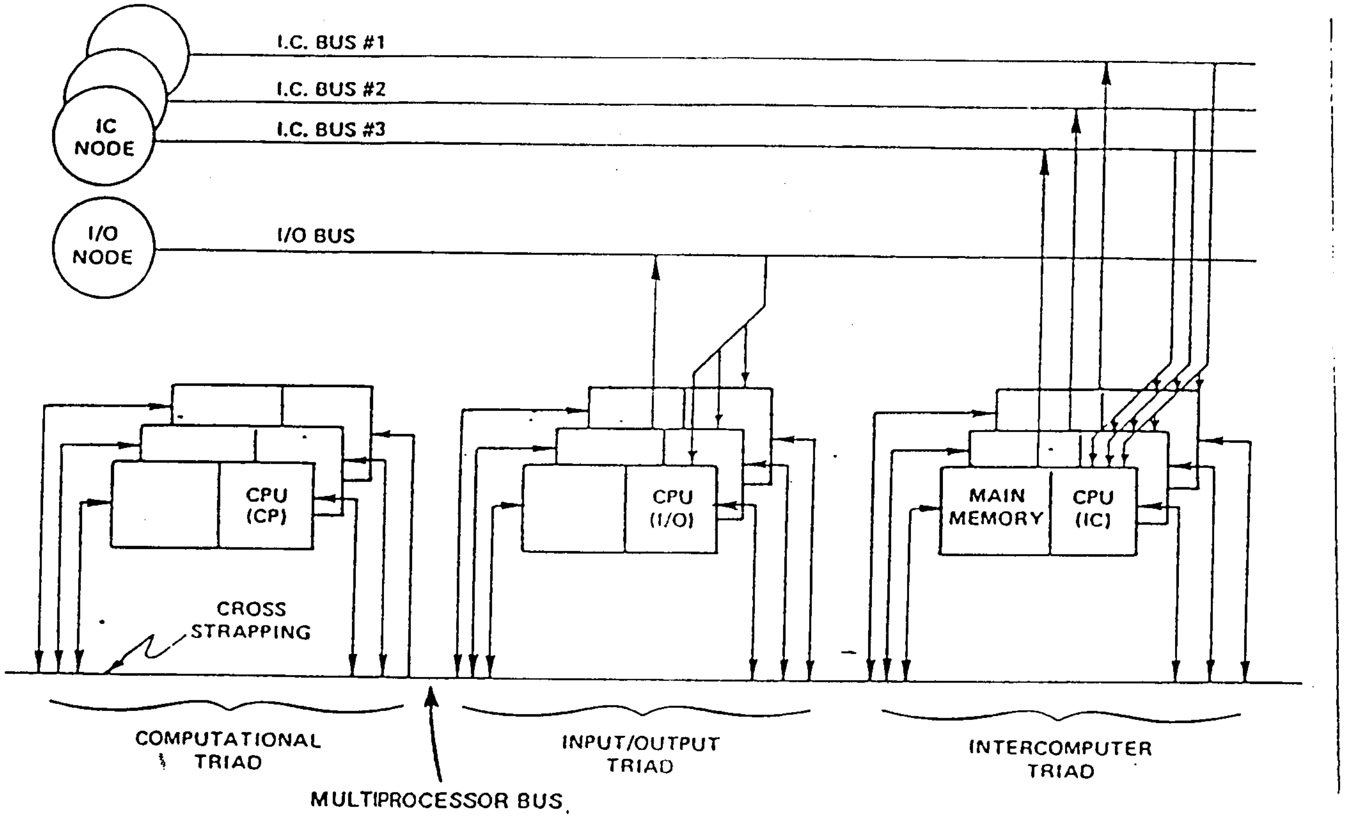


Figure 2.4. Fault Tolerant Multiprocessor Architecture

- Function Migration.

2.3 AIPS Requirements and Features Impacting Reliability Assessment [2]

A number of AIPS requirements and architectural features impact reliability assessment. Among those the following are of particular significance for the purpose of this report.

1. Resource requirements are, for some applications, large and hence the number of high level components (processors, memories, etc.) can become large.

2. A high degree of fault tolerance is required resulting in the need to account for failure of fault handling as well as the exhaustion of components.

3. Applications require both short and very long mission times.

4. For some applications, the architecture results in large nodal networks.

5. The Intercomputer Network is partially cross-strapped.

6. The function migration feature required for some applications can complicate reliability analysis.

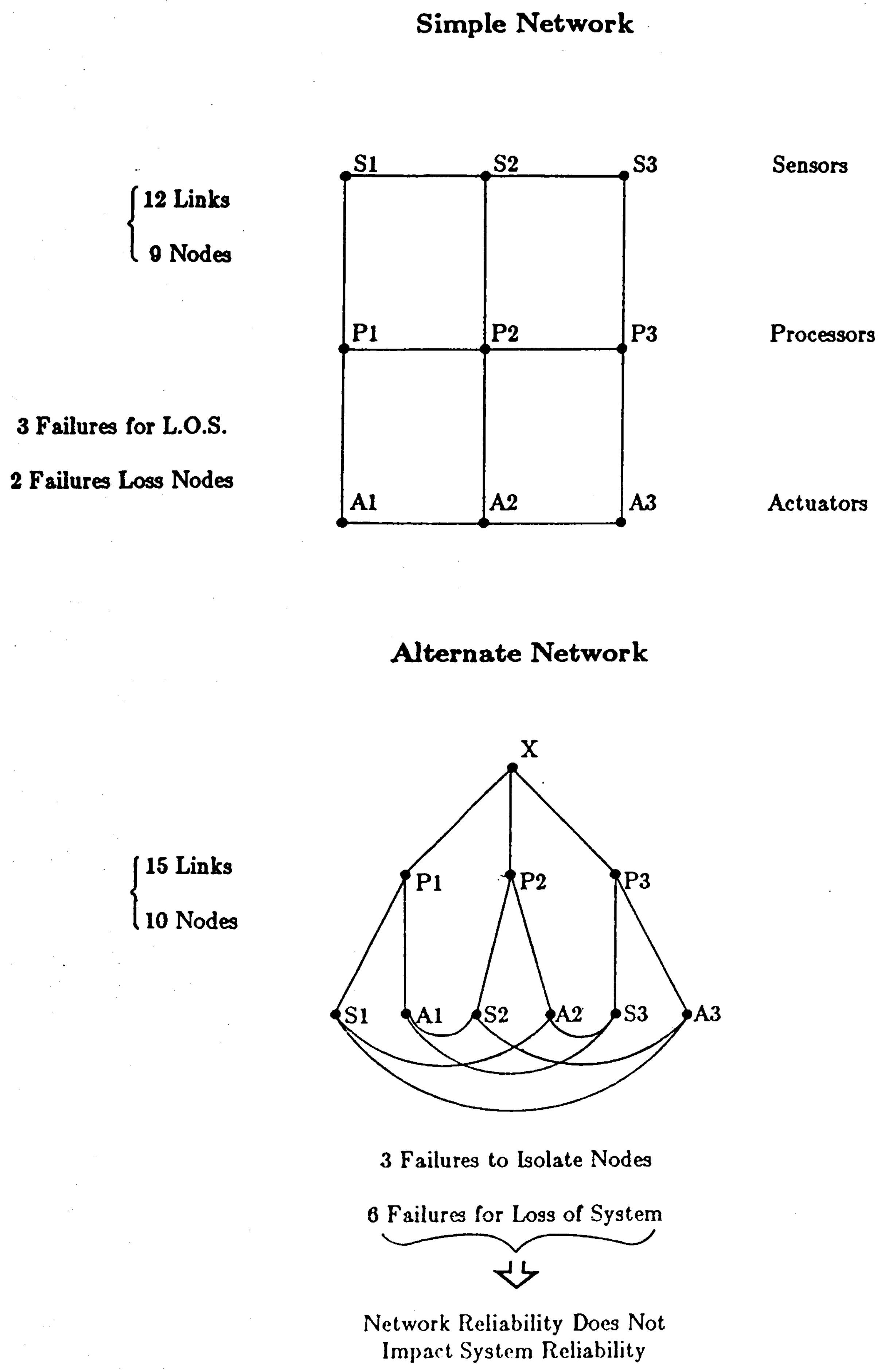
Some applications for AIPS will permit system maintenance and repair (open system), others will not (closed system). Certain space missions will require the use of unpowered spare system modules, and hence the capability to model different failure rates for powered and unpowered components will be needed.

The use of function migration will impact reliability analysis in a number of ways. For example, loss of the system function will depend on whether function migration can be completed. This could depend upon whether a particular fault occurs before or after the need for function migration. Consequently, loss of system function will depend on the order or sequence of fault occurrence.

The long mission times could impact the accuracy of reliability estimates made using numerical approximations.

Partial cross-strapping of the IC networks dictates that processing sites and the IC network cannot be analyzed independently (structurally decomposed).

The large nodal communication networks required impact the reliability analyses. Figure 2.5 shows a simple nodal communications network between a triple redundant set of sensors, processors, and actuators. This network is connected in a planar topology. It can be determined by observation that the loss of two links can isolate a node and that the loss of three links will lead to system failure. Determining the number of failure combinations that lead to loss of system is slightly more difficult but is not too demanding. However, the more complex network given in Figure 2.6 is much more difficult to analyze. In applications using the AIPS architecture, network failures can be a major factor determining system unreliability. Consequently, the capability to analyze complex nodal networks will be necessary for some AIPS applications. Further, this capability could be used to develop better network topologies such as the alternate network shown in Figure 2.5. With this alternate non-planar topology, three failures are required to isolate a node and six failures are required for loss of system. In such a case, network reliability would be sufficiently high on short missions that system reliability would not be affected.



Simple Network

12 Links
9 Nodes

3 Failures for L.O.S.

2 Failures Loss Nodes

Alternate Network

15 Links
10 Nodes

3 Failures to Isolate Nodes

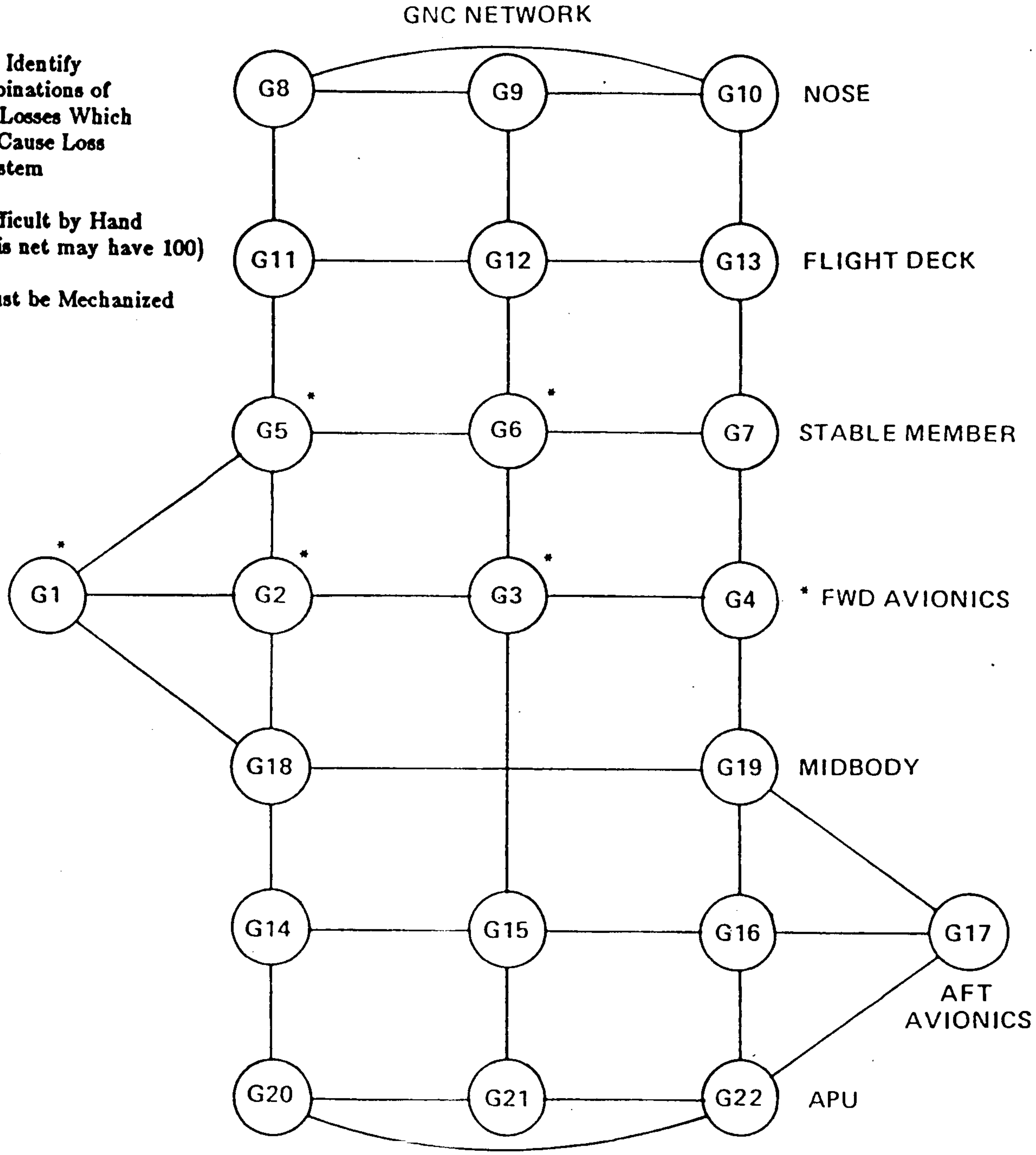
6 Failures for Loss of System

Network Reliability Does Not
Impact System Reliability

Figure 2.5. Simple Network Topologies

Problem: **To Identify Combinations of Link Losses Which Will Cause Loss of System**

- **Difficult by Hand (This net may have 100)**
- **Must be Mechanized**



* {G1, G2, G3 – ROOT NODES FOR ONE PROCESSING SITE
  {G4, G5, G6 – ROOT NODES FOR OTHER PROCESSING SITE

Figure 2.6. AIPS Network for a Candidate Application

3.0 OVERVIEW OF ARIES AND CARE III

3.1 Introduction [3]

Because of the ultrareliability requirements of the AIPS architecture, an analytic method of assessing reliability is required. This method must be sufficiently general to cover the wide range of systems that can be developed with AIPS. It must also be computationally feasible. One widely used method is to model the system as a finite-state, continuous-parameter Markov process $X(t)$, $t \geq 0$. In this model, the state probabilities are defined as $p_j(t) = P[X(t)=j]$, the probability that the system is in state j at time t; the transition probabilities as $p_{ij}(t,t+h) = P[X(t+h)=j \mid X(t)=i]$, the probability that the system is in state j at time t+h given that it was in state i at time t; and the transition rates $q_j(t)$ and $q_{ij}(t)$ as

$$q_{ij}(t) = \frac{d}{dt} p_{ij}(t), \; i \neq j$$

and

$$\begin{aligned} q_j(t) &= \frac{d}{dt} p_{jj}(t) \\ &= \frac{d}{dt}[1 - \sum_{i \neq j} p_{ij}(t)] \\ &= -\sum_{i \neq j} q_{ij}(t) \, . \end{aligned}$$

The system's state probabilities can then be found by solving the matrix equation

$$P'(t) = Q(t)P(t) \, ,$$

where $P(t) = (p_1(t), p_2(t), \ldots, p_n(t))$ is the state probability vector for the system's n operational states and

$$Q(t) = \left[\begin{cases} q_{ij}(t) & , \ i \neq j \\ q_j(t) & , \ i = j \end{cases}\right]$$

is the transition rate matrix. The reliability of the system at time t is then given by

$$R(t) = \sum_{i=1}^{n} p_i(t) \ .$$

Both ARIES and CARE III use this Markovian model; however, they differ in their definition of states and transition probabilities. In ARIES, the Markov process is assumed to be time-homogeneous; i.e., the transition probabilities $p_{ij}(t,t+h)$ depend not on the initial time t but on the elapsed time h. As a result of this assumption, the states of the model must have exponentially distributed holding times. Fault-occurrence states are differentiated according to configuration so that a state reconfigured with spares is different from a state with the same number of active modules but in which an uncovered spare failure has occurred. This distinction is made because the system can degrade from the former but not from the latter state. There are no fault-handling states: coverage is assumed to be instantaneous and is incorporated into the transition rates as a constant probability.

In CARE III, time-homogeneity is not required and non-exponentially distributed holding times are allowed. The fault-occurrence states are defined only by the number of operational active and spare modules: no distinction is made as in ARIES between degradable and nondegradable configurations. However, the transition rates are formulated so that the state probabilities are the same as they are in ARIES. [4] Coverage is modeled in CARE III by fault-handling states, which represent the detection, isolation, and recovery from errors, and failure states, which are entered because of coverage failures. Both of these reliability tools are discussed in the following sections.

3.2 ARIES[5] [6] [7]

3.2.1 General Description

ARIES is an interactive, unified reliability modeling tool developed by Ng and Avizienis at UCLA. The current version, ARIES 82, is written in C for use on UNIX systems and is intended primarily as a teaching aid in the evaluation-based design of FT computers.[6]

In ARIES, a system is defined to be a series configuration of homogeneous subsystems, each of which can be modeled as a finite-state, continuous-parameter, time-homogeneous Markov process. State aggregation is achieved through this structural decomposition since, rather than considering the system as a whole, each subsystem is analyzed separately and the results combined to give system reliability. State reduction is also achieved by approximating fault-handling states through instantaneous coverage.

In ARIES there are six basic models defining closed, repairable, and renewable systems as follows:

Type 1	Closed FT System with Permanent Faults,
Type 2	Closed FT System with Transient Fault Recovery,
Type 3	Mission-Oriented Repairable System,
Type 4	Repairable System with Transient Fault Recovery,
Type 5	Repairable System with Restart, and
Type 6	Periodically Renewed Closed FT System.

The Type 1 system is a closed fault tolerant system. It does not undergo any external repair or renewal and all faults that occur are assumed to be permanent faults. The system can have powered or unpowered spares and can degrade after the spares are exhausted. However, the system's ability to degrade can be blocked by unrecoverable spare failures, since it is assumed that if an undetected and unrecoverable failure exists in a spare, the system cannot activate succeeding spares and will fail when that spare is switched in. It is also assumed that spares are periodically tested, that spare selection is predetermined, and that a failed module is removed from the system.

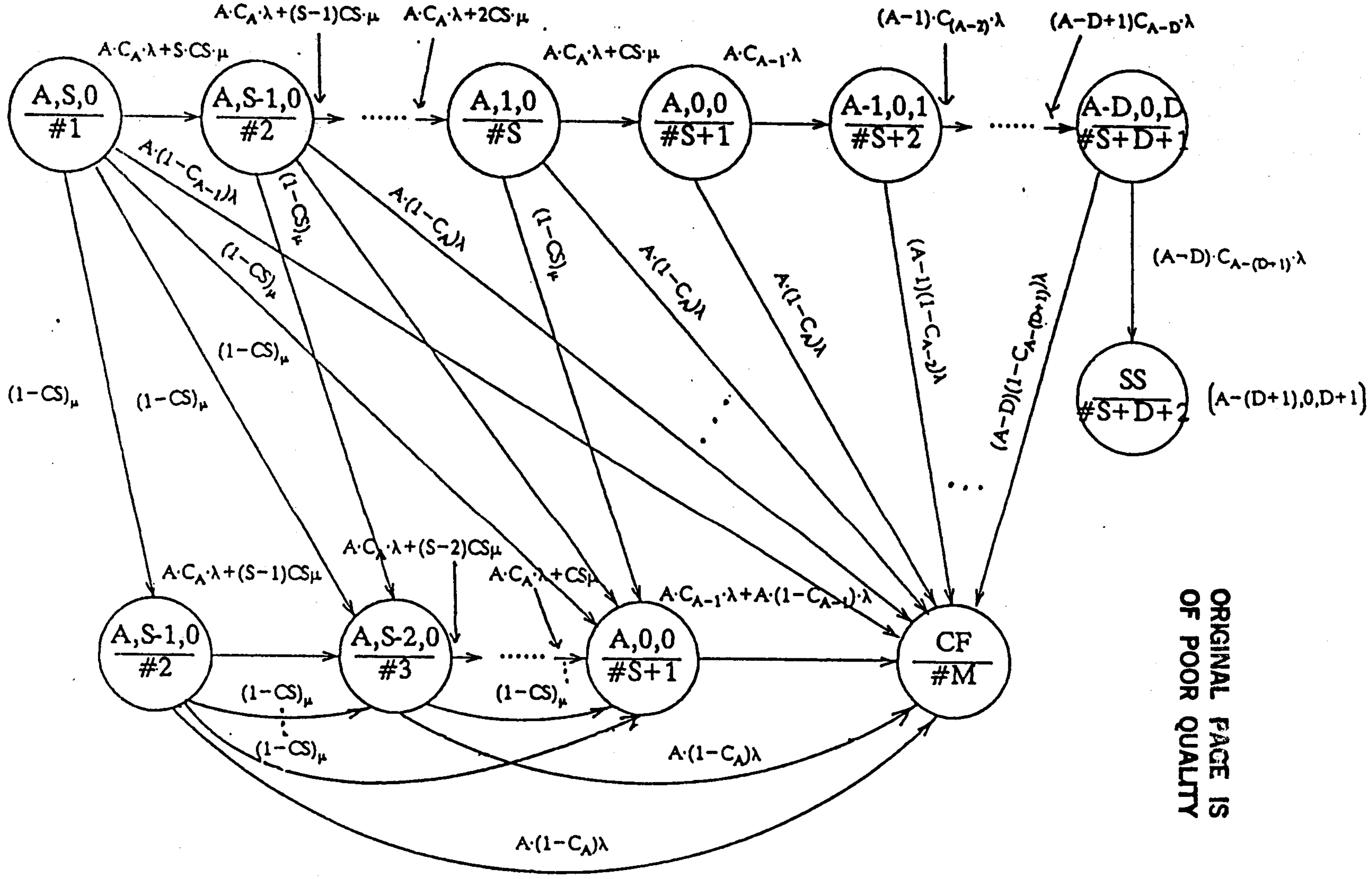
The model for the closed FT system (Type 1) is shown in Figure 3.1. The states in this model correspond to triples of the form (y,s,d), where

y = the number of fault−free active units,
s = the number of available spares,and
d = the number of degradations allowed

and $\overline{(y,s,d)}$, where

y = the beginning number of active units,
s = the number of accessible spares,and
d = 0.

The (y,s,d) states represent reconfigurations of the system as active modules fail and are replaced by spares until all spares are exhausted and the system degrades, terminating in one of two final states (safe shutdown or system failure). The $\overline{(y,s,d)}$ states represent reconfigurations of the subsystem that cannot be degraded because an undetected and unrecoverable error exists in a spare and will cause system failure when that spare is switched in. There are no states to represent fault handling: these states are approximated by coverage probabilities associated with the transitions between the fault occurrence states.



ORIGINAL PAGE IS
OF POOR QUALITY

A = # Active
S = # Spares
D = # Degradations
λ = Active Failure Rate
μ = Spare Failure Rate
CS = Spare Coverage
C_A = Coverage While Spare Remain
C_{Ai} = Coverage for Transition to *ith* Degradation

Figure 3.1. Markov Model for ARIES Type 1 System

This model is instantiated by assigning values for the parameters D, S, CS, λ, μ, $\underline{Y}$, and$\underline{CY}$. The parameter D is the number of degradations the system can sustain, i.e, the number of active units that can be lost without replacement; S, the number of spares. CS is the coverage associated with each spare; if CS < 1, then the blocked spare states, $(\overline{y,s,d})$, of the model can be entered. λ and μ are the failure rates for the active and spare units, respectively, and are assumed to be constant. If $\mu = \lambda$, the spares are assumed to be powered; if $\mu < \lambda$, they are assumed to be unpowered. Although unpowered spares are allowed, μ must be greater than zero and $\frac{\lambda}{\mu}$ must be no greater than 10^6. The number of active modules in each degraded configuration is entered as a vector $\underline{Y} = (A, A-1, \ldots, A-D, A-(D+1))$, where Y[0] is the initial number of active units, Y[i] is the number after the i-th degradation, and Y[D+1] is the number in the safe shutdown state. The coverage probabilities associated with the transitions between configurations is entered as a vector $\underline{CY} = (C_A, C_{A-1}, \ldots, C_{A-D}, C_{A-(D+1)})$, where CY[0] is the coverage probability used for all transitions while any spares remain and CY[i] is that used for the transition to the i-th degradation. If there are no spares in the system, CY[0] is never used.

Each of the six models has an identifying set of parameters. These parameters specify configuration, failure modes, and coverage mechanisms for each system type. For a complete list of the ARIES parameters, see Figure 3.2.

Systems that do not conform to the assumptions for Types 1 - 6 or cannot be decomposed into subsystems of these types cannot be accurately described by those models. However, any system that can be represented by a single state transition-rate

$Y[0]$ = Initial number of active modules

S = Initial number of spare modules

D = Number of degradations allowed in the active set

$\underline{Y}$ = Active resource vector $(Y[0],...,Y[D],Y[D+1])$

$\underline{Z}$ = Computing capacity vector $(Z[0],...,Z[D],0)$

λ = Failure rate of one active module

μ = Failure rate of one spare module

ν = Failure rate of one good module in safe shutdown condition

τ = Transient fault arrival rate of one active module

$\bar{D}$ = Mean duration of a transient fault

CS = Coverage for recovery from spare failures

$CY[i]$ = Coverage associated with the transition to
the degraded configuration specified by $Y[i]$

$\underline{CY}$ = Coverage vector for active failures
= $CY[0],...CY[D],CY[D+1]$,

NP = Number of recovery phases for transient faults

CR = Recoverability from transient faults

χ = Interference rate for transient faults
= The failure rate of all hardware involved
in executing the transient recovery processes

$T[i]$ = The duration of the ith recovery phase
for transient faults

$\underline{T}$ = Recovery duration vector for transient faults
= $T[1],...,T[NP]$

$CE[i]$ = The effectiveness of the ith recovery phase
for transient faults

$\underline{CE}$ = Recovery effectiveness vector for transient faults
= $CE[1],...,CE[NP]$

Figure 3.2. ARIES Parameters

matrix can be solved by ARIES. For these Type 7 systems, the user enters the complete system transition-rate matrix rather than specifying values for model parameters. This user-specified matrix is then incorporated into the solution of the system in the same manner as the matrix that is generated from the fixed ARIES models.

3.2.2 Solution Method

As a result of the time-homogeneous restriction in ARIES, the transition-rate matrix Q(t) simplifies to

$$Q(t) = \left[\begin{cases} q_{ij} \ , & i \neq j \\ q_j \ , & i = j \end{cases} \right]$$

and the matrix equation simplifies to

$$P'(t) = QP(t) \ .$$

Thus,

$$P(t) = e^{Qt}P(0) \ .$$

This system is solved in ARIES as

$$P(t) = \sum_{i=1}^{n} e^{\sigma_i t} \left[\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{Q - \sigma_j I}{\sigma_i - \sigma_j} \right] P(0) \ ,$$

where σ_i is an eigenvalue of Q.[3] The solution's use of Sylvester's theorem to evaluate e^{Qt} requires that the transition-rate matrix have distinct eigenvalues. This requirement restricts the ratio of the active unit failure rate (λ) to the spare unit failure rate (μ) in a system with unpowered spares to $\frac{\lambda}{\mu} \leq 10^6, \ 0<\mu<\lambda$.

To implement the solution, the transition-rate matrix, Q, is determined from either the specified parameters or from the user-specified matrix. For closed systems, the eigenvalues of Q are computed from the model parameters; otherwise, they are computed by reducing Q to upper Hessenberg form and applying the QR algorithm. If nondistinct eigenvalues occur, the duplicates are dropped from the computation.

Next, the probability polynomial coefficient matrix, B, is constructed from Q; the *distinct* eigenvalues, $\underline{\alpha}$, of Q; and the initial state probability distribution, P(0). The initial probability distribution P(0) for closed and repairable systems and closed phases of a PRC system is

$$P(0) = (1,0,\ldots,0)\ ;$$

for the renewal phase of a PRC system,

$$P(0) = (1,0,\ldots,0)e^{Q_1\beta},$$

where Q_1 is the transition rate matrix for the closed operation phase.

After B is constructed, P(t) is computed for each state k, from B and $\underline{\alpha}$, as

$$P_k(t) = \sum_j b_j^k e^{-\sigma_j t}.$$

Once the state probabilities are solved, the reliability of the subsystem is computed as

$$R(t) = \sum_k P_k(t);$$

i.e., as the sum of the state probabilities of the constituent states.

With the reliability $R_n(t)$ of each of the n subsystems comprising the system thus computed and with the assumption of serial configuration of subsystems, the system reliability R(t) is computed as

$$R(t) = \prod_{i=1}^{n} R_i(t)\ .$$

3.2.3 Outputs

System reliability is reported for user-specified time intervals. For each time interval, the reliability of the complete system and the reliability of each component subsystem is reported. The report is displayed on the terminal screen but can also be written to a log file, plotted on a SOLTEC281 plotter, or filtered to a UNIX plotting tool.

In addition to system reliability, ARIES can compute and display the mean time to first system failure, the normalized percentage of failure of each component subsystem, the reliability improvement factor and the mission time improvement factor of one system over other systems, the system failure rate, and, for renewable systems, life-cycle measures.

3.3 CARE III

3.3.1 General Description[8] [9] [10]

In CARE III, a system is defined to be a configuration of stages, where each stage is a group of identical modules. Stage failures are independent. Stages within a system may be dependently coupled as described by a fault tree. A module occupies a distinct state for each combination of its fault status (whether a fault has occurred or not), fault category (mode of failure and associated occurrence rate), and coverage state (detection and handling of the fault). Denoting module a in stage x by (x,a), the states occupied by a are defined by the vector (d(x,a),i(x,a),c(x,a)), where

$$d(x,a) = \begin{Bmatrix} 0 & \text{if } (x,a) \text{ is operational} \\ 1 & \text{if } (x,a) \text{ is faulty} \end{Bmatrix},$$

$$i(x,a) = \text{fault category, and}$$

$$c(x,a) = \text{coverage state.}$$

The states of the system are then defined by the M-dimensional vector $(\underline{d},\underline{i},\underline{c})$, where

$$\begin{aligned}
\underline{d} &= (d(1,1),\ldots,d(x,n(x)),\ldots,d(N,n(N))),\\
\underline{i} &= (i(1,1),\ldots,i(x,n(x)),\ldots,i(N,n(N))),\\
\underline{c} &= (c(1,1),\ldots,c(x,n(x)),\ldots,c(N,n(N))),\\
n(x) &= \text{number of modules in } x\text{th stage,}\\
N &= \text{number of stages in system, and}\\
M &= \sum_{x=1}^{N} n(x).
\end{aligned}$$

To reduce the number of system states, aggregate states are constructed by grouping states according to the number of faulty modules in a stage, the system fault tree, the coverage structure (i.e., fault-handling states), and the critical pairs fault trees. This reduced system is only semi-Markov; but, assuming a large difference between the rates for the coverage states and those for the fault-occurrence states, it can be decomposed into a semi-Markov coverage model and a non-homogeneous Markov reliability model.

3.3.1.1 Coverage Model

Three types of faults are represented in CARE III: permanent, intermittent, and transient. A permanent fault is any fault that persists until the device is repaired; an intermittent fault, any fault that persists only part of the time due, for example, to a loose connection, a poor bond, etc; and a transient fault, any fault which is not caused by a permanent defect, but nevertheless manifests a faulty behavior for some finite time and then disappears.[11] The User's Guide defines error as any condition in which a module is incorrectly performing its function. Although the User's Guide is not explicit about the endurance of an error, the CARE III fault models implicitly assume that an error, once produced, cannot disappear.

The CARE III coverage model consists of two models and accommodates two types of coverage failures: single fault and double fault. Both of these models are discussed in the following sections.

3.3.1.1.1 The Single-Fault Model

A single fault coverage failure occurs when a fault in a module causes an error before the fault is detected and the module isolated. The single-fault model is shown in Figure 3.3.

Let F = event of a fault at time t
(any of the 3 fault types),
E = event of an error at time t, and
$\bar{F}, \bar{E}$ = complement of F, E.

The states are

$A = F\bar{E}$: the fault persists but has not produced an error,
$B = \bar{F}\bar{E}$: an intermittent or transient fault has healed without producing an error,
$A_E = FE$: the fault persists and has produced an error,
$B_E = \bar{F}E$: the intermittent fault has healed but the error persists,
A_D: the fault was detected in the active state,
B_D: the fault was detected in the benign state,
D_{P_A}: the fault was detected as permanent from A_D, and
D_{P_B}: the fault was detected as permanent from B_D.

In CARE III's terminology states $F\bar{E}$ (A) and FE (A_E) are *active latent states*; $\bar{F}E$ (B_E) is a *benign latent state*; $\bar{F}\bar{E}$ (B) is the *benign state*. This distinction is important since

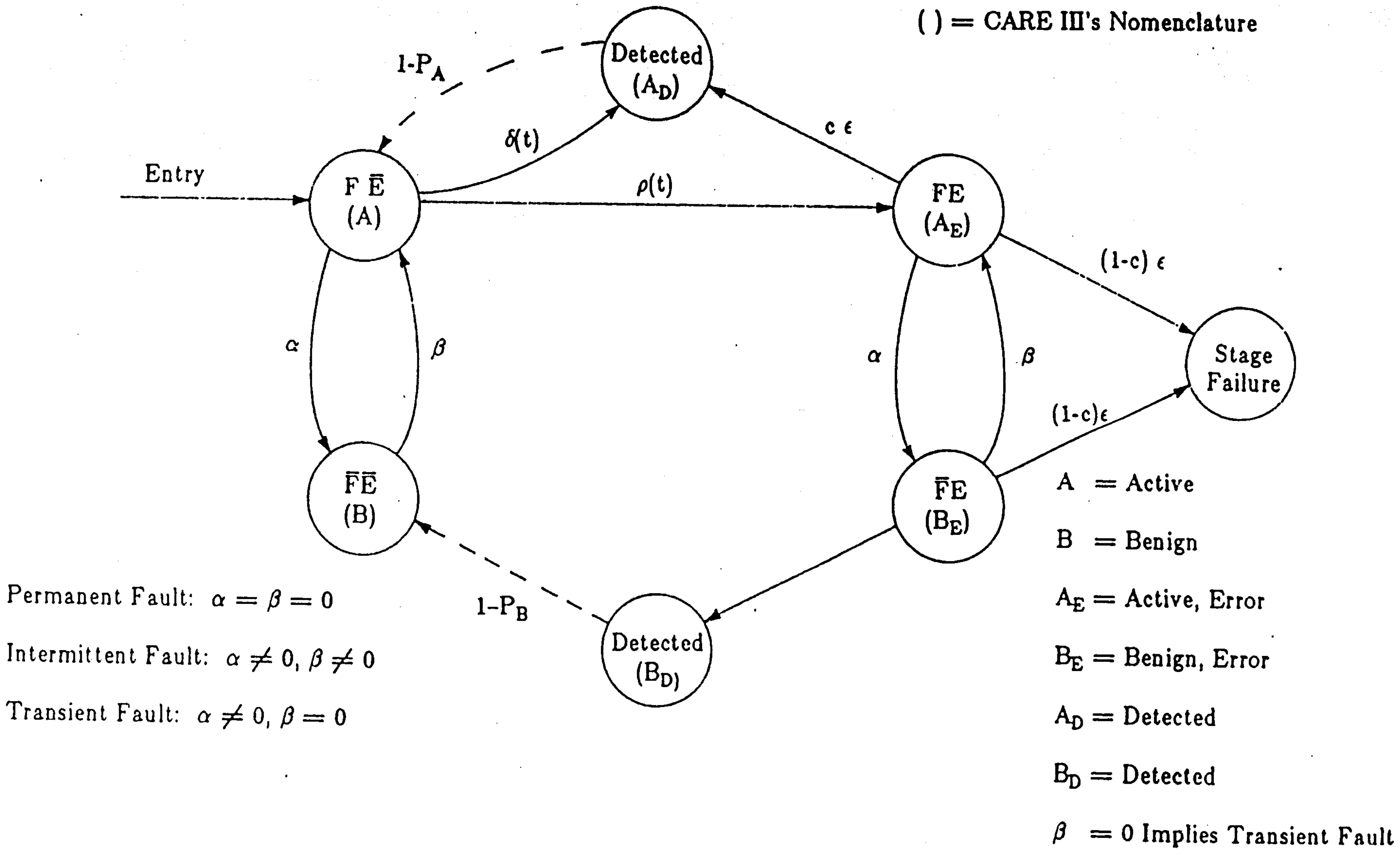


Figure 3.3. Single-Fault Model of CARE III

CARE III assumes that co-existing latent faults in two distinct modules either within a stage or between stages (as specified by the user) constitutes loss of system. These pairs are referred to as *critical pairs*.

Within the single fault model, the possible transitions and the corresponding transition rates are

A to B	alpha,
A to A_D	$\delta(t)$,
A to A_E	$\rho(t)$,
A_E to B_E	alpha,
A_E to A_D	$c\epsilon(\tau)$,
A_E to Failure	$(1-c)\epsilon(\tau)$,
B to A	beta,
B_E to A_E	beta,
B_E to B_D	$c\epsilon(\tau)$,
B_E to FAILURE	$(1-c)\epsilon(\tau)$,
A_D to A	instantaneous,
A_D to D_{P_A}	instantaneous,
B_D to B	instantaneous,and
B_D to D_{P_B}	instantaneous.

The transition rates α and β are constant rates; the functions $\delta(t)$, $\rho(t)$, and $\epsilon(t)$ are restricted to either exponential or uniform densities of the form

$$\theta\exp(-\theta t), \quad t > 0$$

or

$$\theta, \quad 0 < t < \frac{1}{\theta}.$$

Assuming that t and τ are measured from the last entry into A or E (A_E or B_E), respectively, then the single fault coverage model is a semi-Markov process.

The transition parameters α and β define the three fault types as follows:

Permanent Fault when $\alpha = \beta = 0$,
Intermittent Fault when $\alpha \neq 0, \beta \neq 0$, and
Transient Fault when $\alpha \neq 0, \beta = 0$.

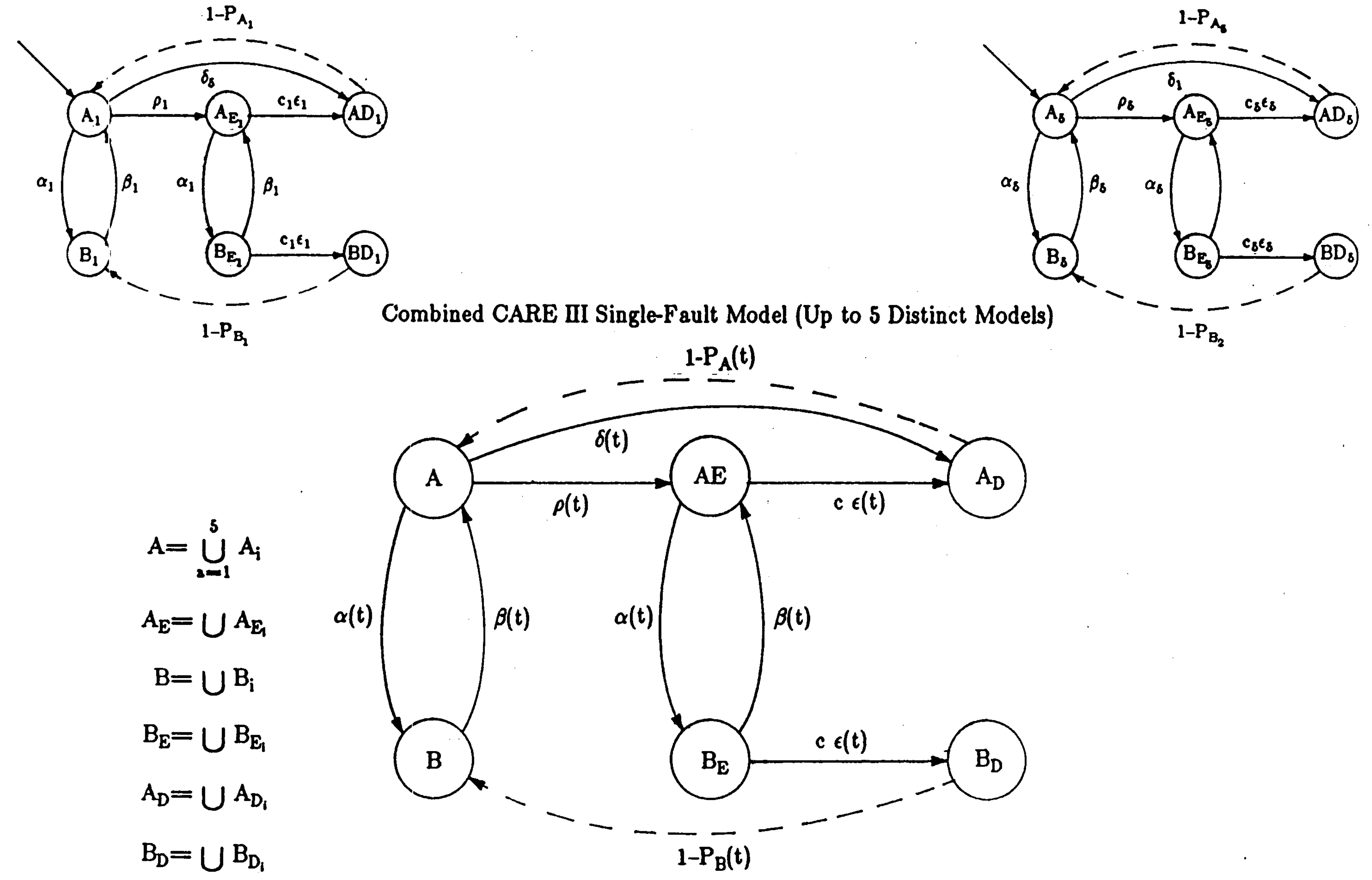
When a Transient Fault reaches the B state, CARE III reconfigures the system to its status prior to the occurrence of the fault (i.e., it treats the system as if the fault had never occurred).

In setting up the system model, the user has the option of defining five different single-fault models (i.e. the user may select five different sets of model parameters α, β, δ, ρ, P_A, P_B). In addition, the user may select a rate of entry (each with a Weibull distribution) for each of the five single-fault models. Let x_j denote the jth single fault model for stage x. Then the rate of entry into the single fault coverage model is given by

$$\lambda(t|x_j) = \lambda(x_j)\omega(x_j)t^{\omega(x_j)-1}.$$

These rates of entry may be different for each of the 70 possible stages accommodated by CARE III.

CARE III then aggregates the single-fault models associated with each stage into one single-fault model by OR-ing the A States, the B States, etc. of Figure 3.3. The resultant aggregate model is non-homogeneous. The aggregation is illustrated in Figure 3.4. CARE III provides the additional option of allowing the user to select non-constant transition rates for δ, ρ and ϵ, corresponding to uniformly distributed sojourn functions.



Combined CARE III Single-Fault Model (Up to 5 Distinct Models)

$$A= \bigcup_{s=1}^{5} A_i$$

$$A_E= \bigcup A_{E_i}$$

$$B= \bigcup B_i$$

$$B_E= \bigcup B_{E_i}$$

$$A_D= \bigcup A_{D_i}$$

$$B_D= \bigcup B_{D_i}$$

Figure 3.4. Combined Single Fault Model

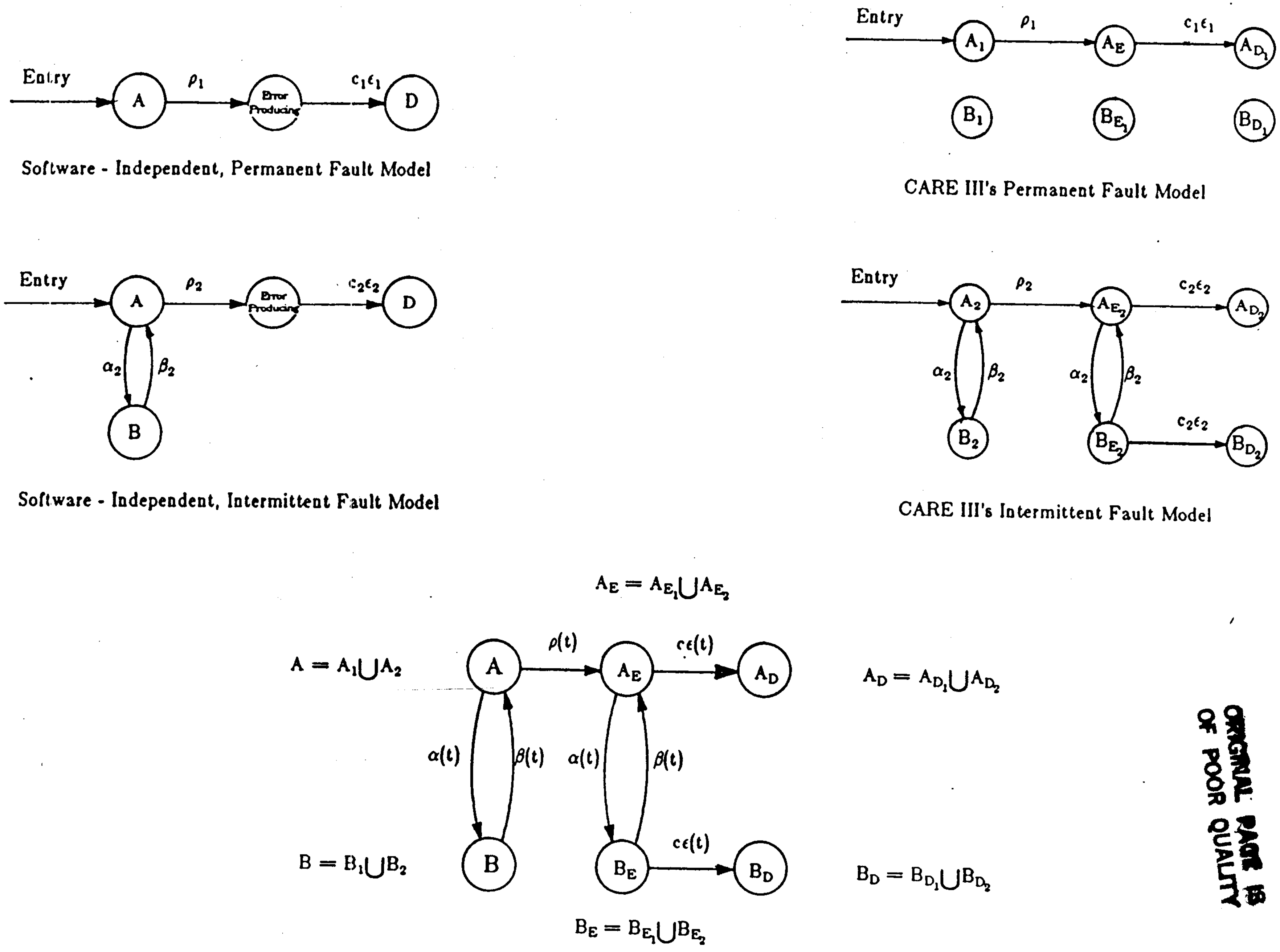
In order to illustrate CARE III's technique for defining single-fault models, consider a single-stage system that may experience two types of faults: permanent and intermittent. The corresponding fault-models are shown in Figure 3.5. For each fault type, the user must define the parameters α, β, c, ϵ, ρ, P_A, P_B. For the permanent fault, $\alpha = \beta = 0$. For the intermittent fault, $\alpha \neq 0, \beta \neq 0$. The user must also define the rate of occurrence associated with each fault type. This is done by selecting a pair of Weibull parameters for each fault type. Figure 3.5 also illustrates the aggregation of the two models into one single-fault model. For example, the aggregated transitions $\alpha(t)$, $\rho(t)$ are derived from the two models as

$$\alpha\left(t\right) = \frac{\alpha_1 P_{A_1}\left(t\right) + \alpha_2 P_{A_2}\left(t\right)}{P_{A_1}\left(t\right) + P_{A_2}\left(t\right)}$$

$$\rho\left(t\right) = \frac{\rho_1 P_{A_1}\left(t\right) + \rho_2 P_{A_2}\left(t\right)}{P_{A_1}\left(t\right) + P_{A_2}\left(t\right)} .$$

3.3.1.1.2 The Double-Fault Model

A potential cause of loss of control is the occurrence of a fault in one component of a redundant set in close time proximity with a previous, but independent, fault in a different component. These combinations are near-coincident faults and are only considered potentially catastrophic if both faults are simultaneously either active or producing an error. CARE III accommodates near-coincident double-faults by allowing the user to designate which modules are vulnerable to double-faults ("critical pairs" in CARE III's terminology). The modules may be paired within a stage or across two stages. CARE III, however, does not handle near-coincident triple, quadruple, etc. fault combinations. The double-fault model is shown in Figure 3.6.



Software - Independent, Permanent Fault Model

CARE III's Permanent Fault Model

Software - Independent, Intermittent Fault Model

CARE III's Intermittent Fault Model

ORIGINAL PAGE IS OF POOR QUALITY

Figure 3.5. Corresponding CARE III Aggregated Single-Fault Model

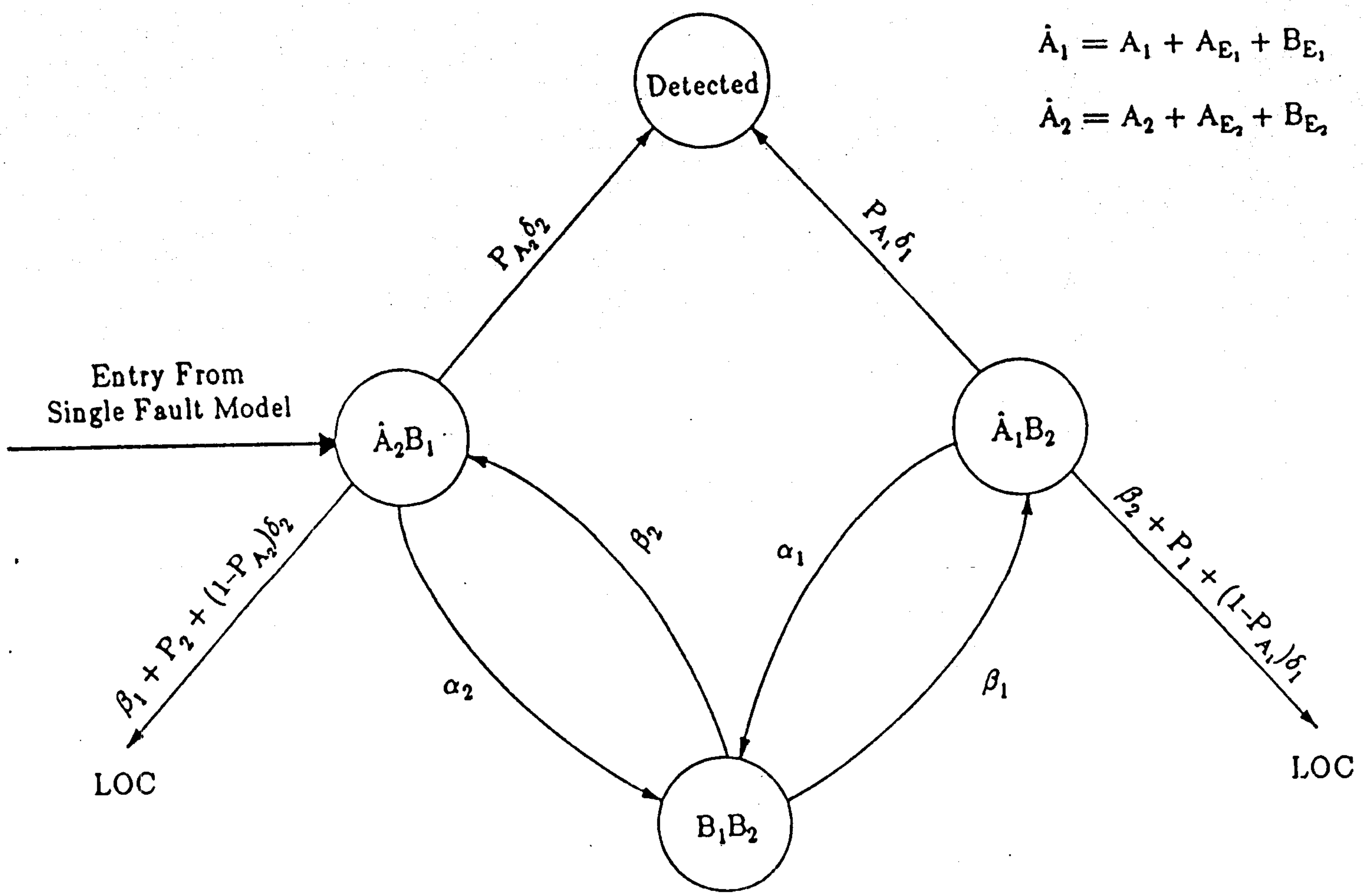


Figure 3.6. Double-Fault Model of CARE III

The fault-handling procedure is as follows:

1. A single fault occurs. If a second fault occurs while the first fault is in one of the states A, A_E or B_E, then CARE III assumes that this constitutes a system failure.

2. If, however, the first fault is in the B state upon the occurrence of the second fault, then state $\hat{A}_2B_1$ of the double-fault model will be entered ($\hat{A}$ as the union of states A, A_E, B_E of the single-fault model). If the detected state is entered, CARE III will configure out the faulty module.

It is important to note that the transitions of the double-fault model are completely determined by those of the single-fault model. Effectively, CARE III assumes that the processes which cause the transitions of the single-fault model are independent across modules. The single and double-fault models are incorporated in combination in the CARE III stage representation as shown in Figure 3.7. It is assumed that near-coincident, double, critical faults always result in loss of system, and no accommodation is made for near-coincident triple or larger combinations of critical faults.

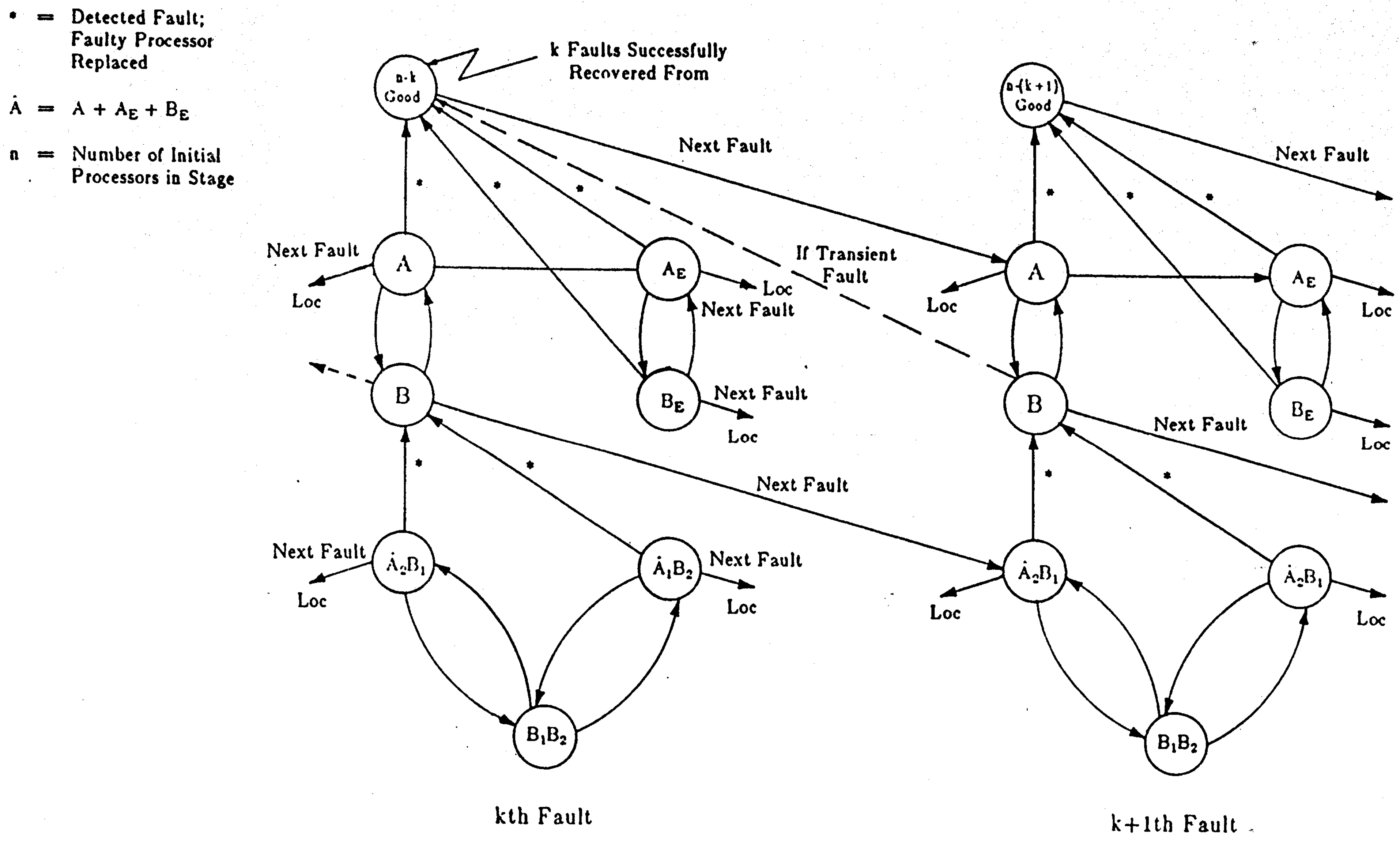

• = Detected Fault; Faulty Processor Replaced
Ȧ = A + A_E + B_E
n = Number of Initial Processors in Stage
k Faults Successfully Recovered From
n-k Good
n-(k+1) Good
Next Fault
If Transient Fault
A
A_E
B
B_E
Loc
Ȧ_2B_1
Ȧ_1B_2
B_1B_2
*
kth Fault
k+1th Fault

Figure 3.7. State Structure of a Stage as Represented by CARE III

3.3.1.2 Reliability Model

In the reliability model, the aggregate states are indexed by a set $\mathbf{L}$ of fault vectors $\underline{l}$, where

$$\underline{l} = (l(1), l(2), \ldots, l(N)),$$
$$l(x) = \text{number of failed modules in } x\text{th stage, and}$$
$$0 \le l(x) \le n(x) \text{ and } 1 \le x \le N.$$

The set $\mathbf{L}$ can be decomposed into two sets L and $\bar{L}$ such that the system is operational for $\underline{l} \in L$ and failed for $\underline{l} \in \bar{L}$ and $\mathbf{L} = L \cup \bar{L}$. The aggregate states can then be grouped into the sets $H(\underline{l})$, $G(\underline{l})$, and $F(\underline{l})$ as follows:

for $\underline{l} \in \bar{L}$:

$$H(\underline{l}) = \left\{ (\underline{d},\underline{i},\underline{c}) : \sum_a d(x,a) = l(x),\ 1 \le x \le N \right\}$$

for $\underline{l} \in L$:

$$G(\underline{l}) = \left\{ \begin{array}{l} (\underline{d},\underline{i},\underline{c}) : \sum_a d(x,a) = l(x),\ 1 \le x \le N \text{ and} \\ \underline{c} \text{ does not specify any coverage failures} \end{array} \right\}$$

$$F(\underline{l}) = \left\{ \begin{array}{l} (\underline{d},\underline{i},\underline{c}) : \sum_a d(x,a) = l(x),\ 1 \le x \le N \text{ and} \\ \underline{c} \text{ specifies at least one coverage failure} \end{array} \right\}.$$

$H(\underline{l})$ is the set of states in which the system has failed due to spares exhaustion; $G(\underline{l})$, the states in which the system is operational; and $F(\underline{l})$, the states in which the system has failed due to coverage failure. Given that the reliability of the system at time t is

$$\begin{aligned} R(t) &= P(\text{system is in state } G(\underline{l}) \text{ at time } t, \underline{l} \in L) \\ &= P(X(t) = G(\underline{l})) \end{aligned}$$

and letting $P(t|\underline{l})$ denote $P(X(t)=G(\underline{l}))$, $Q(t|\underline{l})$ denote $P(X(t)=F(\underline{l}))$, and $S(t|\underline{l})$ denote $P(X(t)=H(\underline{l}))$, the reliability of the system is

$$\begin{aligned} R(t) &= \sum_{\underline{l}\epsilon L} P(t|\underline{l}) \\ &= 1 - \sum_{\underline{l}\epsilon L} Q(t|\underline{l}) - \sum_{\underline{l}\epsilon \bar{L}} S(t|\underline{l}). \end{aligned}$$

3.3.2 Solution Method

Given that for a fault vector $\underline{l}$, $\underline{l}+\underline{1}(y)$ is $\underline{l}$ with one more fault in stage y, the possible transitions between the aggregate states are

(a) $\underline{l}\epsilon L$: $G(\underline{l})$ to $F(\underline{l})$,
(b) $\underline{l}\epsilon L$ and $\underline{l}+\underline{1}(y)\epsilon L$: $G(\underline{l})$ to $G(\underline{l}+\underline{1}(y))$,
(c) $\underline{l}\epsilon L$ and $\underline{l}+\underline{1}(y)\epsilon L$: $G(\underline{l})$ to $F(\underline{l}+\underline{1}(y))$,
(d) $\underline{l}\epsilon L$ and $\underline{l}+\underline{1}(y)\epsilon \bar{L}$: $G(\underline{l})$ to $H(\underline{l}+\underline{1}(y))$,and
(e) $\underline{l}\epsilon \bar{L}$ and $\underline{l}+\underline{1}(y)\epsilon \bar{L}$: $H(\underline{l})$ to $H(\underline{l}+\underline{1}(y))$.

Note that there are no transitions from $F(\underline{l})$ states since these states are absorbing.

Denoting these rates as $\mu(t|\underline{l})$ for (a); $\lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y))$ for (b); $\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{1}(y))$ for (c); and $\lambda^{*}(t|\underline{l}, \underline{l}+\underline{1}(y))$ for (d) and (e), the forward differential equations for the system are

$$\begin{aligned} \frac{d}{dt}P(t|\underline{l}) &= -P(t|\underline{l})\lambda(t|\underline{l}) + \sum_{x} P(t|\underline{l}-\underline{1}(x))\lambda^{(1)}(t|\underline{l}-\underline{1}(x),\underline{l}), \\ \frac{d}{dt}Q(t|\underline{l}) &= P(t|\underline{l})\mu(t|\underline{l}) + \sum_{x} P(t|\underline{l}-\underline{1}(x))\lambda^{(2)}(t|\underline{l}-\underline{1}(x),\underline{l}), \text{and} \qquad (1) \\ \frac{d}{dt}S(t|\underline{l}) &= -S(t|\underline{l})\lambda^{*}(t|\underline{l}) + \sum_{x} [P(t|\underline{l}-\underline{1}(x)) + S(t|\underline{l}-\underline{1}(x))]\lambda^{*}(t|\underline{l}-\underline{1}(x),\underline{l})], \end{aligned}$$

where

$$\lambda(t|\underline{l}) = \mu(t|\underline{l}) + \sum_{x}\lambda^{*}(t|\underline{l}, \underline{l}+\underline{1}(x))$$

and

$$\lambda^{*}(t|\underline{l}) = \lambda(t|\underline{l}) - \mu(t|\underline{l}).$$

Considering the conditions governing transitions b and c,

$$\lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y)) + ,\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{1}(y)) = ,\text{and}\lambda^{*}(t|\underline{l}, \underline{l}+\underline{1}(y)).$$

Furthermore, due to the high reliability of the systems modeled by CARE III, $\lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y))$ and $\lambda(t|\underline{l})$ must generally be much larger than $\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{1}(y))$ and $\mu(t|\underline{l})$, respectively. Therefore,

$$\begin{aligned}\lambda^{*}(t|\underline{l}) &= \lambda(t|\underline{l}) - \mu(t|\underline{l})\\ &\approx \lambda(t|\underline{l})\end{aligned}$$

and

$$\begin{aligned}\lambda^{*}(t|\underline{l}, \underline{l}+\underline{1}(y)) &= \lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y)) + \lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{1}(y))\\ &\approx \lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y)).\end{aligned}$$

For computation of system unreliability, it is necessary to compute the $Q(t|\underline{l})$ occupancy probabilities. If the transitions $\mu(t|\underline{l})$, $\lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{1}(y))$, and $\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{1}(y))$ were known, then the $P(t|\underline{l})$'s and, hence, $Q(t|\underline{l})$'s could be solved for by simple quadratures. Schematically, the aggregated states of the stage model are shown in Figure 3.8. Let

$s_1, s_2, \ldots, s_n$ = states of the $\underline{l}$-th operational model,
$p_1, p_2, \ldots, p_n$ = corresponding occupancy probabilities,and
$\delta_1, \delta_2, \ldots, \delta_n$ = corresponding exit transitions .

It can be shown that

$$\dot{p}_1 + \dot{p}_2 + \cdots + \dot{p}_m = -\sum_{i=1}^{m}\delta_i p_i + G(t) \ ,$$

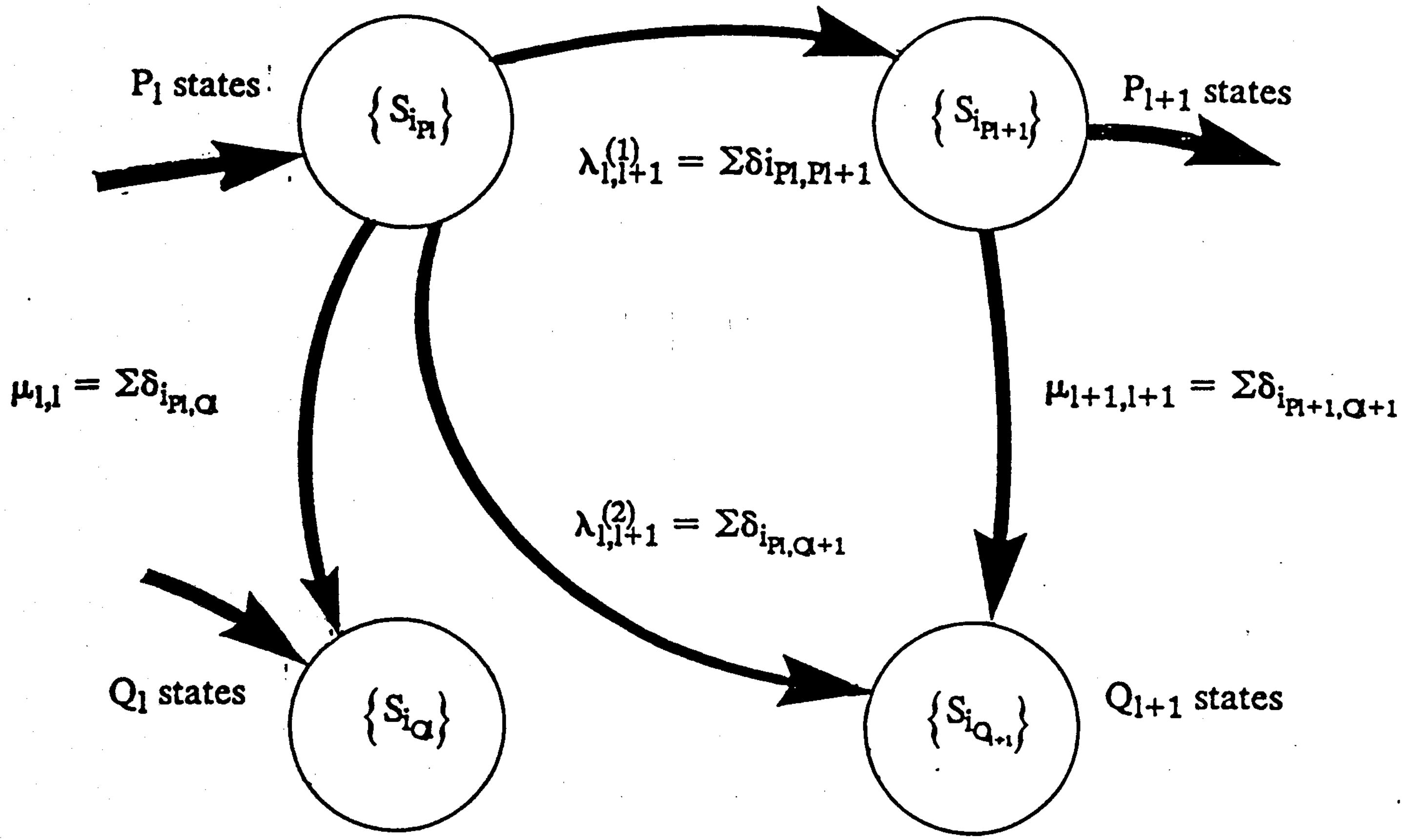

P_l states
$\{S_{i_{Pl}}\}$
$\lambda^{(1)}_{l,l+1} = \Sigma\delta i_{Pl,Pl+1}$
$\{S_{i_{Pl+1}}\}$
P_{l+1} states
$\mu_{l,l} = \Sigma\delta_{i_{Pl,Ql}}$
$\mu_{l+1,l+1} = \Sigma\delta_{i_{Pl+1,Ql+1}}$
$\lambda^{(2)}_{l,l+1} = \Sigma\delta_{i_{Pl,Ql+1}}$
Q_l states
$\{S_{i_{Ql}}\}$
$\{S_{i_{Ql+1}}\}$
Q_{l+1} states

Figure 3.8. Schematic of Aggregated States of Stage Model

where G(t) is a linear combination of the occupancy probabilities of the previous (i.e, l-1) operational model. It is important to note that G is independent of the occupancy probabilities of the l+1 operational model.

Accordingly, the aggregated occupancy probability P_l is

$$\dot{P}(t|l) = p_1 + p_2 + \cdots + p_n$$

and

$$\dot{P}(t|l) = -P(t|l)\lambda(t|l) + G \ , \tag{4}$$

where

$$\lambda(t|l) = -\frac{\sum_{i=1}^{m} \delta_i p_i}{\sum_{i=1}^{m} p_i} \ . \tag{5}$$

The required transition probabilities are

$$\lambda^{(1)}(t|l, l+l(y)) = \frac{\sum_{i \in A} \delta_i p_i}{\sum_{i=1}^{m} p_i} , \tag{6}$$

$$\lambda^{(2)}(t|l, l+l(y)) = \frac{\sum_{i \in B} \delta_i p_i}{\sum_{i=1}^{m} p_i} , \tag{7}$$

and

$$\mu(t|l) = \lambda(t|l) - \lambda^{(1)}(t|l, l+l(y)) - \lambda^{(2)}(t|l, l+l(y)) \ . \tag{8}$$

Since the computation of $p_1(t)$, $p_2(t)$, ..., $p_n(t)$ would require the solution of the entire model, alternate expressions for the occupancy probabilities are obtained by solving the model in isolation from the rest of the system.

Assuming that the l-th operational model was entered at time τ, then, if the initial conditions are known, the occupancy probabilities of the internal states $s_1, s_2, \ldots, s_m$ can be found. Let these probabilities be denoted by

$$\hat{p}_1(t-\tau),\ \hat{p}_2(t-\tau),\ \ldots,\ \hat{p}_m(t-\tau).^{3}$$

Then

$$p_i(t) = \int_{\tau}^{t} \hat{p}_i(t-\tau)\mathrm{Prob}[\text{operational model was entered in } (\tau,\tau+d\tau)] \ . \qquad (9)$$

Although the Prob[operational model was entered in $(\tau,\tau+d\tau)$] is not known, an approximate value can be found by assuming that coverage is perfect; i.e, that system failure is due entirely to exhaustion of components. Let $P^{*}_{l-1}(t)$ be the probability that the system is operational after l-1 faults; then $P^{*}_{l-1}(t)$ can be obtained by combinatorial methods; i.e,

$$P^{*}(t|\underline{l}) = \prod_{x} \binom{n(x)}{l(x)} \Big[1 - r(t|x)\Big]^{l(x)} \Big[r(t|x)\Big]^{n(x)-l(x)},$$

where $r(t|x) = \exp\left[-\int_{0}^{t}\sum_{i}\lambda(u|x_i)du\right]$ denotes the reliability of a module in stage x. Let η_l be the rate of the next fault. In general, η_l will be a function of the fault rate[4], λ, of each module and l; e.g., in a triplex voting system with spares, $\eta_l = 3\lambda$ where λ = the failure rate of a single module. Then,

$$\mathrm{Prob}[l-\text{th model was entered in } (\tau,\tau+d\tau)] \approx P^{*}_{l-1}(\tau)\eta_l(\tau)d\tau \qquad (10)$$

[3] t represents global time; t - τ, local time

[4] this rate could be Weibull distributed, in which case η_l is also a function of t

(η_l is a function of τ for a Weibull distribution).

Note that $P^*_{l-1}(\tau)$ is the probability that the system has experienced exactly l-1 faults at time τ and has survived to time τ.

Accordingly, from (9),

$$p_i(t) \approx \int_{\tau=0}^{t} \hat{p}_i(t-\tau)P^*_{l-1}(\tau)\eta_l d\tau \tag{11}$$

and, from (7),

$$\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{l}(y)) \approx \frac{\sum_{i\in B}\delta_i(t) \int_{\tau=0}^{t} \hat{P}_i(t-\tau)P^*_{l-1}(\tau)\eta_l d\tau}{\sum_{\text{all } i} \int_{\tau=0}^{t} \hat{P}_i(t-\tau)P^*_{l-1}(\tau)\eta_l d\tau} , \tag{12}$$

and similarly for $\lambda^{(1)}(t|\underline{l}, \underline{l}+\underline{l}(y))$.

Thus, to obtain the desired transitions,

(1) For each l, compute $\hat{p}_1(t-\tau)$, $\hat{p}_2(t-\tau)$, $\cdots$.

(2) Compute $P^*_{l-1}(\tau)\eta_l(\tau)$.

(3) Evaluate the integrals (11).

(4) Compute the transitions according to (12).

In actual practice, CARE III makes another approximation in the computation of $\lambda^{(2)}(t|\underline{l}, \underline{l}+\underline{l}(y))$: since (11) can be rewritten as

$$p_i(t) \approx \int_{x=0}^{t} \hat{p}_i(x)P^*_{l-1}(t-x)\eta_l(t-x)dx$$

and, in practice, $P^*_{l-1}(t)$ is a much more slowly varying function than $\hat{p}_i(x)$, P^*_{l-1} can be approximated by

$$P^*_{l-1}(t-x) \approx a(t) + xb(t) + x^2c(t) \tag{13}$$

over the range of x in which $\hat{\rho}_i(x)$ is significantly different from zero.

Substituting these transition rates, which are perfect coverage rates, in the equation for $P(t|\underline{l})$, yields the equation

$$\frac{d}{dt}P^*(t|\underline{l}) = -P^*(t|\underline{l})\lambda^*(t|\underline{l}) + \sum_x P^*(t|\underline{l}-\underline{1}(x))\lambda^*(t|\underline{l}-\underline{1}(x), \underline{l})$$

for the probability of $\underline{l}$ faults at time t, given perfect coverage.

Replacing $P^*(t|\underline{l})$ for $P(t|\underline{l})$ in the equations for $Q(t|\underline{l})$ and $S(t|\underline{l})$ results in

$$Q(t|\underline{l}) = \int_0^t \left[P^*(u|\underline{l})\mu(t|\underline{l}) + \sum_x P^*(u|\underline{l}-\underline{1}(x))\lambda^{(2)}(u|\underline{l}-\underline{1}(x), \underline{l})\right]du$$

and

$$S(t|\underline{l}) \approx P^*(t|\underline{l}).$$

Thus, CARE III can solve for the $Q(t|\underline{l})$'s without first solving for the $P(t|\underline{l})$'s and the reliability of the system can be computed as

$$R(t) = 1 - \sum_{\underline{l}\varepsilon L} Q(t|\underline{l}) - \sum_{\underline{l}\varepsilon L} P^*(t|\underline{l}).$$

4.0 TEST CASES

4.1 Introduction

In order to evaluate how well CARE III and ARIES can be used to assess the reliability of AIPS architectures, it was necessary to determine how useful and applicable these tools are. Also, since each tool has inherent limitations, it was necessary to determine how flexible each tool is with respect to accommodating systems that stress those limitations. Thus, several sample systems were selected to demonstrate the use of, applicability, limitations, and relative accuracy of CARE III and ARIES. These test cases do not test all of the features of each tool, nor do they attempt to verify the tools. In particular, they do not test all of the ARIES system types nor all of the performance measures that it computes. For CARE III, the impact of state aggregation in assessing very large systems, the full use of the fault handling model, and non-constant failure rates were not tested. These test case results coupled with the AIPS requirements serve as a basis for a relative assessment of the two reliability modeling tools.

The test cases range in complexity from a single processor architecture to a system suitable for flight control applications. Cases were selected to demonstrate relative strengths and weaknesses of the two modeling tools. Also, it was absolutely essential that accurate solutions could be obtained for the test cases. For each case a solution was obtained based on standard analysis techniques and subject to assumptions appropriate for the particular scenario and parameters. The solutions were calculated using simple computer programs. Other than the use of double precision variables, no special numerical techniques were employed to ensure the accuracy of the calculations. Consequently, the accuracy is limited to that inherent in double precision floating point arithmetic (64 bits) and in the numerical techniques used to compute the exponential function. Under these conditions it was determined that computation of $e^{-\lambda}$ for $\lambda<10^{-15}$ was subject to error. Since the probability of system failure on the order of 10^{-10} was of interest, the accuracy under these limitations was judged to be adequate. The test cases were then solved using CARE III and ARIES and the three results compared. Due to limitations in either CARE III or ARIES, results from only one of these models could be obtained for some cases. In addition, wherever feasible, the test cases were described as both Type 1 and Type 7 for ARIES systems and the results compared. It should be noted that ARIES reliability results are normally reported to only seven significant digits: to obtain results suitable for comparison, it was necessary to modify the AIRES code to output 17.

The test cases, solutions, results, and difficulties encountered are discussed in the following sections.

4.2 Simplex Processor

A simplex processor was analyzed to point out any computational, as opposed to modeling, differences. A constant failure rate of λ was assumed. The probability of failure (unreliability) for this system is given by:

$$P(SF) = 1-e^{-\lambda t} .$$

For small λt,

$$P(SF) \approx \lambda t\ .$$

The results for each method are summarized in the following table:

λt	Direct Calculation	ARIES 82*	CARE III
0	0	0	0
1.59×10^{-23}	-2.78×10^{-17}	0	1.59×10^{-23}
1.30×10^{-19}	-2.78×10^{-17}	0	1.30×10^{-19}
1×10^{-16}	6.94×10^{-17}	6.94×10^{-17}	9.99×10^{-17}
5×10^{-16}	4.85×10^{-16}	4.85×10^{-16}	5.00×10^{-16}
1×10^{-15}	9.99×10^{-16}	9.99×10^{-16}	1.00×10^{-15}
1×10^{-12}	9.99×10^{-13}	9.99×10^{-13}	9.99×10^{-13}
1×10^{-10}	9.99×10^{-11}	9.99×10^{-11}	1.00×10^{-10}
1×10^{-3}	9.995×10^{-4}	9.995×10^{-4}	9.995×10^{-4}
1	6.32×10^{-1}	6.32×10^{-1}	6.32×10^{-1}

* ARIES reports reliability. Unreliability was obtained by subtracting ARIES reliability answers from 1.

Observe that for $\lambda t \geq 10^{-15}$ all methods give the same answer. Also, note that CARE III continues to provide accurate results for much smaller values of λt.

The ability of CARE III to provide accurate answers stems from computing unreliability directly. Thus, computations involving very small differences between two numbers which are close to unity are avoided. This, in turn, avoids approaching the accuracy limitations imposed by finite arithmetic. In fact, CARE III uses single precision arithmetic where the direct calculation method and ARIES use double precision arithmetic.

While unimportant for this simple case, this distinction between CARE III and ARIES is important when analyzing more complex systems. Both accuracy and computation resource requirements are issues.

4.3 TMR

For the next case, a TMR system with no spares was chosen. The probability of system failure (P(SF)) for this system is given by

$$P(SF) = 1 + 2e^{-3\lambda t} - 3e^{-2\lambda t}.$$

The estimates of unreliability from the hand calculation, from CARE III, and from the two ARIES types agreed closely and are summarized in the following table:

t	Direct	ARIES 1	ARIES 7	CARE III
0	0	0	0	0
.01	2.99996139042E-12	2.99996E-12	2.99996E-12	2.9999939165E-12
.10	2.99995001063E-10	2.99995E-10	2.99995E-10	2.9999519535E-10
1	2.999500043E-8	2.999500043E-8	2.999500043E-8	2.9994993156E-8
5	7.4937529682E-7	7.4937529682E-7	7.4937529682E-7	7.4937446470E-7
10	2.99500474671E-6	2.99500474671E-6	2.99500474671E-6	2.9950040243E-6
7000	.50512196468	.50512196468	.50512196468	.50512194633

4.4 M out of N

The next system considered was an M out of N system; i.e., one in which failures in M units out of N beginning units causes system failure. For this case, a seven out of twelve system with perfect coverage was chosen. A failure rate of 10^{-4} per hour and a mission time of eight thousand hours were assumed. Using the standard combinatorial solution,

$$P(SF) = \sum_{k=7}^{12} \frac{12!}{k!(12-k)!} p^k q^{12-k}, \quad \text{where}$$
$$p = 1 - e^{-\lambda t} \quad \text{and}$$
$$q = e^{-\lambda t},$$

P(SF) of .5288303411826796 at t=8000 was expected.

In the initial attempts to solve this system as a Type 1, it was discovered that ARIES was not correctly computing systems with more than one degradation and no spares: the system would maintain perfect reliability for more than ten thousand hours before a sudden decrease of several orders of magnitude. In addition, the Type 1 results did not agree with the Type 7 results. Therefore, another modification was made to the ARIES code to produce reasonable reliability computations for the Type 1 system. Also, it was determined that an accuracy parameter had to be adjusted from its default value for an accurate computation of the Type 7 system.

For this particular scenario, the ARIES Type 1 solution was .52883034118268013 at t=8000; the Type 7 solution was .52883034118268137 at t=8000. Likewise, the CARE III solution was .52883034118 at t=8000. A graph of the unreliability estimates from CARE III, ARIES, and the direct calculation is included in Figure 4.1. This graph illustrates the close agreement among the three solutions for the computed time range.

4.5 Quintuplex

For this system, a failure rate of 10^{-4} per hour, a mission time of 10 hours, permanent faults, and imperfect coverage were assumed. System failure was defined to be the occurrence of four or more faults or the occurrence of a sufficient number of faults to preclude forming a majority from the remaining active processors. In defining the single fault model, it was assumed that (1) a fault is detected immediately as it produces an error, (2) single point faults are excluded and (3) only two concurrent active faults can cause system failure. Thus, for the CARE III single-fault model shown in Figure

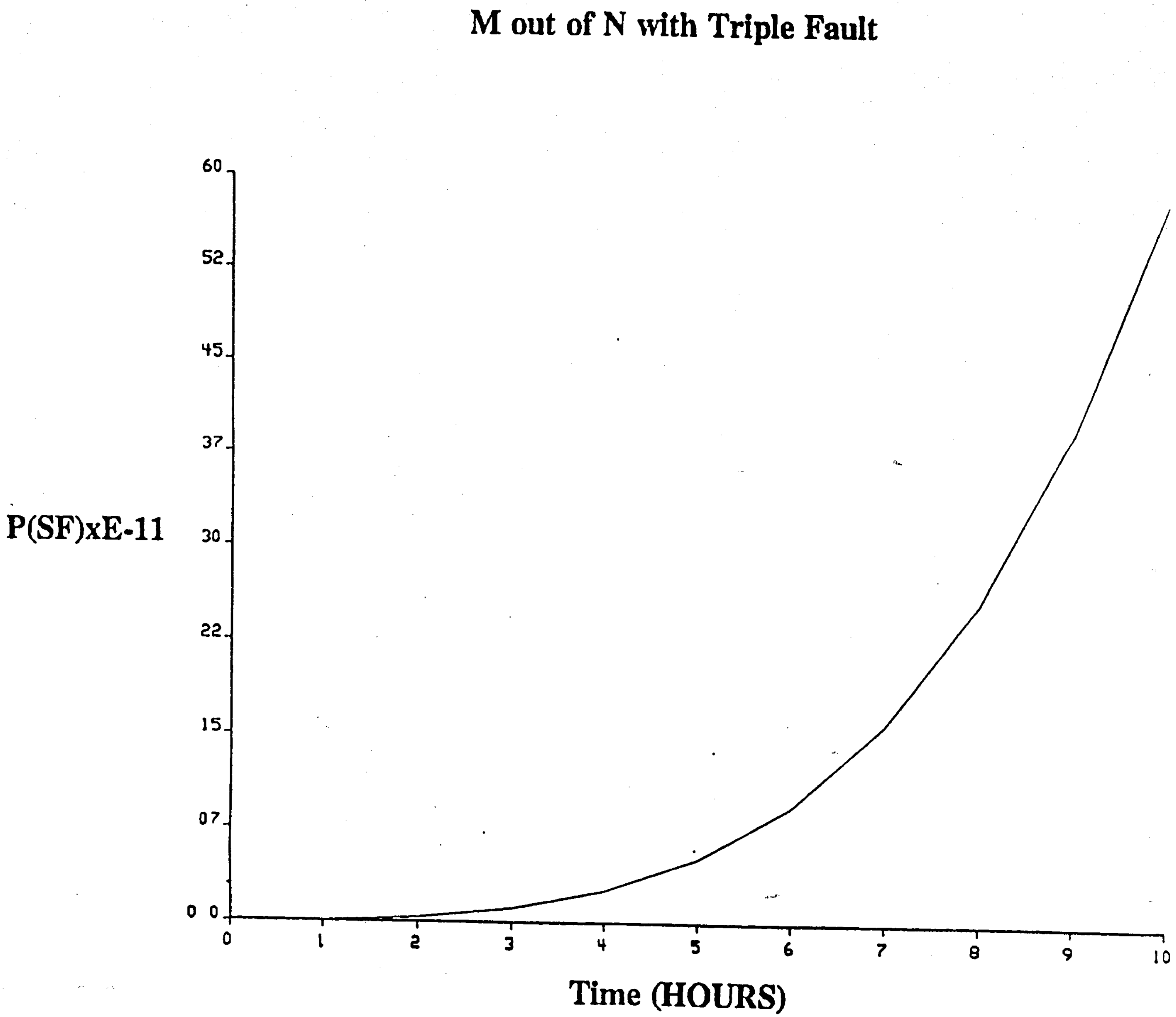


Figure 4.1. Test Case 3

3.3, P_A, P_B, ϵ, c, δ and ρ had to be selected consistent with these assumptions. It was also necessary that the selected parameters would result in a double-fault model consistent with these assumptions. Thus, the parameters were defined as follows:

$P_A = P_B = 1$,
$\epsilon = 0$,
$c = 1$,
$\rho = 0$, and
$\delta = 3600$/hour.

The resulting double-fault model is shown in Figure 3.6.

This system can be represented by the Markov model shown in Figure 4.2, where A is a single fault and AA is a double fault. In this model the path 5 good - A - AA - SF exposes the system to a triple fault during the recovery period, so that the probability of loss of three out of five in time t is approximately $30\frac{\lambda^3}{\delta^2}t$. Since the time spent in recovery is small relative to the failure rate, the fault recovery states can be approximated by instantaneous coverage. With the instantaneous coverage approximations, the model can be represented by the simplified model of Figure 4.3.

Since probability of loss of three out of five in time t is approximately $30\frac{\lambda^3}{\delta^2}t$, triple coincidences can be considered remote and can therefore be ignored. Thus, the dominant path to SF due to lack of coverage is 5-4-SF. Using Laplace transforms,

$$Lp\left[P_{cov}(SF)\right] \approx \frac{1}{S}\left(\frac{5\lambda}{S+4\lambda}\right)\left(\frac{4\lambda}{S+4\lambda}\right)c_1(1-c_2).$$

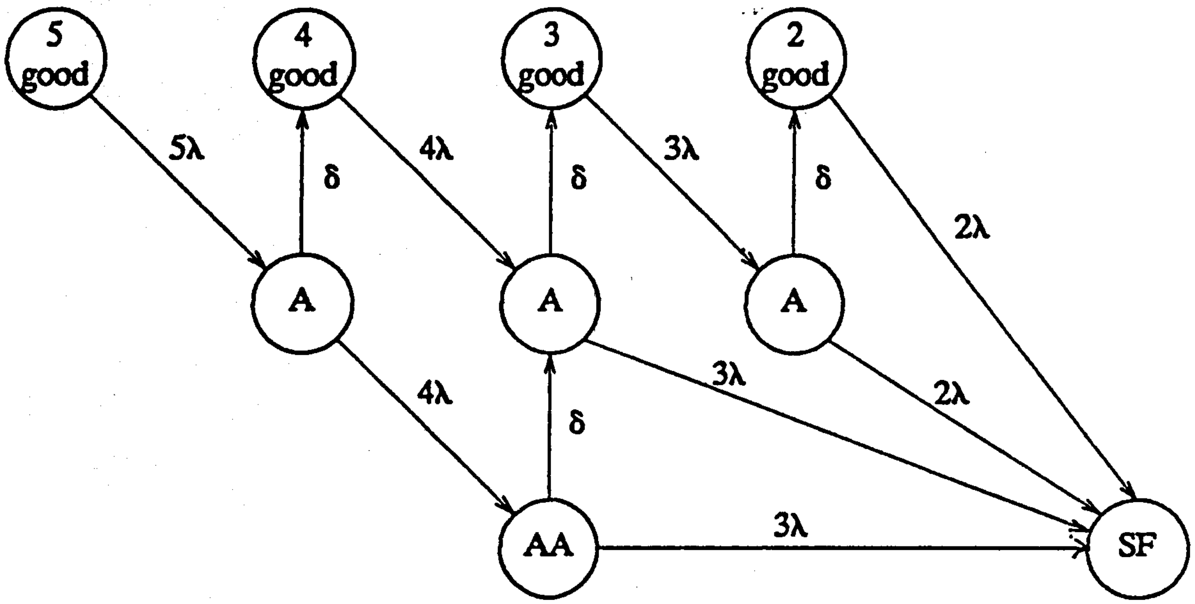
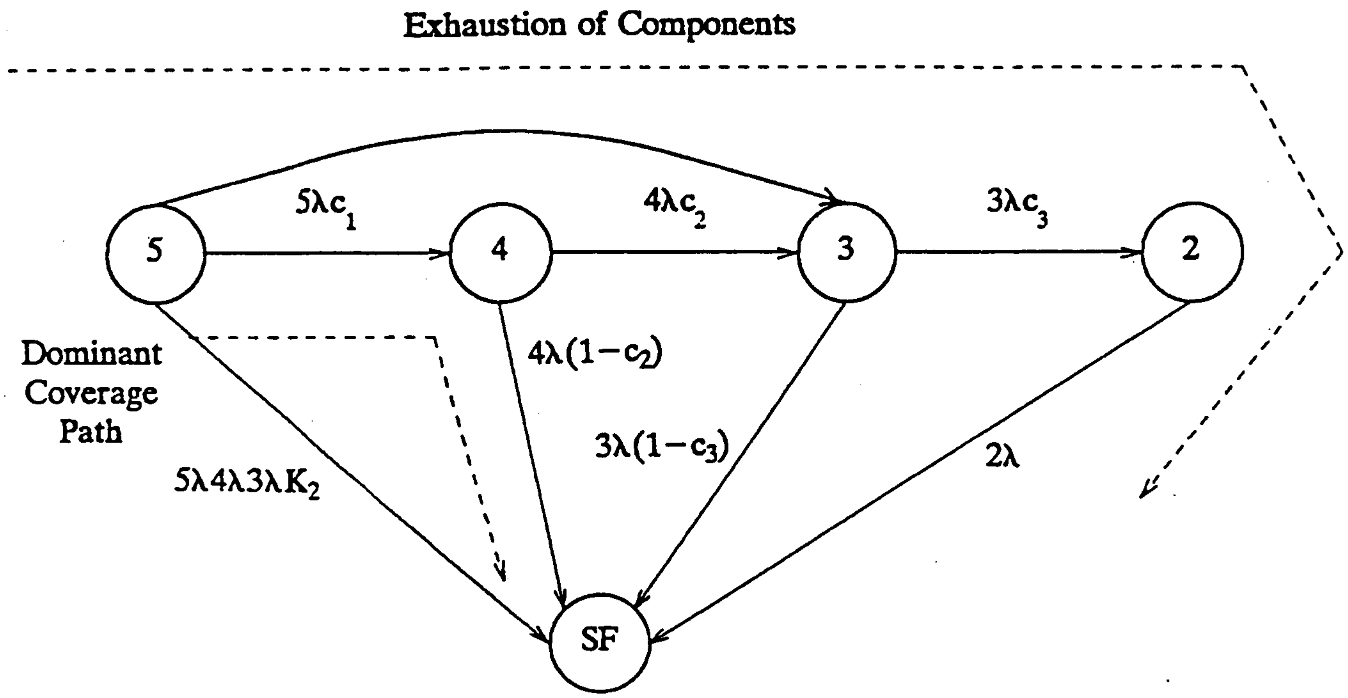


Figure 4.2. Markov Model for Test Case 4



$$c_1 = \frac{\delta}{\delta+4\lambda}$$

$$c_2 = \frac{\delta}{\delta+3\lambda}$$

$$c_3 = \frac{\delta}{\delta+2\lambda}$$

$$k_1 = \left(\frac{1}{\delta+4\lambda}\right)\left(\frac{2\delta}{2\delta+3\lambda}\right)$$

$$k_2 = \left(\frac{1}{\delta+4\lambda}\right)\left(\frac{1}{2\delta+3\lambda}\right)+\left(\frac{1}{\delta+4\lambda}\right)\left(\frac{2\delta}{2\delta+3\lambda}\right)\left(\frac{1}{\delta+3\lambda}\right)$$

Figure 4.3. Instantaneous Coverage Model for Test Case 4

By Partial Fraction Expansion and taking the inverse transform,

$$P_{cov}(SF) \approx c_1(1-c_2)\left[1-5e^{-4\lambda t} + 4e^{-5\lambda t}\right]$$

The exhaustion of components is approximately the failure of four out of five processors. Thus,

$$P(SF) \approx \frac{3\lambda}{8}\left[1-5e^{-4\lambda t} + 4e^{-5\lambda t}\right] + 5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t} + \left(1-e^{-\lambda t}\right)^5 .$$

For small λt,

$$P(SF) \approx \frac{30\lambda^3 t^2}{8} + 5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t} + \left(1-e^{-\lambda t}\right)^5 ,$$

so that at time $t=10$, $P(SF) = 5.81936x10^{-12}$.

For the CARE III analysis, this system was described as a one-stage system consisting of five active modules and requiring a minimum of two fault-free modules for continued operation. The system fault tree was described as consisting of one input and one output, where the output, system failure, is contingent upon the failure of the stage. A critical pair fault tree was also included specifying critical pairing between every two of the five stage modules. Since CARE III does not allow for the triple fault, the $P_{cov}(SF)$ computed by CARE III is dominated by the Q(2) probability, i.e., the probability of failure after two faults, and the P(SF) is therefore overestimated. However, taking the Q(3) component of the $P_{cov}(SF)$ computed by CARE III, which corresponds to the 5-4-SF coverage path of the model, and adding this to the P^* ($P_{exh}(SF)$ assuming perfect coverage) component computed by CARE III, yields

$$P(SF) = 8.221588319x10^{-12} + 4.9860181088x10^{-12} = 5.8181769407x10^{-12}$$

at time $t = 10$.

There is no transition in the ARIES model to correspcnd to the transition from 5 good to 3 good in this case. Thus, to construct an ARIES Type 1 description of this case, the system was approximated by subsuming the 5 good to 3 good path into the 5 good to 4 good path. Using this approximation, the P(SF) was computed to be $5.81801 \mathrm{x} 10^{-12}$ at time t = 10.

The full Markov model was initially used to construct an ARIES Type 7 system and the P(SF) was computed to be $5.83694 \mathrm{x} 10^{-12}$ at time t=10. However, when this same model was used with the states indexed so that the transition-rate matrix was upper triangular rather than tridiagonal, the P(SF) was incorrectly computed. The results from these two Type 7 descriptions are compared to the direct calculation in the following table:

t	Direct Calculation	ARIES Type 7	ARIES Type 7 Re-Indexed
0	0	0	$1.826535678 \times 10^{-8}$
1	8.83×10^{-15}	1.83×10^{-15}	$1.825623497 \times 10^{-8}$
5	5.2039×10^{-13}	5.1459×10^{-13}	$1.822027046 \times 10^{-8}$
10	5.81936×10^{-12}	5.83694×10^{-12}	$1.818007445 \times 10^{-8}$

Although the initial Type 7 estimate agrees fairly well with the direct calculation for t=10 hours, the re-indexed model yields completely inaccurate estimates. This demonstrates ARIES' sensitivity to the ordering of states.

Finally, the instantaneous coverage Markov model was used to construct an ARIES Type 7 system. For this model, the P(SF) was computed to be $5.81907 \mathrm{x} 10^{-12}$ at time t = 10. The graph included in Figure 4.4 illustrates the close agreement among the estimates from this Type 7 description, the Type 1, the CARE III, and the direct calculation.

4.6 TMR with Powered Spares and Permanent Faults

The fifth system considered was a TMR with two powered spares and permanent faults. For this system, a failure rate of 10^{-4} per hour, a mission time of 10 hours, and imperfect coverage were assumed. In defining the single fault model, the parameters were selected as before so that

$$\begin{aligned} &P_A = P_B = 1, \\ &\epsilon = 0, \\ &c = 1, \\ &\rho = 0, \quad \text{and} \\ &\delta = 3600/\text{hour}. \end{aligned}$$

This system can be represented by the Markov model shown in Figure 4.5. Using instantaneous coverage, the model can be represented by the simplified model shown in Figure 4.6. Since the dominant path to SF due to lack of coverage is (3,2) - SF,

$$P_{cov}(SF) \approx (1-c)(1 - e^{-3\lambda t}).$$

P(SF) due to exhaustion of components is the probability of loss of four out of five, so that

$$P_{exh}(SF) \approx 5(1 - e^{-\lambda t})^4 e^{-\lambda t} + (1 - e^{-\lambda t})^5 \ .$$

Thus,

$$P(SF) \approx \frac{6\lambda^2 t}{\delta} + 5(1 - e^{-\lambda t})^4 e^{-\lambda t} + (1 - e^{-\lambda t})^5 \ .$$

Then for $\lambda = 10^{-4}$, $\mu = 3600$ per hour and $t = 10$ hours, $P(SF) = 1.7165269 \times 10^{-10}$.

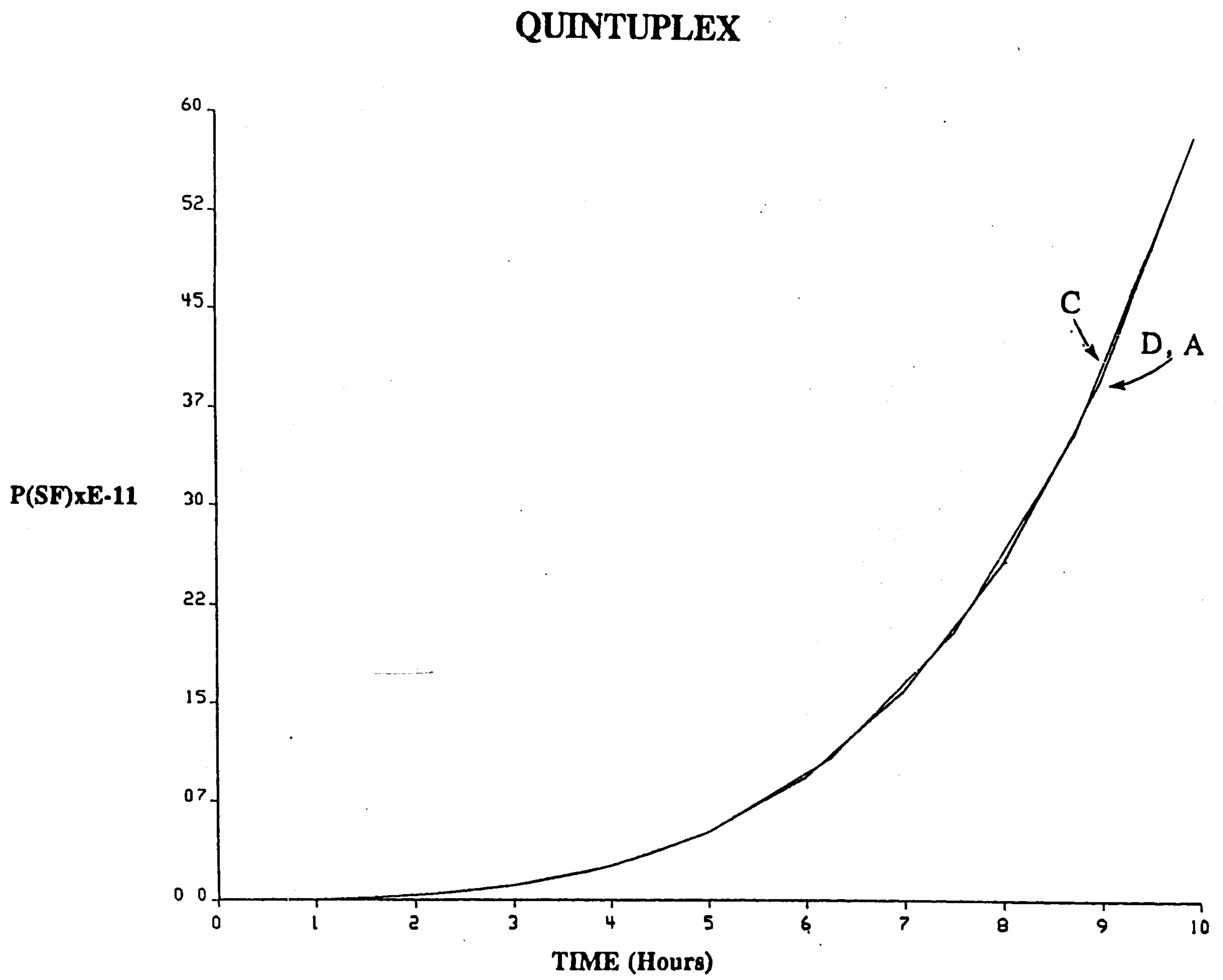


Figure 4.4. Test Case 4

Model

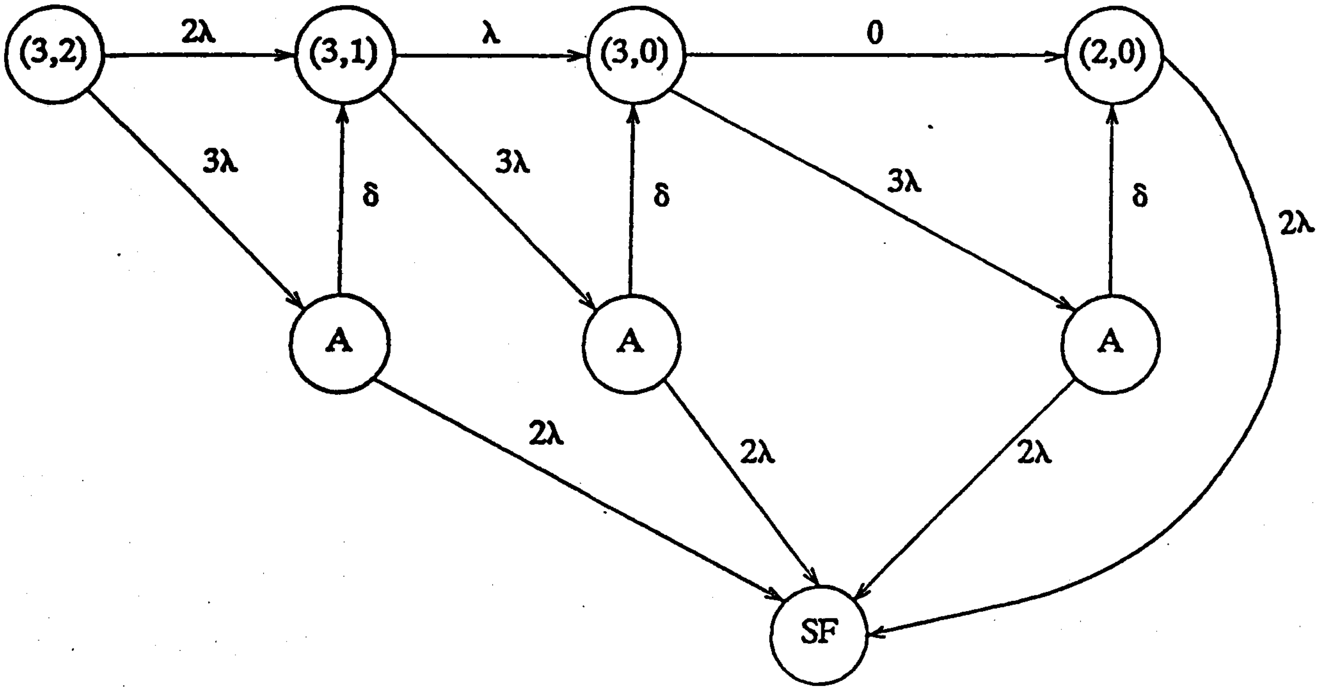
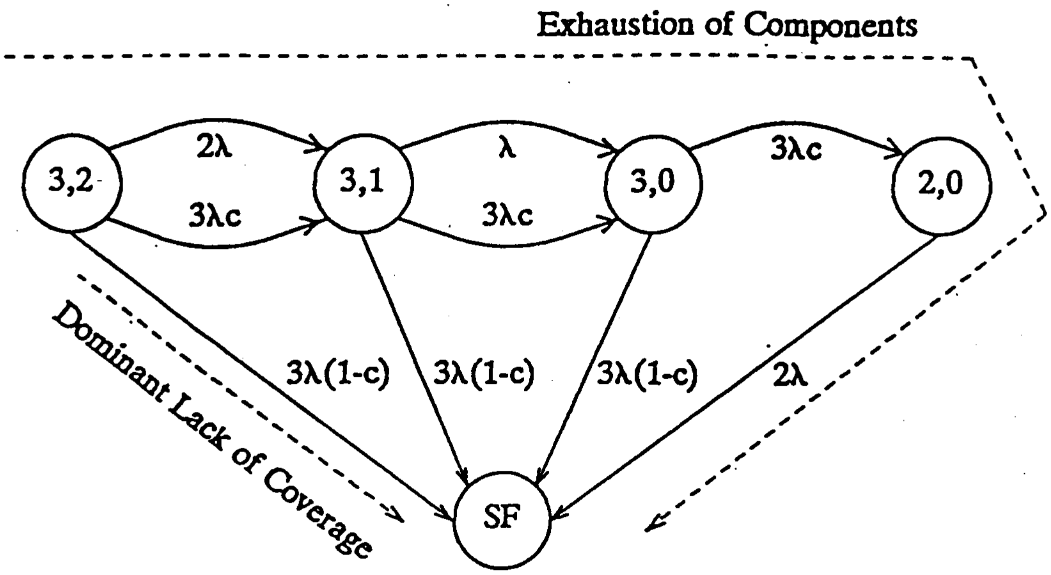


Figure 4.5. Markov Model for Test Case 5



$$(1\text{-}c) = \frac{2\lambda}{2\lambda + \delta} \simeq \frac{2\lambda}{\delta}$$

Figure 4.6. Instantaneous Coverage Model for Test Case 5

For the CARE III analysis, this system was described as a one-stage system consisting of five active modules and requiring a minimum of two fault-free modules for continued operation. The configuration of this system into three active and two powered spare units was specified by means of the NOP parameter. The system fault tree was described as consisting of one input and one output, where the output, system failure, is contingent upon the failure of the stage. A critical pair fault tree was also included specifying critical pairing between every two of the five stage modules. With this system description and assuming an active unit failure rate of 10^{-4} and a mission time of 10 hours, CARE III computed the P(SF) to be $1.7191249813 \text{x} 10^{-10}$.

For the ARIES analysis, the system was described first as a Type 7 and then as a Type 1. The instantaneous coverage Markov model was used to construct the transition matrix for the Type 7 analysis and the P(SF) was computed to be $1.716543 \text{x} 10^{-10}$ at time $t = 10$. For the Type 1 analysis the system was described as starting with three active units and two spares and able to sustain one degradation (or reconfiguration). The active and spare failure rates were specified to be 10^{-4} per hour and the coverage parameters for the possible system configurations were computed from the instantaneous coverage Markov model. With this system description, the P(SF) was computed to be $1.7165291 \text{x} 10^{-10}$ at time $t = 10$.

A graph of the results is included in Figure 4.7a. This graph illustrates the close agreement among the estimates from CARE III, ARIES, and the direct calculation. Figure 4.7b shows the results obtained from an earlier version of CARE III. CARE III estimates oscillate and are offset from the direct calculation.

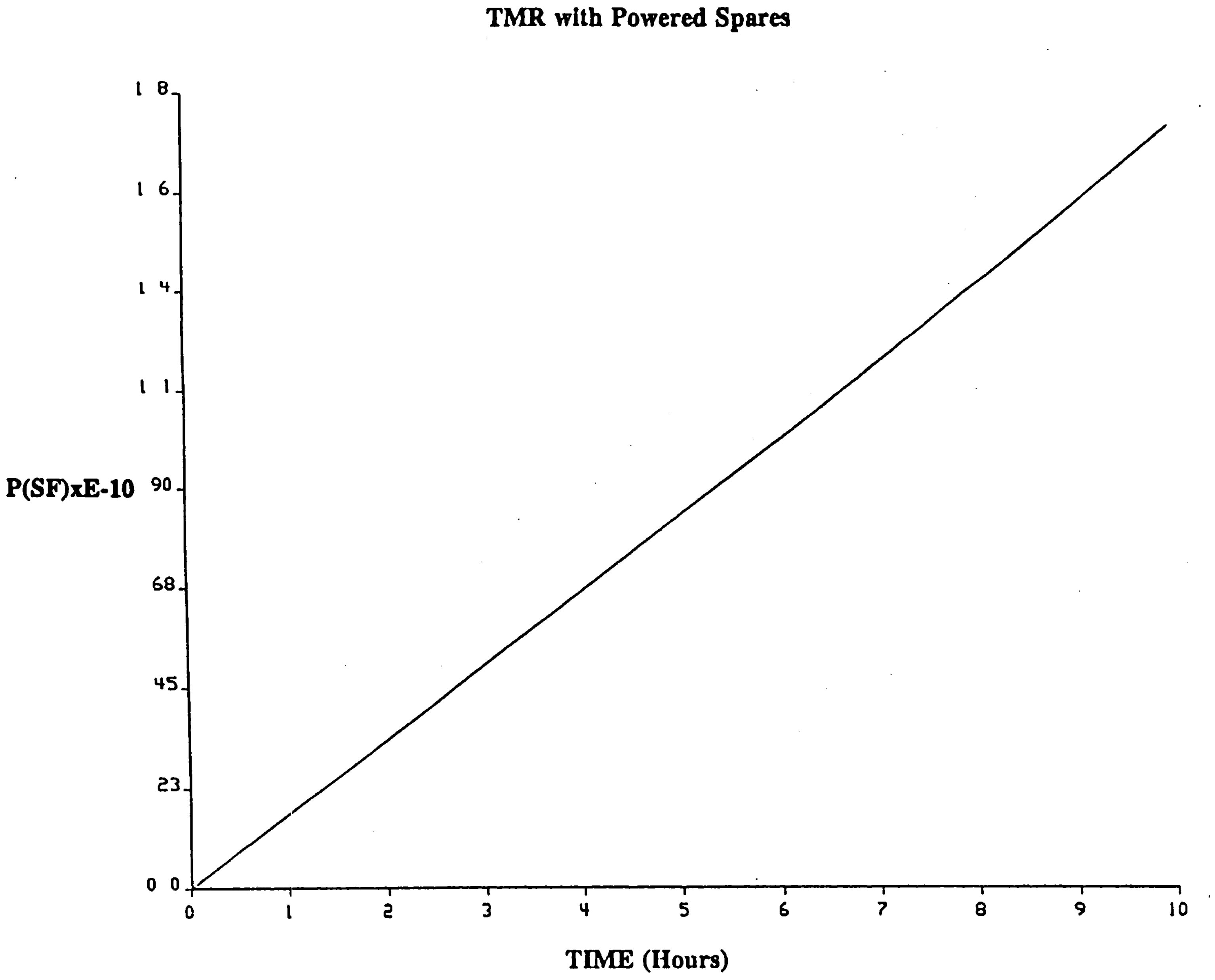


Figure 4.7a. Test Case 5

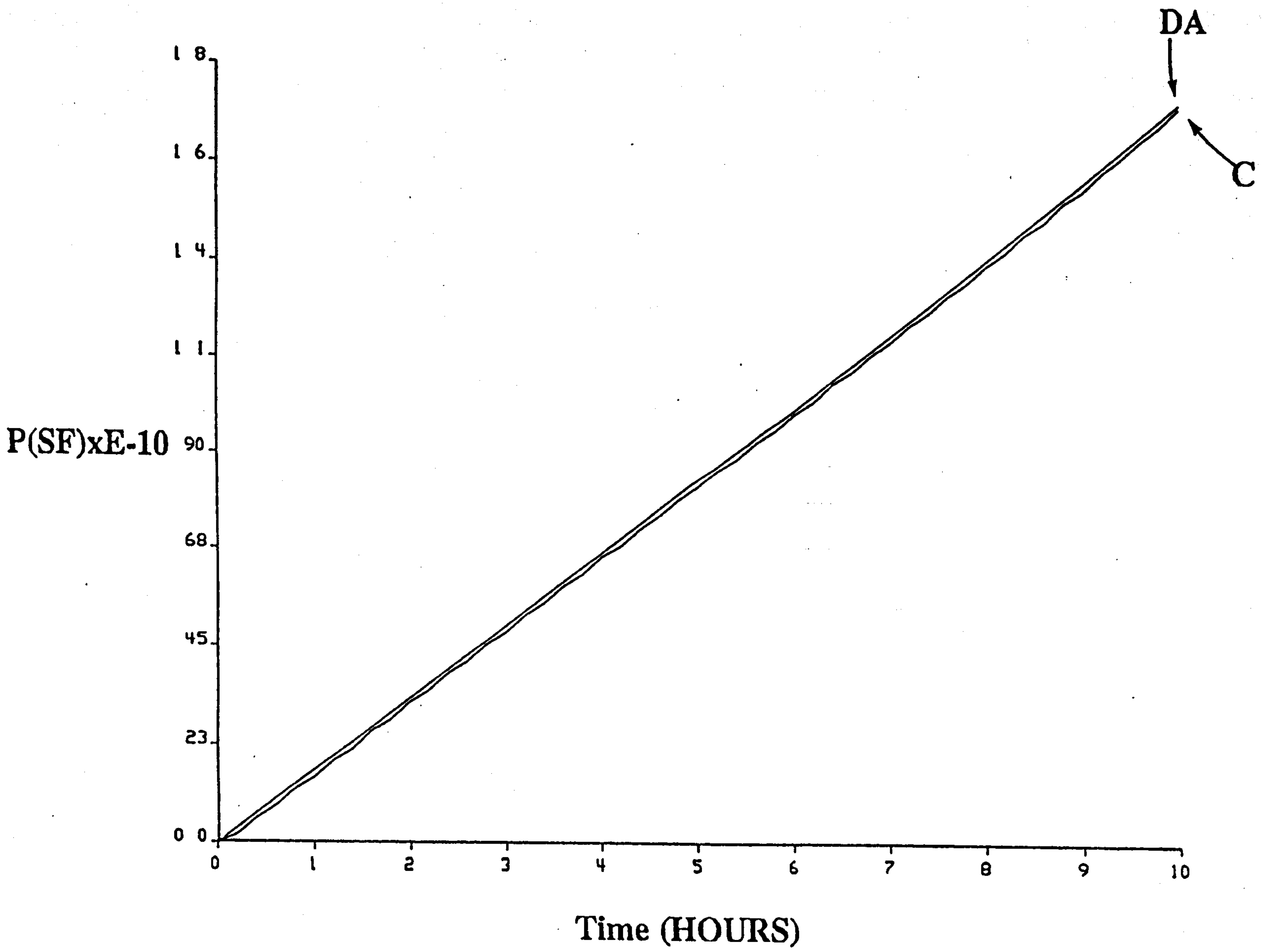


Figure 4.7b. TMR with Powered Spares
(Early Version of CARE III)

4.7 TMR with Unpowered Spares

For the sixth system, a TMR with seven unpowered spares and permanent faults was chosen. A failure rate of 10^{-4} per hour, a mission time of 10 years = 87,600 hours, and imperfect coverage were assumed. The single fault model parameters are the same as for Test Case 4.

Since the spares are unpowered, it was assumed that the failure rate for a spare is zero until that spare is switched in to replace a failed active module. After the spare becomes active, its failure rate is the same as that of an active module. This system is represented by the Markov model shown in Figure 4.8. Approximating the fault recovery states with instantaneous coverage as before, the model can be represented by the simplified model in Figure 4.9.

Using Laplace transforms, the P(SF) due to lack of coverage is

$$\begin{aligned} \mathrm{Lp}\left[P_{cov}(SF)\right] &= \frac{3\lambda(1-c)}{S}\left[\frac{1}{S+3\lambda} + \frac{3\lambda c}{(S+3\lambda)^2} + \cdots + \frac{(3\lambda c)^7}{(S+3\lambda)^8}\right] \\ &\approx \frac{3\lambda(1-c)}{S(S+3\lambda)}\ , \end{aligned}$$

so that

$$P_{cov}(SF) \approx \frac{2\lambda}{\delta}\left[1-e^{-3\lambda t}\right]\ .$$

Likewise, the P(SF) due to exhaustion of components is

$$\mathrm{Lp}\left[P_{exh}(SF)\right] = \frac{2\lambda}{S+2\lambda}\left(\frac{3\lambda c}{S+3\lambda}\right)^8\ .$$

By partial fraction expansion for repeated roots and Lp^{-1} ,

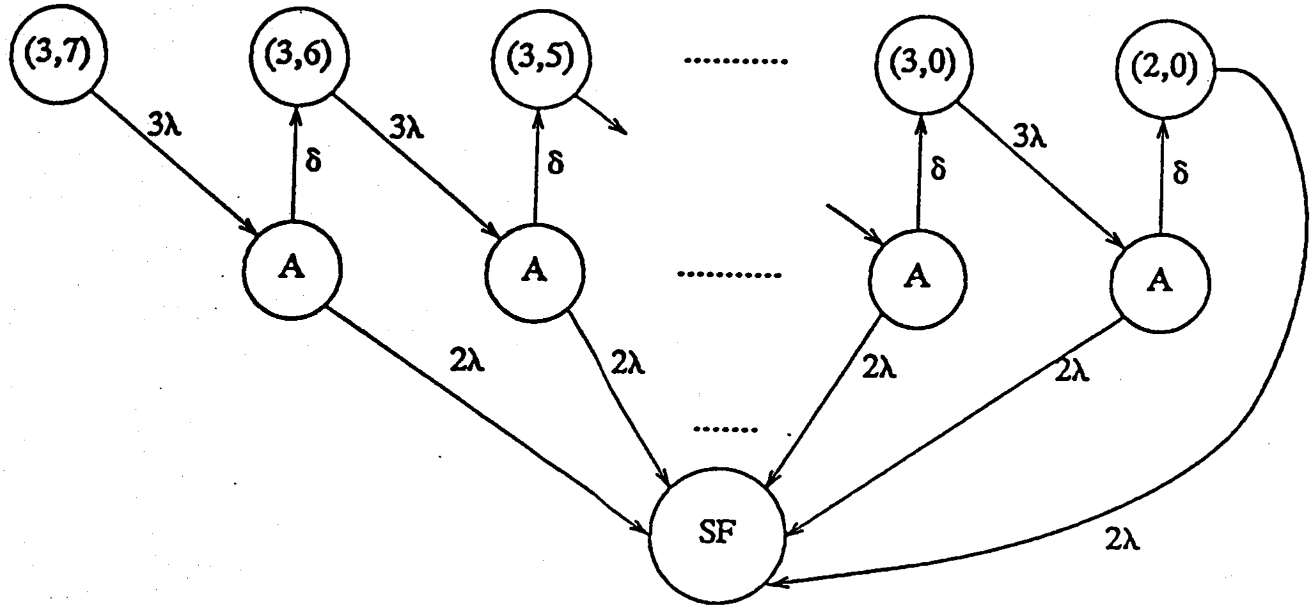
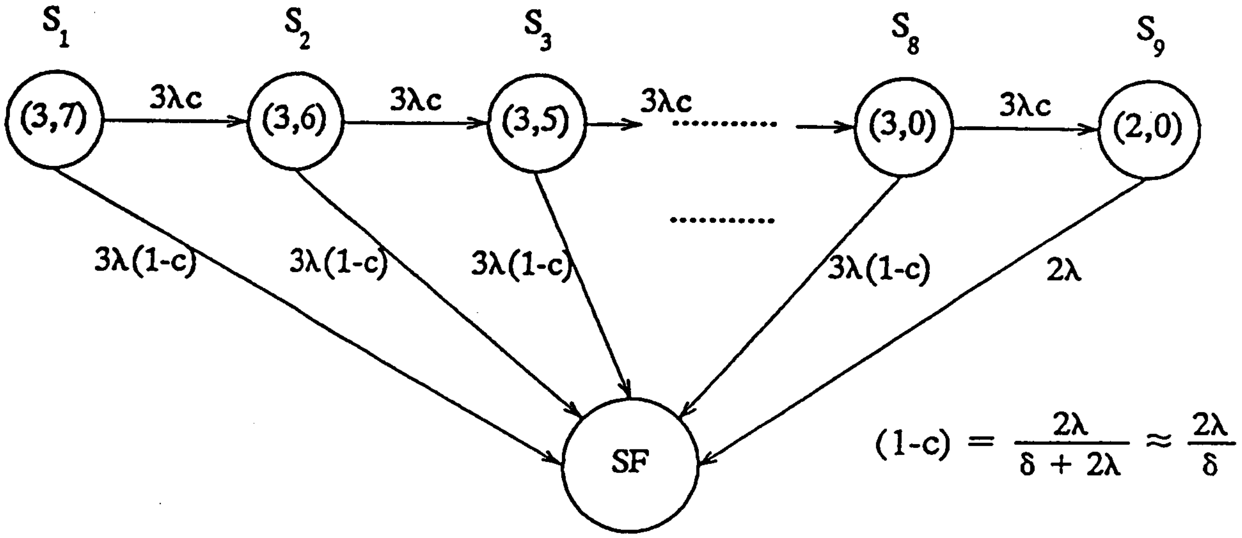


Figure 4.8. Markov Model for Test Case 6



$$(1\text{-}c) = \frac{2\lambda}{\delta + 2\lambda} \approx \frac{2\lambda}{\delta}$$

Figure 4.9. Instantaneous Coverage Markov Model for Test Case 6

$$P_{exh}(SF) = 1-3^8e^{-2\lambda t} + e^{-3\lambda t}\left[6560 + 2186(3\lambda)t + 728(3\lambda)^2\frac{t^2}{2} + 242(3\lambda)^3\frac{t^3}{6} + 80(3\lambda)^4\frac{t^4}{24} + 26(3\lambda)^5\frac{t^5}{120} + 8(3\lambda)^6\frac{t^6}{720} + 2(3\lambda)^7\frac{t^7}{5040}\right] .$$

The repeated roots in the solution for exhaustion of components are a result of the unpowered spare assumptions. In the expression for $P_{exh}(SF)$ derived by expanding these roots, all terms up to the ninth power cancel. This cancellation causes computational problems in the first one thousand hours. In the Markov model for this case, the unpowered spare assumptions result in a transition-rate matrix with non-distinct eigenvalues. Since the ARIES solution method is based on an assumption of distinct eigenvalues, this case also causes computational problems for ARIES.

In an ARIES Type 1 system, spares are assumed to be unpowered if the spare failure rate, μ, is less than the active module failure rate, λ. Because of the distinct eigenvalue restriction, μ must be greater than zero and $\mu \geq \frac{\lambda}{10^6}$. For this test case, the modified version of ARIES can compute reliability with $\mu = \frac{\lambda}{10}$ while the unmodified version can compute reliability with $\mu = \frac{\lambda}{100}$ (but with computational errors for $t < 10000$ hours).

Since ARIES will not allow μ to be zero, it overestimates the unreliability as compared to the direct calculation. Also, making μ as small as ARIES would accept for this case (to minimize the overestimation) resulted in computational errors for $t < 10000$. The overestimation and the computational errors are illustrated in the graph of the results included in Figure 4.10.

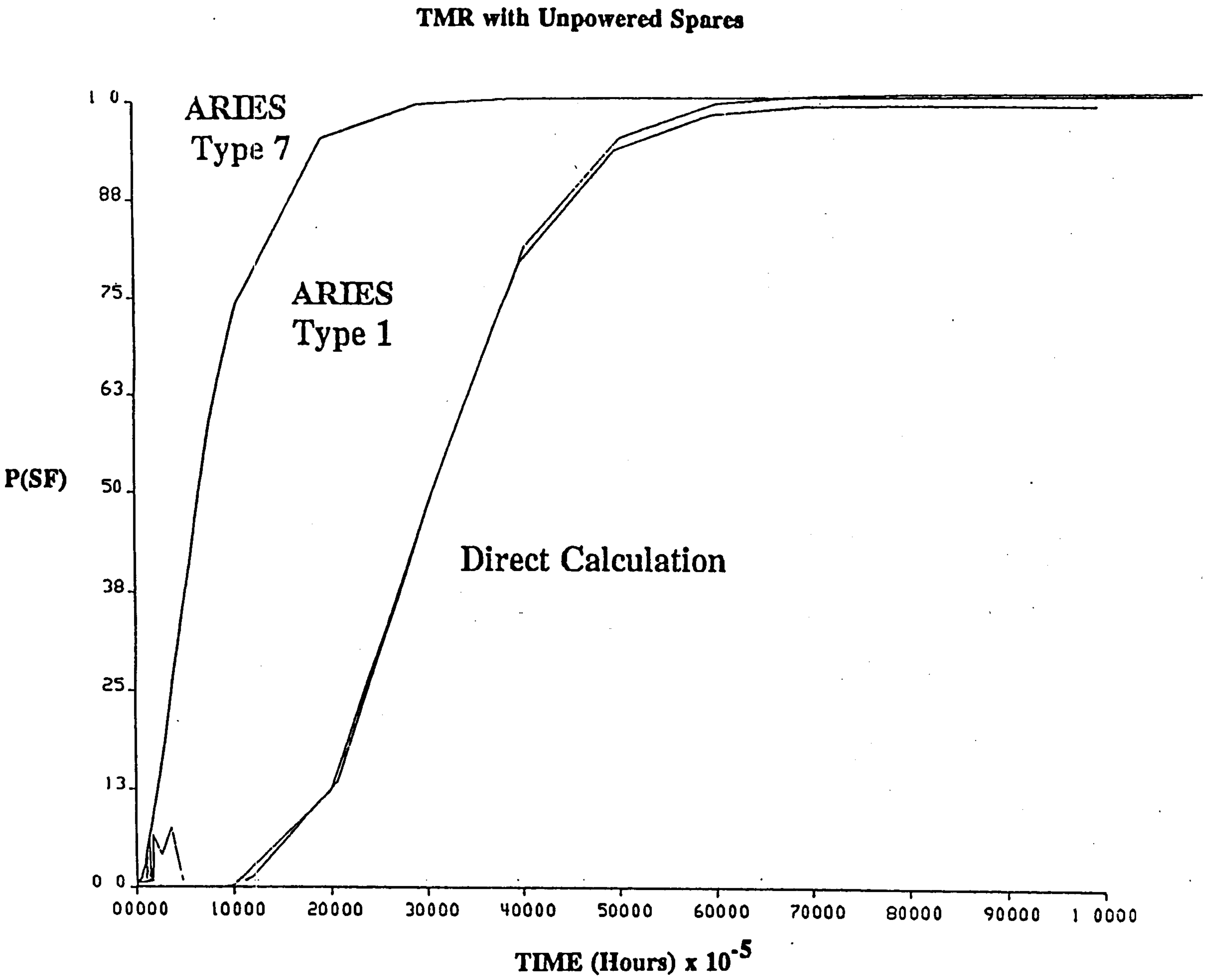


Figure 4.10. Test Case 6

In the Type 7 system, the transition-rate matrix is entered directly by the user and any non-distinct eigenvalues are dropped from the computation. Thus, in this case with eigenvalues of -3λ (occurring 8 times) and -2λ, the duplicates are dropped so that the system is solved with only two eigenvalues, -3λ and -2λ. As a result, the solution for this system is the same as that for a TMR with no spares, and the estimates of unreliability cannot agree with those from the Type 1 and the direct calculation. The graph of the Type 7 estimates is included in Figure 4.10 for comparison with the other graphs.

Since CARE III assumes that spares are powered, it was not possible to use CARE III for this case.

4.8 AIPS-Like FCS

For the seventh system, a very simple AIPS-like FCS was chosen to highlight the assumptions required to use ARIES and CARE III to estimate the reliability of an AIPS-like architecture. The system shown in Figure 4.11 was assumed to consist of eight sets of quad sensors, eight sets of quad activators, and two triplex processors. Failure rates of 10^{-4} per hour per sensor, 10^{-4} per hour per actuator, and 10^{-3} per hour per processor; perfect coverage for the sensors and actuators, imperfect coverage for the processors; permanent faults; and a mission time of 10 hours were assumed. The single fault model parameters are the same as for Test Case 4. The system was assumed to operate as follows:

- After loss of the triplex processor set (three faults), its functions are performed by the second triplex set, provided that it is still functional.

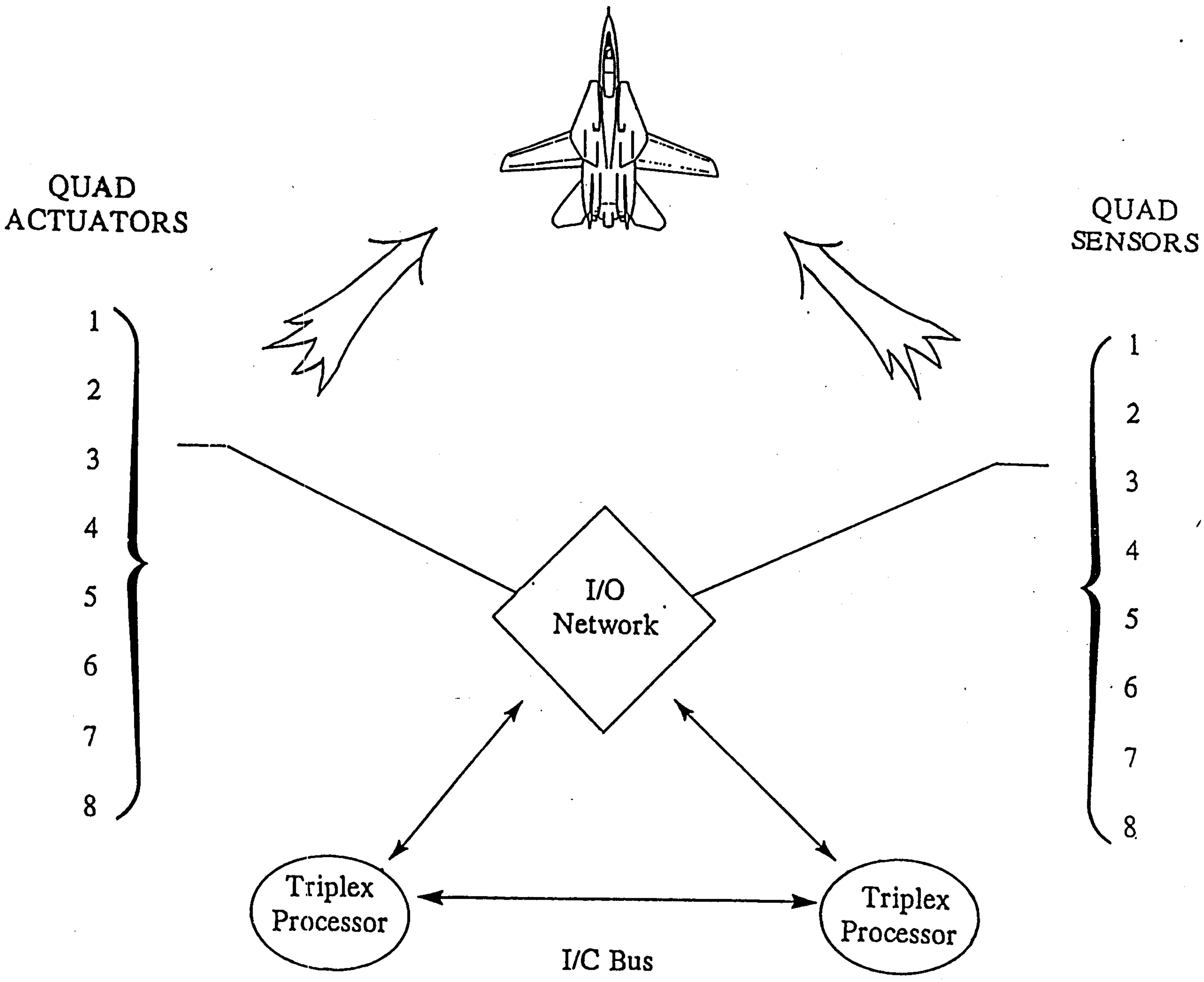


Figure 4.11. Fault Tolerant Flight Control System

- The second triplex set was formerly performing non-critical functions and was not vulnerable to critical fault pairs.

System failure occurs if and only if

- a sensor set is lost,
- an actuator set is lost, or
- the processing function is lost; i.e., two of the first triplex set are lost or two of the second triplex set are lost.

In this system, the two triplex sets simulate FTMP and the reversion to the second triplex set simulates functional migration. It was assumed that functional migration is always successful. Point-to-point wiring, i.e., a 100% reliable network, was assumed. Since triplex subsystems are considered triple, near-coincident faults are not a factor in system failure. Also, sequence-dependent faults are not a factor in system failure because of the reliability of the bus network.

The solution was obtained by decomposing the system into independent subsystems so that

$$P(SF) \approx P(E_S) + P(E_A) + P(E_{P_1}E_{P_2}) \ ,$$

where

E_S = Event of loss of a sensor set (1 of 8),
E_A = Event of loss of an actuator set (1 of 8),
E_{P_1} = Event of loss of primary processor set (1 of 1),and
E_{P_2} = Event of loss of backup processor set (1 of 1) .

Since a sensor set is lost when three out of four sensors in the set are lost, and there are eight sets,

$$P(E_S) = 32\lambda_S^3 t^3 \ .$$

Likewise,

$$P(E_A) = 32\lambda_A^3 t^3 \ .$$

Since the processor sets are triplex, loss of two results in loss of the set. It is immaterial whether two faults are nearly coincident in this scenario. Thus, the single fault model is unnecessary and

$$\begin{aligned} P(E_{P_1}E_{P_2}) &= P(E_{P_1})P(E_{P_2}) \\ &= (3\lambda_P^2 t^{2)}(3\lambda_P^2 t^{2)} \\ &= 9\lambda_P^4 t^4 \ . \end{aligned}$$

Thus,

$$P(SF) \approx 32\lambda_S^3 t^3 + 32\lambda_A^3 t^3 + 9\lambda_P^4 t^4 \ ,$$

so that at 10 hours P(SF) = 1.54E-7.

For the CARE III analysis, the system was described as an 18-stage system represented by the system fault tree in Figure 4.12. With this description, CARE III computed the P(SF) at 10 hours to be 1.5090886052E-07.

For the ARIES analysis, this system had to be defined as a series configuration of homogeneous subsystems. It was therefore necessary to combine the two processor subsystems into one subsystem to accommodate their particular configuration; the Markov model in Figure 4.13 describes the combined subsystem. Note that the Markov model for the combined subsystem contains more states than the two separate subsystem models would. A transition rate matrix for a type 7 system was constructed from this

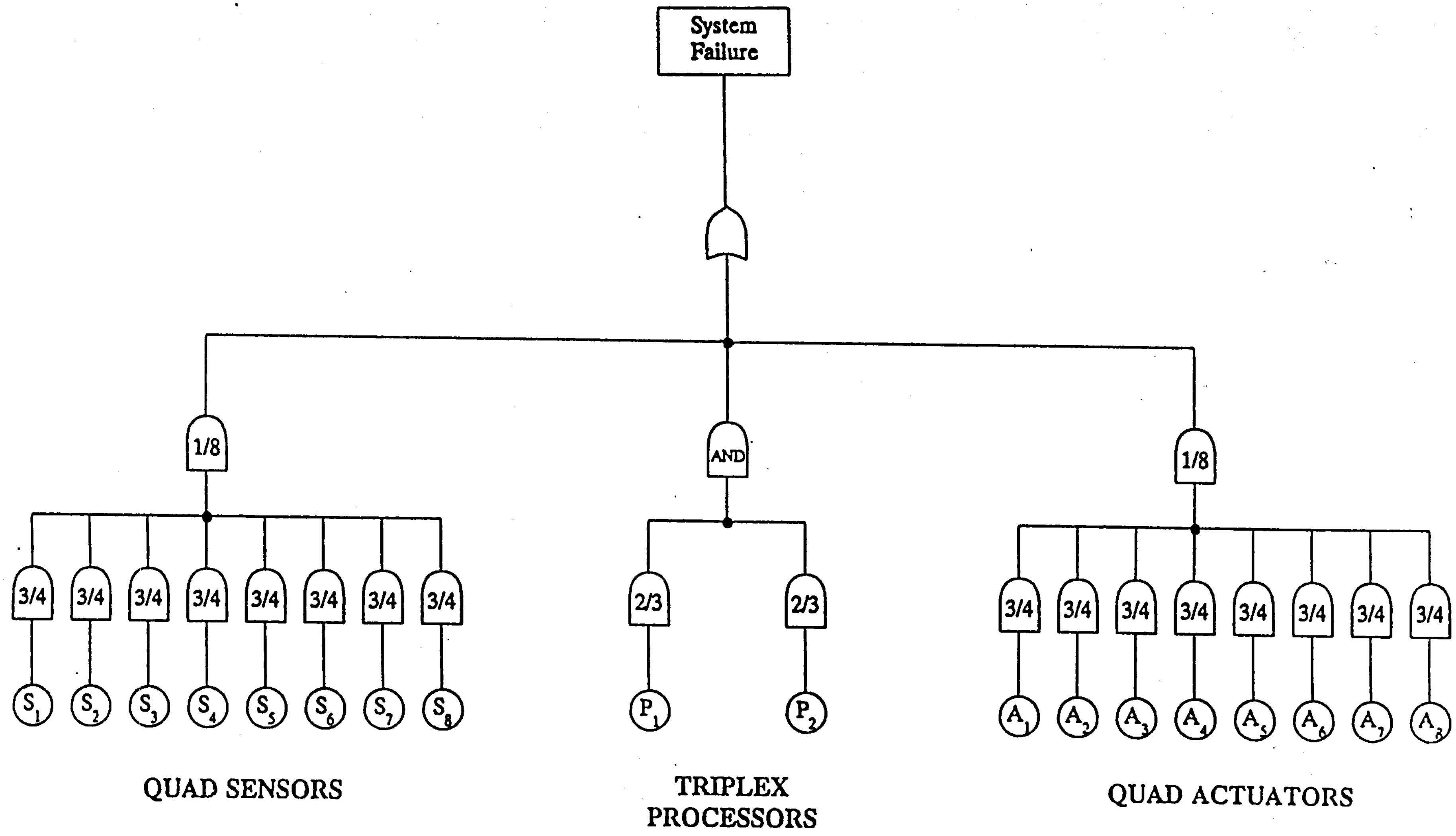
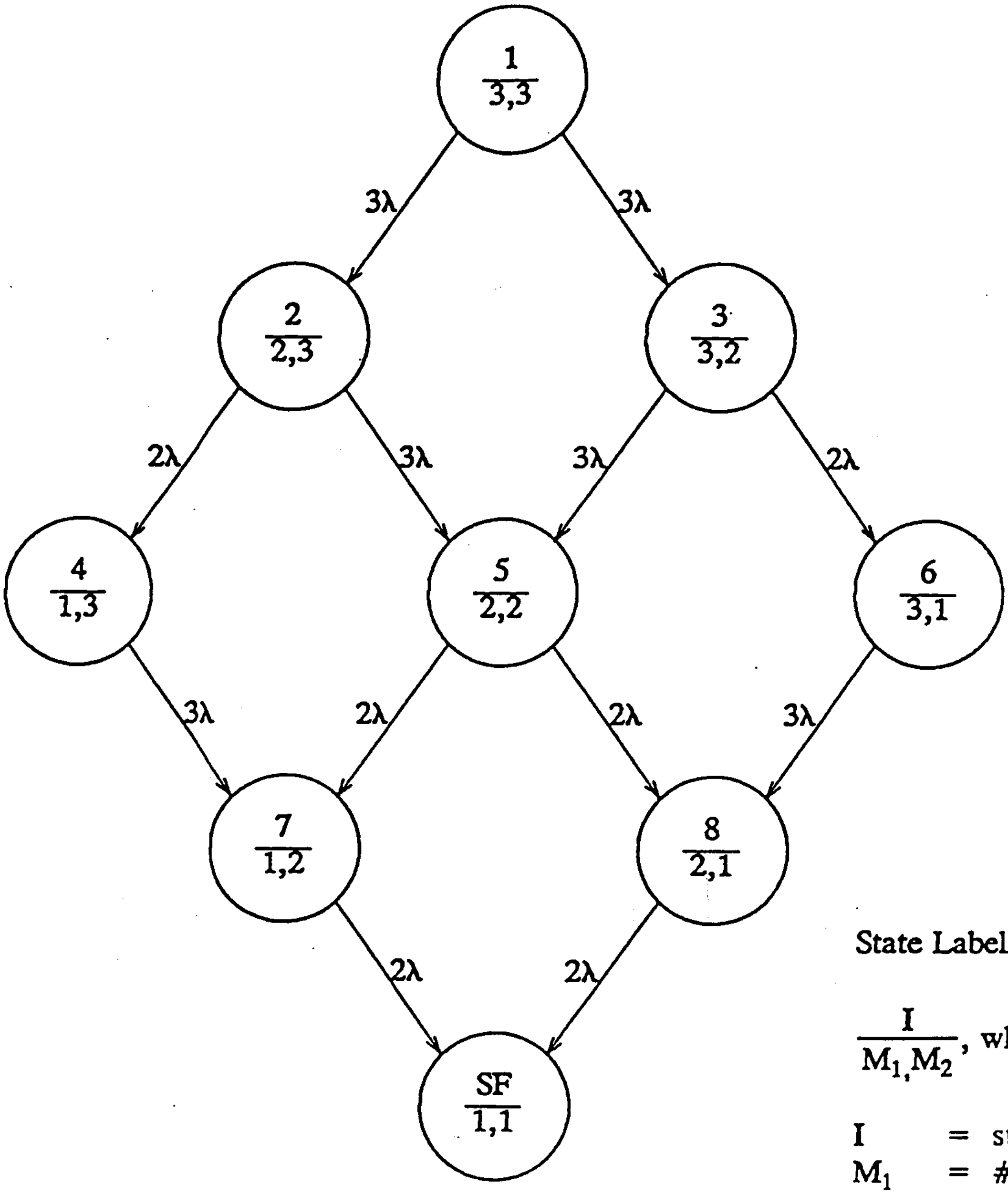


Figure 4.12. System Fault Tree for Test Case 7



State Labelling:

$\frac{I}{M_1,M_2}$, where

I = state index
M_1 = # of good units on first triplex
M_2 = # of good units of second triplex

Figure 4.13. Markov Model for Processors of Test Case 7

Markov model. The complete system was then solved by ARIES as a series configuration of 16 type 1 (sensors and actuators) and one type 7 subsystems, resulting in a P(SF) of 1.5090900654E-7 at 10 hours.

A graph of the results is included in Figure 4.14.

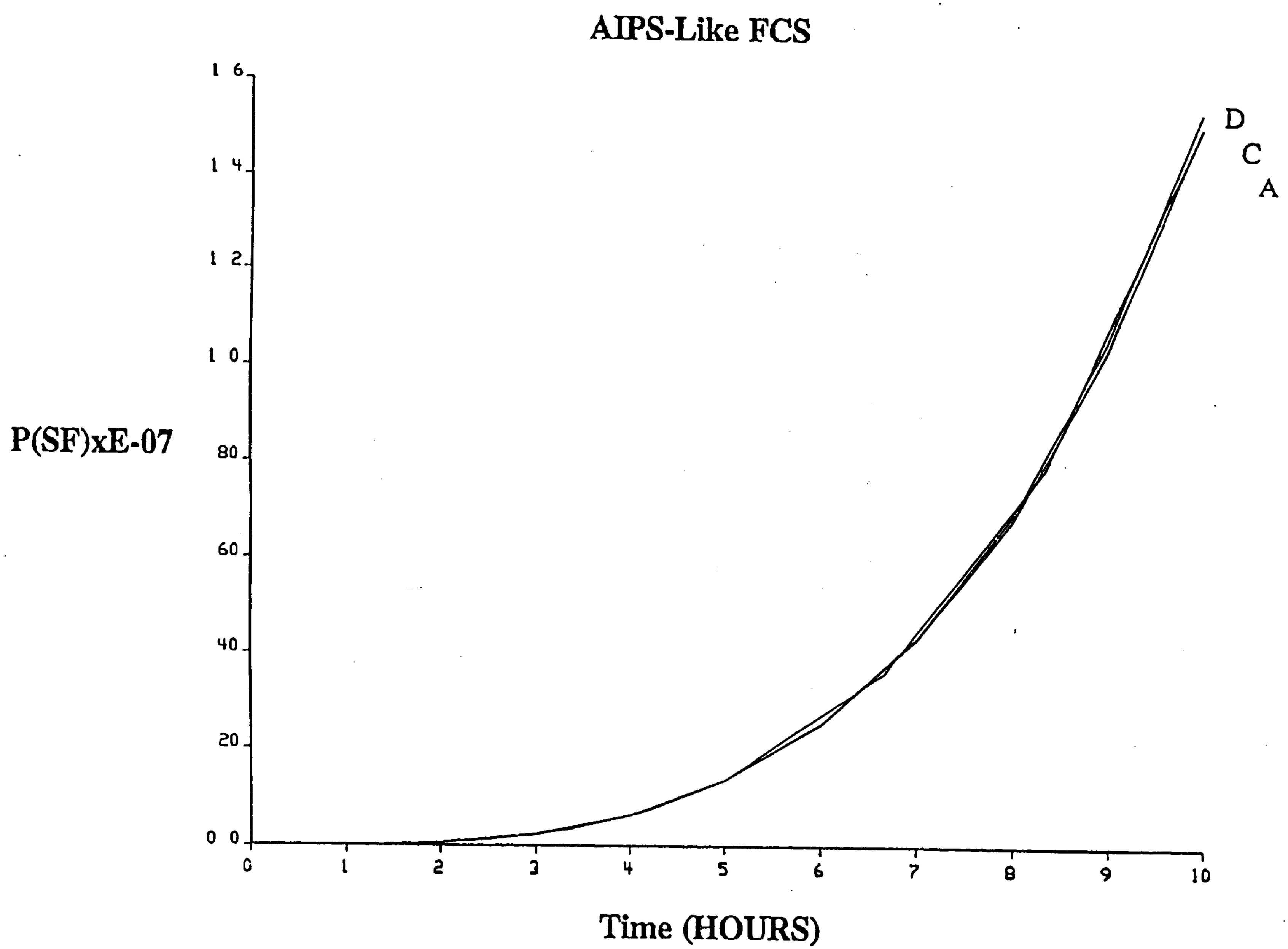


Figure 4.14. Test Case 7

5.0 Assessments and Conclusions

5.1 Objective and Leading Particulars

The objective of this section is to assess the potential benefits and limitations of CARE III and ARIES 82 when used for advanced fault tolerant systems applications. These benefits and limitations reported here were identified following a review of the AIPS requirements, a study of the models upon which the tools were based, and application of these tools to the test cases described in Section 4.0, as well as to other simple systems.

It is expected that the results of this investigation will provide guidance for planning future reliability modeling research and development activities at NASA-LaRC. To this end, it is important to recognize and understand both the potential benefits and limitations of these tools. Understanding of these issues will help prevent misapplication of the tools. Limitations with respect to application of these tools to advanced systems could be eliminated by improvements or by the development of new tools.

The observations and comments regarding these tools fall into three categories. The most important category includes issues which have a clear and direct impact on the capability to effectively represent advanced fault tolerant system configurations. Another category includes issues which are likely to impact application of these tools to advanced fault tolerant systems. Most items discussed will fall into these categories. Finally, the utility of automated tools often is limited by the demands placed upon the user. Consequently, a category for user-related issues is included.

It should be noted that limitations have been identified for use of these tools to model advanced architectures, in a wide range of aerospace applications. In order to not seem unduly negative, these results must be viewed within the context of the applications for which these tools were originally developed. Further, the significance of a particular limitation must be judged by the importance and scope of the advanced architectural feature that creates the limitation.

5.2 CARE III Assessment

CARE III is the most recent in a series of reliability assessment tools developed by NASA LaRC. It was designed primarily for analyzing ultrareliable flight control systems. It is described as a general purpose reliability analysis and design tool for fault tolerant systems and it is capable of handling large highly reliable systems. A fault handling model is used to model detection, isolation, and recovery processes. CARE III provides a variety of stationary and nonstationary fault and error models. These include permanent, transient, intermittent, design, latent, and software faults or errors. CARE III features a user-oriented fault tree language for describing complex system configurations and success criteria.[11] [12]

A number of CARE III's characteristics would be useful for analysis of advanced systems. The most important is the capability to analyze large systems. In the fault occurrence model, CARE III can handle up to 70 stages as well as 2000 total events and 70 input events. Input events are the lowest level input to gates in the fault tree and other events are inputs or outputs at higher levels in the fault tree. A stage may comprise one or more modules. Each stage with replicated modules is treated as an M out of N subsystem. When coupled with the options for multiple fault handling models, very large and complex systems can be modeled. CARE III accomplishes a large state reduction by decomposition and aggregation techniques. The fault occurrence and fault handling parts of the model are decomposed under the assumption that there are several orders of magnitude difference between the fault occurrence and the fault recovery rates. This is referred to as a temporal decomposition. Further decomposition and aggregation occurs when states across stages are aggregated based on the fault tree and the critical pair tree. This is somewhat similar to some of the structural decomposition and aggregation techniques used in other reliability tools.[3] [13]

The flexible fault handling/coverage/double fault features of CARE III distinguish it from other reliability analysis tools. For applications where mission duration is short relative to the time between failure occurrences, system failure due to failures in fault handling or critically coupled double faults during recovery may be significant relative to failure by exhaustion of components. In such applications, the capability to model the fault handling and recovery processes should be important.

CARE III's capability to model nonconstant failure rates (Weibull distribution) also distinguishes it from some other reliability modeling tools. This feature is useful for systems that contain components subject to wear out, such as mechanical actuators and some electronic components, and possibly for electronic systems subject to radiation exposure. For applications where nonconstant failure rates and failures due to component exhaustion are significant, CARE III's features could prove useful.

CARE III has undergone extensive testing and verification. The numerical accuracy for extremely reliable and ultra-reliable reliable systems should be adequate.

In summary, the CARE III features that have potential value for reliability analysis of advanced fault tolerant aerospace systems are the capability to handle large systems, the somewhat flexible fault handling model, the capability to have nonconstant fault occurrence rates and the capability to model near coincident failures by the critically coupled pair or double fault model.

A number of CARE III's limitations with respect to AIPS applications stem from space missions of long duration. As noted earlier, Care III was specifically designed to evaluate reliability for air transport flight control systems. Mission durations are considerably shorter in these applications. Emphasis will shift from fault handling failures to exhaustion of components failures. The product of mission duration and failure rate changes by several orders of magnitude. As a result, approximations used in the CARE III computations could no longer be valid. Also, the longer mission intervals and the need to conserve power or weight in space applications can dictate the need to use unpowered spare modules. Presumably, these modules, while unpowered, would have lower failure rates than their powered counterparts.

In Section 4.6 it was indicated that CARE III requires that spare modules have the same failure rate as active modules. Finally, some space applications will operate as open systems, i.e., maintenance will be permitted. CARE III only models closed (maintenance free) systems.

The need to model sequence dependent failures sometimes arises when fault tolerant systems are considered. One of the more important cases for AIPS stems from the function migration concept. The concept can allow a function to be carried out by an alternate processing site (system resource) when the processing site initially used for the function fails. The capability to migrate the function could depend upon a fault-free intercomputer network or a mass memory resource. If the failure of the initial processing site occurs prior to the loss of the mass memory, the function can be migrated successfully. If the mass memory failure precedes the loss of the initial processing site, the function will be lost. In the function migration cases, reliability analysis may focus on exhaustion of resources rather than coverage failures. CARE III can be used to bound the effects of sequence-dependent failures. However, the sequence dependence failure modes introduced by function migration could require better capability in this area.

In Section 2.0 the need to analyze the reliability of large nodal communication networks was identified. CARE III cannot model these networks. It should be noted that tools to analyze reliability for these networks have not been developed.

Several potential limitations of the CARE III fault handling model have been identified. These are

1. The fundamental assumption that sojourn times in the fault handling model are small relative to the time between fault occurrences may not be valid for latent faults or for some intermittent faults.
2. The fault handling models used are independent of system state. For some systems it may be realistic to expect coverage to deteriorate as system resources are reduced. CARE III can be used to bound the reliability of such systems.

3. The fault handling model is constrained to a single entry state, to have identical transition rates (α, β) between active and benign for faulted and error-producing states, and transitions between some states of the model are omitted. These are flexibility issues of more interest for research purposes.
4. The double fault model is conservative. A system failure results if two critically coupled faults occur even though neither has produced an error. This assumption could result in a too conservative prediction when faults of long latency periods are present, e.g., software-dependent hardware faults.

Multiple near coincident faults, multiple faults that occur within the fault handling interval following the occurrence of the first fault, of order higher than two cannot be modeled by CARE III. This case was demonstrated by the quintuplex example of Section 4.0. As indicated, the reliability for this simple system could be obtained indirectly from CARE III analysis of a TMR with two spares. The quintuplex configuration, an important fault tolerant configuration, is not presently used in AIPS, but that is not to say that critical triples will not arise in any AIPS applications nor should one expect the quintuplex to be absent from other advanced fault tolerant systems. Further, it should not be inferred that the indirect method using CARE III will work satisfactorily for more complex configurations or where other critical triples arise.

CARE III calculates reliability based on the assumption that the probability that there are no failed modules in the system equals 1 at $t=0$. Perfect dispatch reliability can be approached but not obtained for complex systems. For extremely reliable systems, very high dispatch reliability is required. Consequently, the capability to set the initial state occupancy probabilities to values other than "perfect dispatch" is highly desirable.

During this investigation, several individuals of differing backgrounds have learned to use CARE III. The earliest user learned at a time when CARE III was being validated and modified and at a time prior to the publication of the user's guides. During this period, results were sometimes suspect due to the status of CARE III modifications. Presently, users are confident of CARE III results. The new user's guides have speeded the learning process and represent a quantum improvement in the documentation.

5.3 ARIES 82 Assessment

ARIES 82 is an interactive, unified reliability modeling tool developed by Ng and Avizienis at UCLA. It models systems which are composed of a series of independent homogeneous subsystems each of which can be modeled as a finite-state, continuous parameter, time-homogeneous Markov process. Limited state aggregation is achieved by analyzing the independent subsystems and combining the results. Fault handling is assumed to be instantaneous and it's effects are captured by constant coverage probabilities which depend upon system state. As indicated in Section 3.0, ARIES 82 can be applied to a wide range of system scenarios.

The features of ARIES 82 which are of potential benefit to advanced fault tolerant system studies are

1. The capability to model closed or open systems.
2. Spare modules can have failure rates that are different than active module failure rates.
3. A state transition matrix can be used to describe a system.
4. An interactive user interface.

Some of the limitations of ARIES 82 are

1. Instantaneous coverage may not be adequate for modeling some systems. When fault handling times are small relative to the time between fault occurrences, this simple model is often adequate.
2. Constant failure rates are not adequate for modeling certain components of aerospace systems.
3. System sizes are limited to relatively small systems.
4. The accuracy of the results are suspect for highly reliable systems. Accuracy limitations are noted several times in Section 4.0.
5. The eigenvalues of the state transition matrix must be distinct. Repeated eigenvalues can occur, for example, when spare failure rates are zero until they are activated.

The accuracy limitations are restrictive. ARIES 82, in contrast to CARE III, computes reliability instead of unreliability. For very reliable systems, this approach stresses the numerical accuracy of the host computer and is the source of some of the accuracy problems. Also, ARIES 82 normally reports only 7-digit results. The sensitivity of the results to the order in which system states are indexed was noted in Section 4.0. Also, nearly distinct eigenvalues can lead to accuracy problems.

ARIES 82 has been in use as a tool to support university teaching and research. But ARIES 82 has not undergone a rigorous validation process. Even for the relatively few and simple cases run for this study, at least two programming errors that produced erroneous results were found.

Learning to use ARIES 82 was judged to be somewhat simpler than CARE III. This was due, in part, to the relative simplicity of the ARIES 82 model.

5.4 Conclusions

A number of useful features were recognized in ARIES 82. Accuracy limitations, lack of formal validation, the presence of programming errors, the lack of product support, and the limitations on system size combine to make ARIES 82 unsuitable for modeling advanced fault-tolerant systems.

CARE III was found to have features desirable for modeling advanced system architectures. Among these were the capability of handling large systems, a somewhat flexible fault handling model, nonconstant failure rates in the fault occurrence model, the provision for near coincident double faults, the computational accuracy required for analyzing ultrareliable systems, and a user interface which provides for simple and flexible system definition.

A number of CARE III limitations were identified. Among the more important system scenarios which were difficult to model or could not be modeled using CARE III were

1. Systems with unpowered spares,
2. Systems where equipment maintenance must be considered,
3. Systems where failure depends on the sequence in which faults occurred,
4. Systems where multiple faults greater than a double near coincident fault must be considered,
5. Systems containing large nodal communications networks that have a significant impact on system reliability, and
6. Systems where less than perfect dispatch reliability must be considered.

Subject to constraints cited in paragraph 5.2 and repeated below, CARE III is best suited for evaluating the reliability of advanced fault tolerant systems for air transport. Characteristics of systems for which CARE III is best suited are

1. The mission time is short relative to the time between failure occurrences. That is, coverage failures dominate exhaustion of component failures.
2. The fault recovery time is short relative to the time between failure occurrences.
3. Either the network reliability cannot impact system reliability or the network can be treated as an independent subsystem whose reliability can be determined by other means.
4. Near coincident multiple faults of order greater than two are not relevant.
5. System reliability should be in the extremely to ultrareliable regime.

6.0. References

References

1. J. Lala, "Advanced Information Processing System," *AIAA/IEEE 6th Digital Avionics Conference Proceedings*, (December 3, 1984).

2. Eliezer Gai, "Advanced Information Processing System (AIPS) Methodology Report," The Charles Stark Draper Laboratory, Inc., Cambridge, MA (July 1984).

3. Kishor Trivedi, *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*, Prentice Hall, Englewood Cliffs, NJ (1982).

4. Robert Geist and Kishor Trivedi, "Ultrahigh Reliability Prediction for Fault-Tolerant Computer Systems," *IEEE: Transactions on Computers* C-32(12)(December 1983).

5. Ying W. Ng and A. Avizienis, "A Unified Reliability Model for Fault-Tolerant Computers," *IEEE: Transactions on Computers* C-29(11)(November, 1980).

6. S. Makam, A. Avizienis, and G. Grusas, *ARIES 82 Users' Guide*, University of California at Los Angeles, Los Angeles (August 1982).

7. Kishor Trivedi and Robert Geist, "A Tutorial on the CARE III Approach to Reliability Modeling," *NASA Contractor Report* 3488(December 1981).

8. L.A. Bryant and J.J. Stiffler, *CARE III Phase II Report User's Manual*, NASA LaRC CR-165864 (September 1982).

9. J.J. Stiffler and L.A. Bryant, *CARE III Phase II Report Mathematical Description*, NASA CR-3566 (November 1982).

10. D.M. Rose, R.E. Altschul, J.W. Manke, and D.L. Nelson, "Review and Verification of CARE III Mathematical Model and Code: Interim Report," *NASA Contractor Report* **166096**(April 1983).

11. S.J. Bavuso and P.L. Petersen, *CARE III Model Overview and User's Guide (first revision),* NASA TM-86404 (April 1985).

12. S.J. Bavuso, "Advanced Reliability Modeling of Fault-Tolerant Computer-Based Systems," *NATO Advanced Study Institute Presentation*, (1982).

13. J.L. Lala, "Interactive Reductions in the Number of States in Markov Reliability Analysis," The Charles Stark Draper Laboratory, Inc., Cambridge, MA (1983).

APPENDIX

FINAL REPORT
NASA CONTRACT # NAS1-16489
TASK 16

COMPARATIVE ANALYSIS OF CARE III AND ARIES 82 FOR RELIABILITY ANALYSIS OF AIPS ARCHITECTURE

March 15, 1985

Robert Baker
Charlotte Scheper

Research Triangle Institute
Research Triangle Park, NC 27709

SCOPE OF WORK

- Learn AIPS and Determine Suitability of CARE III and ARIES for AIPS Analysis
- Compare CARE III and ARIES
- Apply CARE III and ARIES to "AIPS Like" Architectures
- Identify Limitations and Recommend Refinements
- Document

AIPS OBJECTIVES

Design a fault and damage tolerant system architecture which satisfies real-time data processing requirements for aerospace applications

Develop support methods for design, evaluation, and verification

AIPS APPLICATION REQUIREMENTS

	Mission	Failure Probability	Thruput	Memory	Mass Memory	I/O Rates
COMMERCIAL AIRCRAFT	10 hrs	10^{-9}	5.5 MIPS	2 MB	15 MB	750 Kb/s
TACTICAL MILITARY AIRCRAFT	4 hrs	10^{-7}	6 MIPS	1 MB	100 MB	1 Mb/s
UNMANNED SPACE PLATFORM	5 yrs	10^{-2}	2 MIPS	750 KB	750 KB	150 Kb/s
UNMANNED SPACE VEHICLE	1 wk	10^{-6}	.5 MIPS	300 KB	300 KB	1.5 Mb/s
DEEP SPACE PROBE	5 yrs	10^{-2}	.5 MIPS	300 KB	1 MB	
MANNED SPACE PLATFORM	20 yrs	10^{-2}	15 MIPS	20 MB	400 MB	15 M/bs
MANNED SPACE VEHICLE	10 days	10^{-7}	1.5 MIPS	3 MB	3 MB	1 Mb/s
RATIO MAX/MIN	40K	10^{7}	30	60	1000	100

AIPS SYSTEM ATTRIBUTES (QUALITATIVE REQUIREMENTS)

- Growth and Change Tolerance
- Accepts Technology Upgrades
- Graceful Degradation
- System Complexity Transparent to User
- Graded Redundancy
- Damage Tolerance

AIPS BUILDING BLOCKS

FTMP

FTP

Intercomputer Network (Fault and Damage Tolerant)

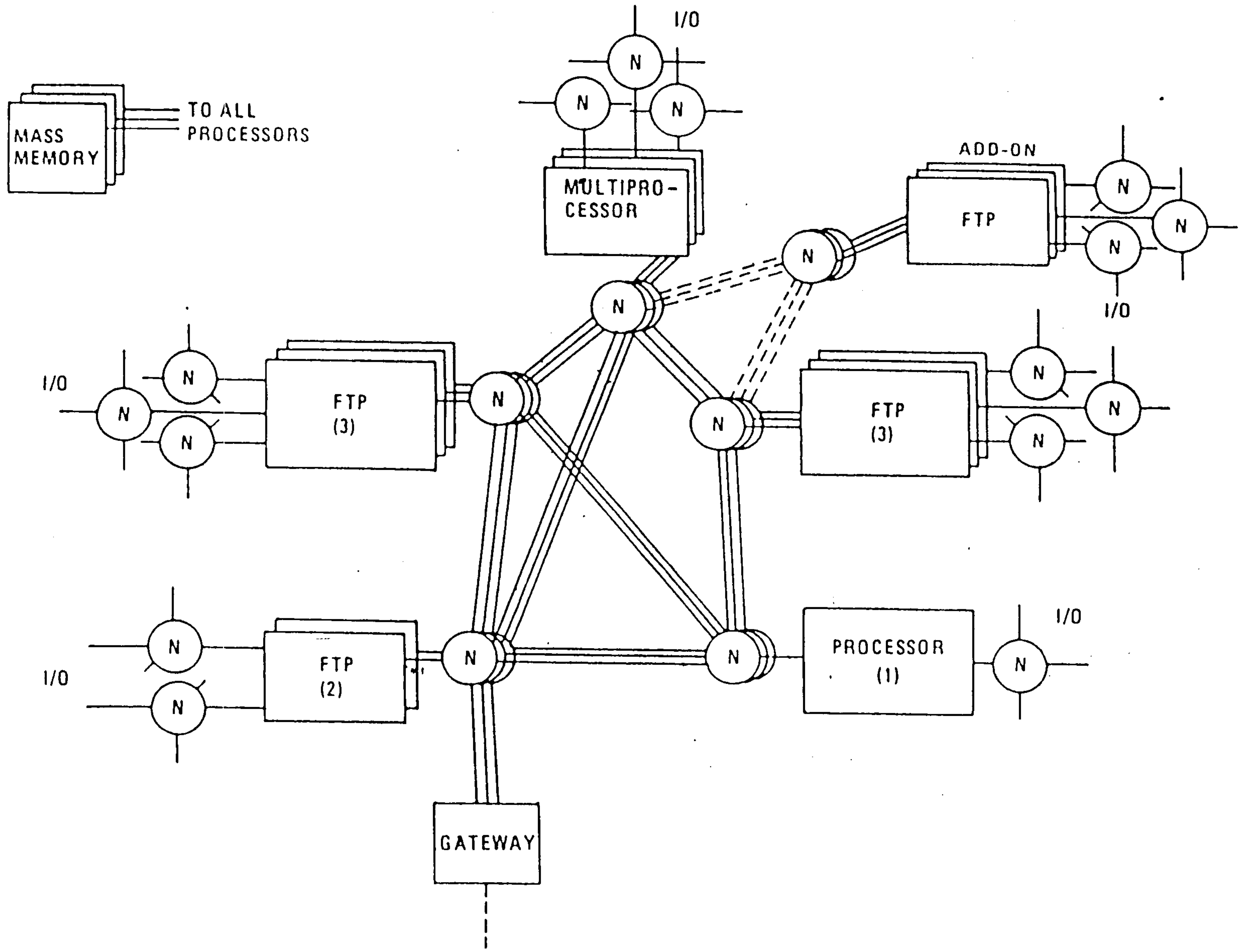
I/O Network (Fault and Damage Tolerant)

Fault Tolerant Mass Memory

Fault Tolerant Power Distribution System

Network Operating System

AIPS
Proof-of-Concept System



SOME KEY FAULT TOLERANT FEATURES OF AIPS ARCHITECTURE

- FTMP and FTP Concepts
- Hardware Redundancy
- Redundant Elements in Tight Synchronism
- Fault Detection and Making Implemented in Hardware
- Fault Isolation and Reconfiguration in Software
- Layered Communications Network
- Source Congruency
- Function Migration

SOME AIPS ARCHITECTURAL FEATURES, CONCEPTS, AND APPLICATION REQUIREMENTS IMPACTING RELIABILITY ASSESSMENT

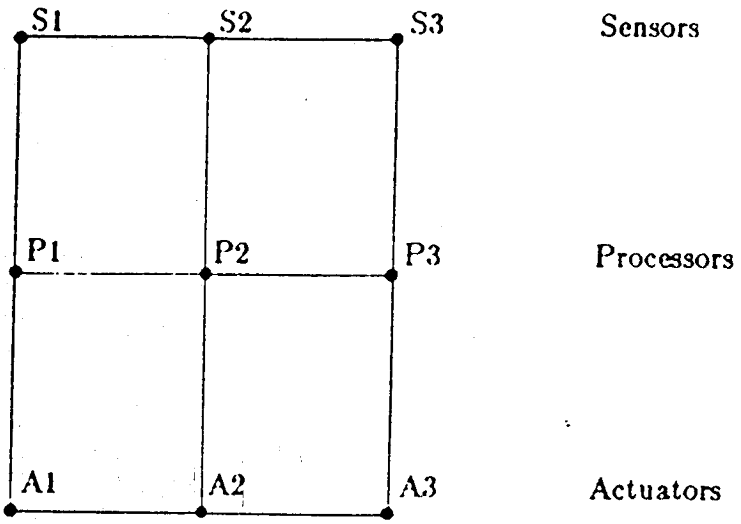
- Function Migration
- Partial Cross-Strapping
- Large Networks
- High Degree of Fault Tolerance
- Both Long and Short Mission Times

Simple Network

12 Links
9 Nodes

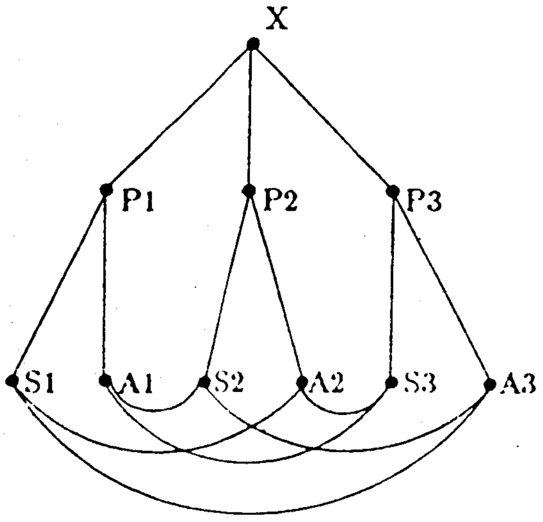
3 Failures for L.O.S.

2 Failures Loss Nodes



Alternate Network

15 Links
10 Nodes



3 Failures to Isolate Nodes

$$\underbrace{\text{6 Failures for Loss of System}}$$

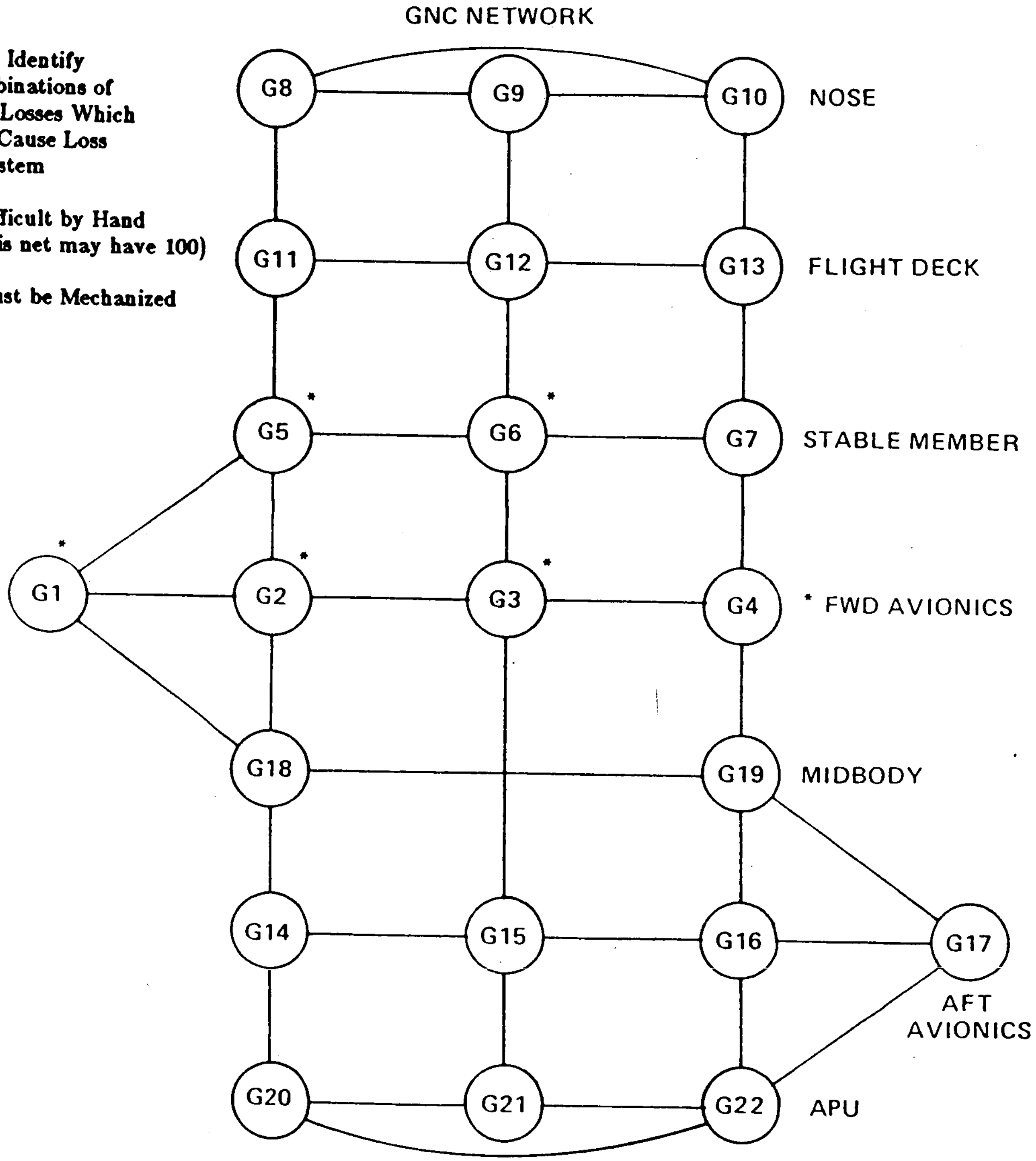
⇩

Network Reliability Does Not
Impact System Reliability

A Draper Proposed AIPS Network

Problem: To Identify Combinations of Link Losses Which Will Cause Loss of System

- **Difficult by Hand (This net may have 100)**
- **Must be Mechanized**



* {G1, G2, G3 – ROOT NODES FOR ONE PROCESSING SITE
{G4, G5, G6 – ROOT NODES FOR OTHER PROCESSING SITE

CARE III FEATURES AND ATTRIBUTES

- Designed for Ultrareliable Flight Control System Analysis and Design
- Handles Large Systems
- Large Reduction of State Space Via Aggregation
- Fault Handling Model {Permanent, Intermittent, Transient}
- Exponential and Wiebull Failure Rates
- Double Fault Model
- Analyze Closed Systems
- Fault Tree Input

m = Maximum Number Of Faults A Stage Can Sustain
And Still Be Operational

x = Fault Detected, Faulty Processor Replaced

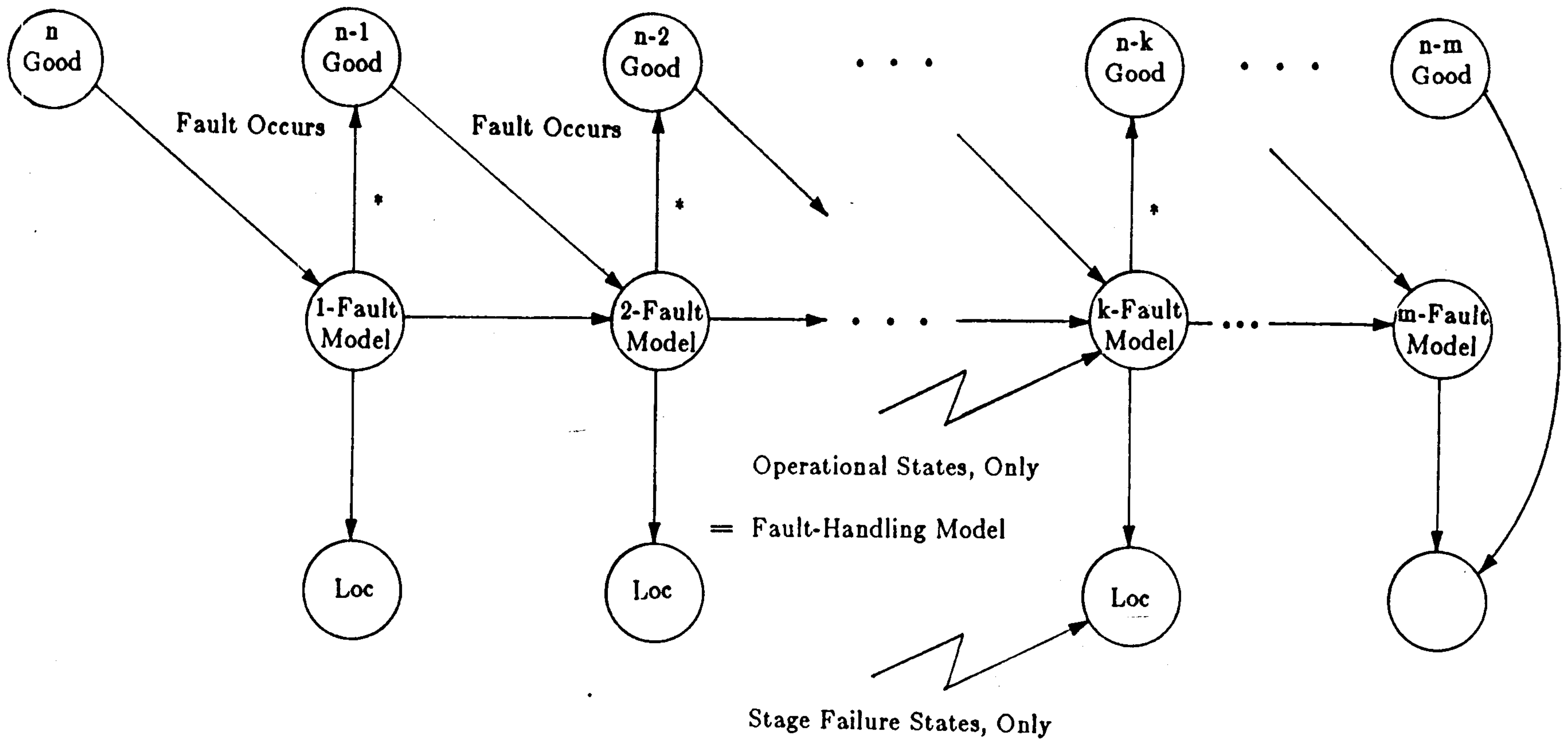
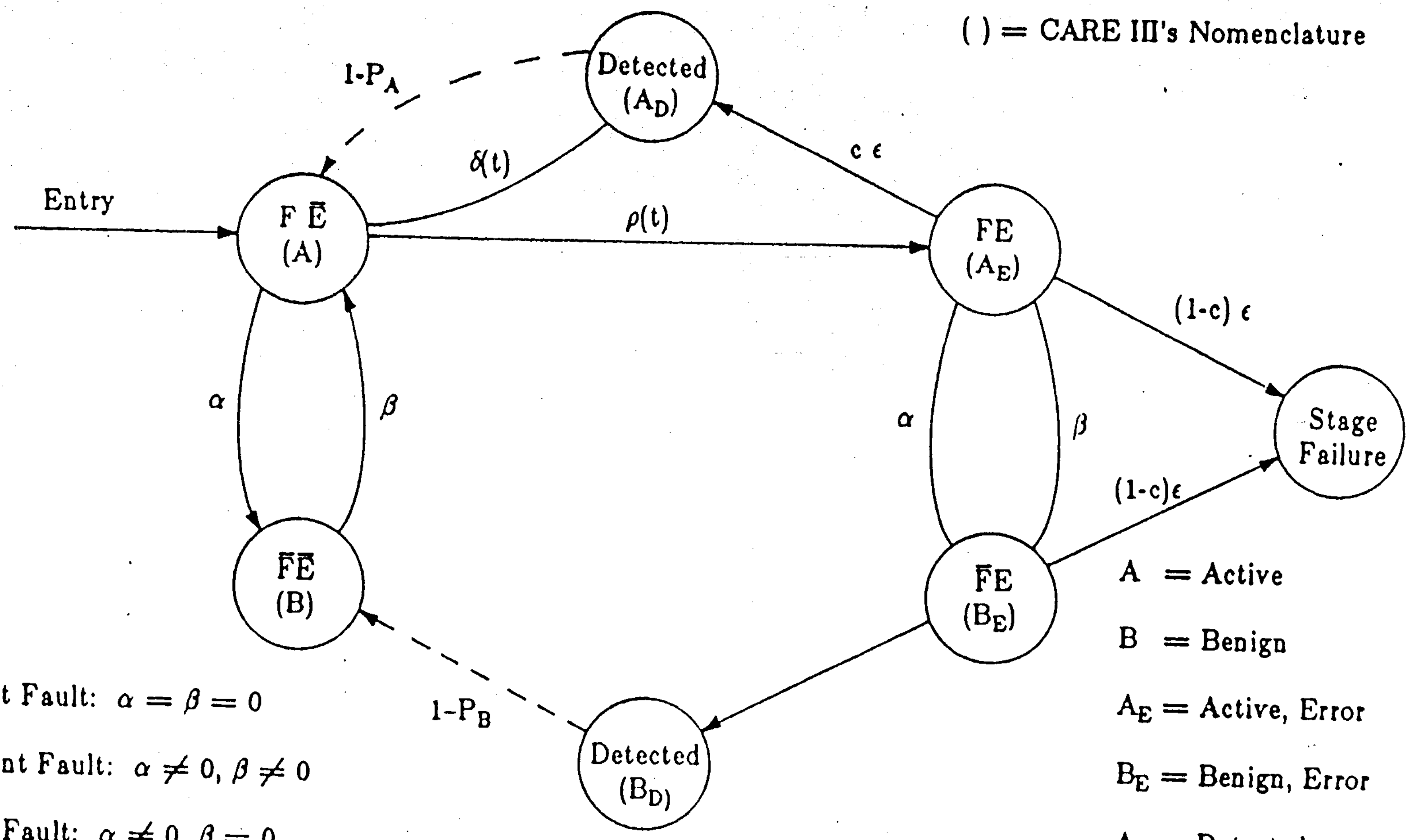


Figure 6-23

AN ALTERNATE STATE REPRESENTATION OF A STAGE

Fault Handling Model of CARE III



( ) = CARE III's Nomenclature

A = Active

B = Benign

A_E = Active, Error

B_E = Benign, Error

A_D = Detected

B_D = Detected

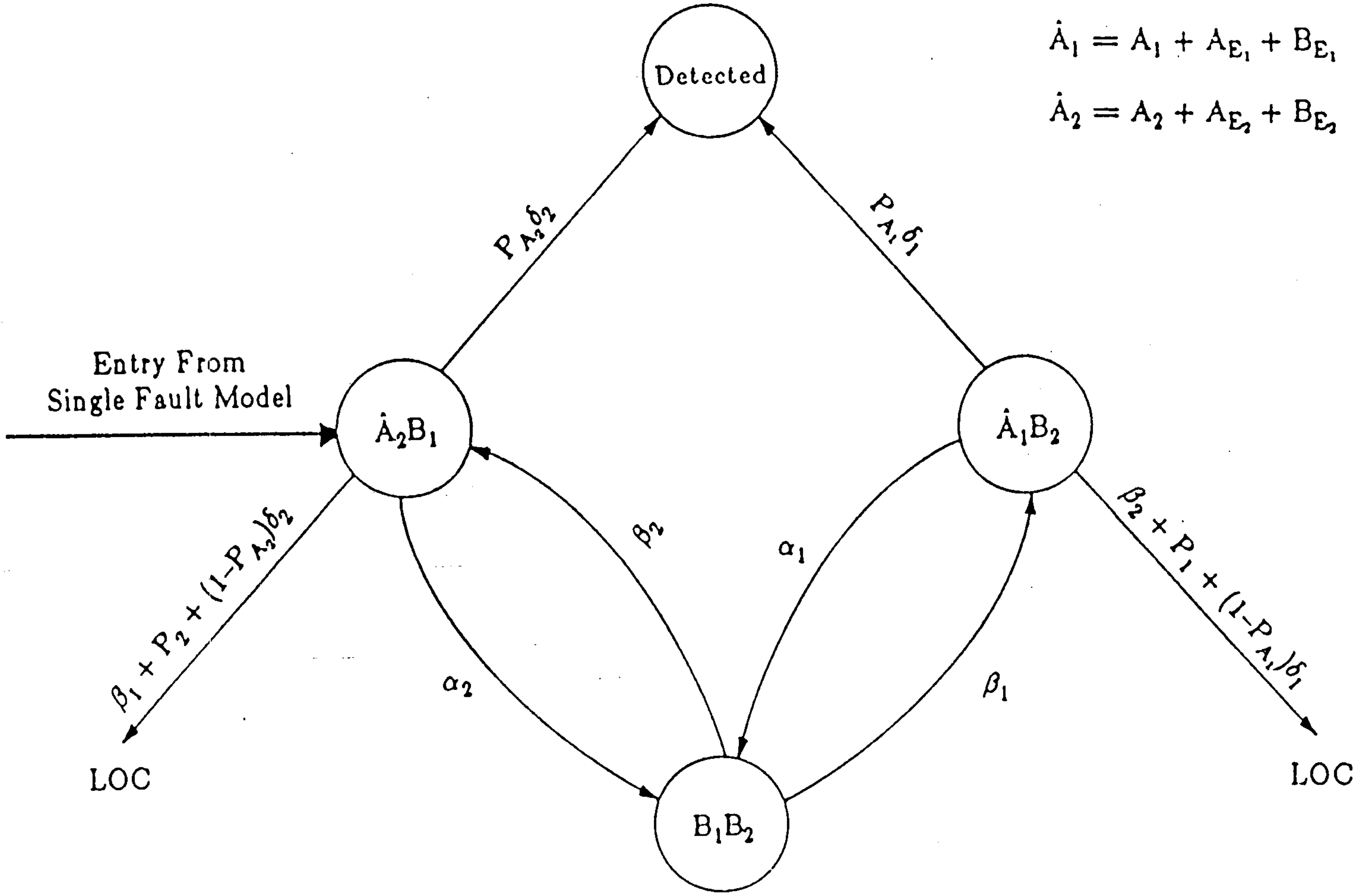
β = 0 Implies Transient Fault

Permanent Fault: $\alpha = \beta = 0$

Intermittent Fault: $\alpha \neq 0, \beta \neq 0$

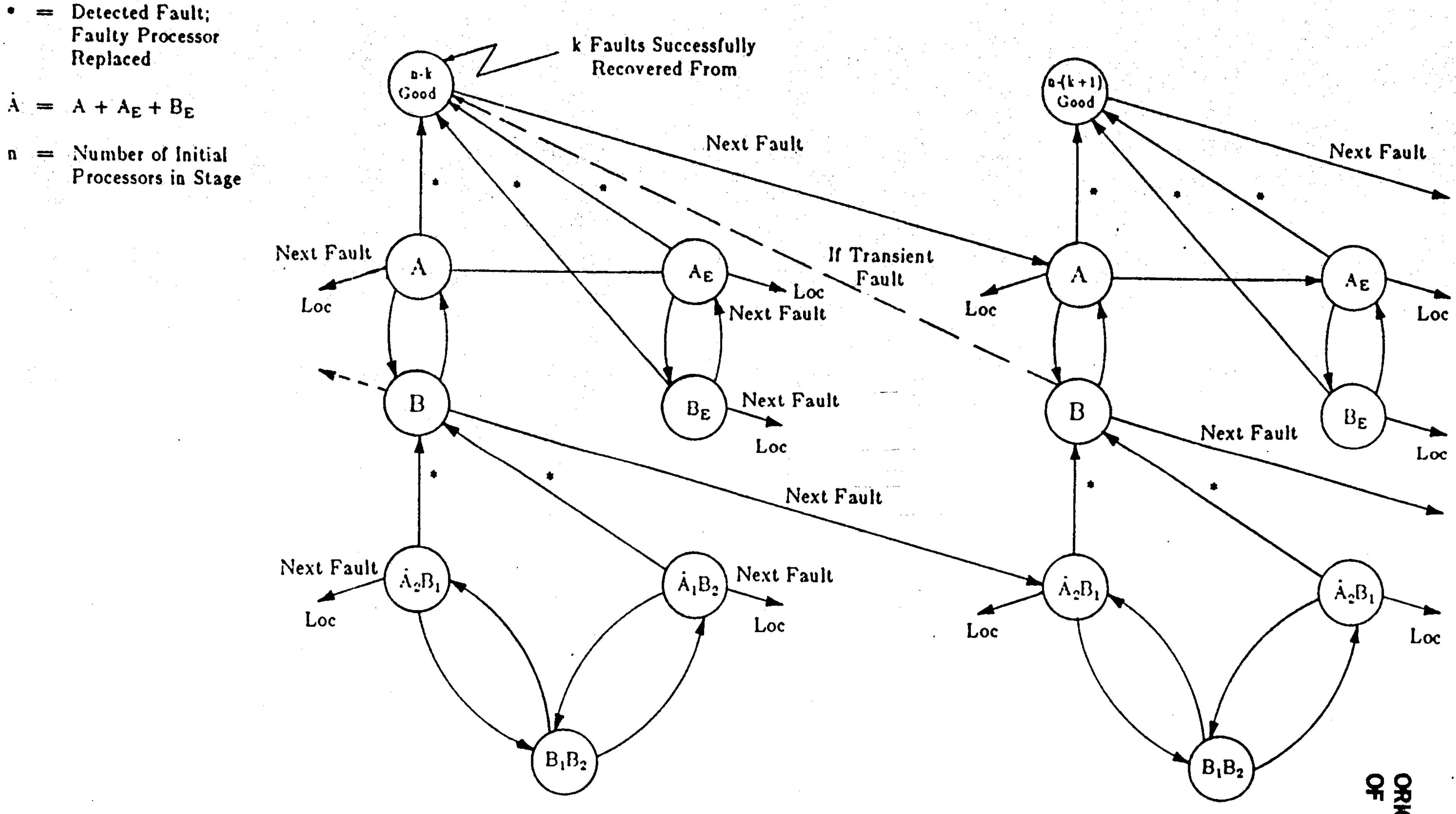
Transient Fault: $\alpha \neq 0, \beta = 0$

Double-Fault Model of CARE III



$$\dot{A}_1 = A_1 + A_{E_1} + B_{E_1}$$

$$\dot{A}_2 = A_2 + A_{E_2} + B_{E_2}$$


* = Detected Fault; Faulty Processor Replaced
$\dot{A}$ = A + A_E + B_E
n = Number of Initial Processors in Stage
k Faults Successfully Recovered From
n-k Good
n-(k+1) Good
A
B
A_E
B_E
$\dot{A}_2B_1$
$\dot{A}_1B_2$
B_1B_2
*
Next Fault
Loc
If Transient Fault

kth Fault

k+1th Fault

State Structure of a Stage
As Represented by CARE III

ARIES 82 FEATURES

Designed and Used for University Reliability Projects

Markov Model

- finite-state
- continuous-parameter
- time-homogeneous

State Aggregation: Limited Structural Decomposition

Instantaneous, State-Dependent Coverage

Constant Transition Rates

Transient and Permanent Faults

Spares

- powered
- unpowered
- blocked

Parametric Description for Six Basic Systems

Matrix Description for General Systems

ARIES SYSTEMS

Type 1	Closed FT System
Type 2	Closed FT System with Transient Fault Recovery
Type 3	Mission-Oriented Repairable System
Type 4	Repairable System with Transient Fault Recovery
Type 5	Repairable System with Restart
Type 6	Periodically Renewed Closed FT System
Type 7	State Transition Rate Matrix

Types 1-6 are fixed models instantiated by user-specified parametric values.

Type 7 accepts a user-defined transition-rate matrix describing the complete system.

TYPE 1

Closed FT System with permanent faults.

No external repair or renewal.

System has spares and can degrade after spares are exhausted.

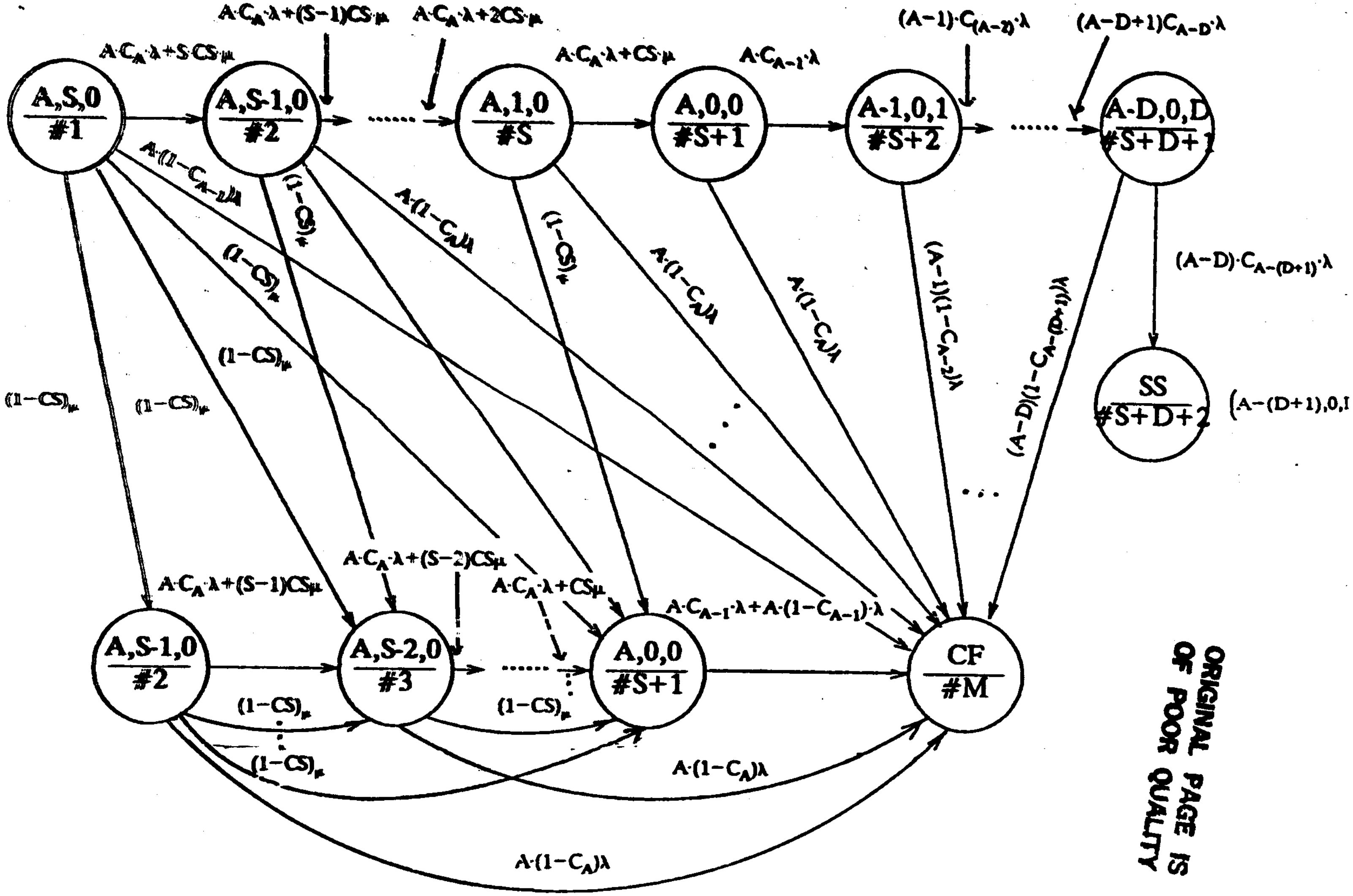
Ability to degrade can be blocked by unrecoverable spare failures.

Standby spares periodically tested.

Spare selection is predetermined.

A failed module is removed from system.

ARIES Markov Model for a Closed FT System (Type 1)



A = # Active
S = # Spares
D = # Degradations
λ = Active Failure Rate
μ = Spare Failure Rate
CS = Spare Coverage
C_A = Coverage While Spare Remain
C_i = Coverage for Transition to *ith* Degradation

TYPE 1 PARAMETERS

D	Number of Degradations
S	Number of Spares
CS	Spare Coverage
λ	Active module failure rate
μ	Spare module failure rate
$\underline{Y}$	Active resource vector
$\underline{CY}$	Coverage vector

$$\underline{Y} = (A, A\text{-}1, . . ., A\text{-}D, A\text{-}(D+1))$$

$$CY = (C_{A,} C_{A-1,} . . . , C_{A-D,} C_{A-(D+1)})$$

TYPE 1 PARAMETERS — RESTRICTIONS & ASSUMPTIONS

$CS<1$	=> $(\overline{A,S,D})$ states can be entered models blocked spares
λ and μ	are constant
$\mu = \lambda$	=> powered spares
$0<\mu<\lambda$	=> unpowered spares
$\lambda/\mu \leq 10^6$	(as specified)
$CY[0]$	is coverage for all transitions from states possessing spares
$CY[D+1]=0$	when no safe shutdown state is provided

TYPE 7 GENERAL MISSION-ORIENTED FT SYSTEMS

Any system that can be represented by a single state transition-rate matrix Q of the form

$$Q = \left[\begin{cases} q_{ij}, i \neq j \\ q_{j}, i = j \end{cases} \right]$$

where q_{ij} is the transition rate from state i to state j, and
q_{i} is the rate from state j to state j

Matrix can be input to ARIES symbolically or with actual numerical values

TYPE 7 (cont.)

System states can be partitioned into 5 disjoint subsets

Full Capacity (FC)
Degraded Capacity (DG)
FC with Blocked Spares (FCB)
Safe Shutdown (SS)
Crash Failure (CF)

so that

$$Q = \begin{array}{|c|c|c|c|c|l}
\quad & \quad & \quad & \quad & \quad & \text{FC} \\ \cline{1-5}
 & & & & & \text{DG} \\ \cline{1-5}
 & & & & & \text{FCB} \\ \cline{1-5}
 & & & & & \text{SS} \\ \cline{1-5}
 & & & & & \text{CF}
\end{array}$$

SOLUTION

Assumptions

System is finite-state, continuous-parameter Markov process.

Markov process is time-homogeneous.

Transition-rate matrix has distinct eigenvalues.

Solution

$$Q = \left[\begin{cases} q_{ij}, i \neq j \\ q_{j}, i = j \end{cases}\right]$$

Transition−Rate Matrix

$$P(t) = \left(p_1(t), p_2(t), \ldots, p_n(t)\right)$$

State Probabilities (n operational states)

$$P(t) = QP(t)$$

System Equation

$$P'(t) = e^{Qt}P(0)$$

Solution

$$P(t) = \sum_{i=1}^{n} e^{\sigma_i t} \left[\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{Q - \sigma_j I}{\sigma_i - \sigma_j} \right] P(0)$$

ARIES Solution using Sylvesters formula

$$R_k(t) = \sum_{i=1}^{n} p_i(t)$$

Reliability of k th subsystem

$$R(t) = \prod_{k=1}^{m} R_k(t)$$

System Reliability (m subsystems)

MOTIVATION AND CRITERIA FOR TEST CASES

Should demonstrate how to use the tool

Should demonstrate general applicability and limitations (not an exhaustive test of features)

Should be solvable using standard techniques

TEST CASES DO NOT DEMONSTRATE FULL CAPABILITY OF CARE III OR ARIES

In Particular for CARE III, the Following Important Features were not Highlighted

- The Impact of Aggregation of States in Handling Very Large Systems
- Full Use of Fault Handling Model Features
- Non-constant Failure Rates

TEST CASES

Simplex Processor

TMR with No Spares

M out of N

M out of N with Triple Fault

TMR with Powered Spares

TMR with Unpowered Spares

AIPS-like FCS

TEST CASE 1

Description

A simplex processor with a constant failure rate λ.

Purpose

A simple case to point out any computational, as opposed to modelling, differences.

Solution

$$P(SF) = 1 - e^{\lambda t}$$

$$\approx \lambda t \text{ for small } \lambda t$$

Results

λt	Direct Calculation	ARIES*	CARE III
0	0	0	0
1.59×10^{-23}	-2.78×10^{-17}	0	1.59×10^{-23}
1.30×10^{-19}	-2.78×10^{-17}	0	1.30×10^{-19}
1×10^{-16}	6.94×10^{-17}	6.94×10^{-17}	9.99×10^{-17}
5×10^{-16}	4.85×10^{-16}	4.85×10^{-16}	5.00×10^{-16}
1×10^{-15}	9.99×10^{-15}	9.99×10^{-16}	1.00×10^{-15}
1×10^{-12}	9.99×10^{-13}	9.99×10^{-13}	9.99×10^{-13}
1×10^{-10}	9.99×10^{-11}	9.99×10^{-11}	1.00×10^{-10}
1×10^{-3}	9.995×10^{-4}	9.995×10^{-4}	9.995×10^{-4}
1	6.32×10^{-1}	6.32×10^{-1}	6.32×10^{-1}

For $\lambda > 10^{-15}$, all methods give the same answer.

CARE III answers are accurate for much smaller values of λt.

Increased accuracy of CARE III results from computing unreliability directly.

*ARIES reports reliability. Unreliability was obtained by subtracting ARIES reliability answers from 1.

TEST CASE 2

Description

A TMR system with no spares.

Constant failure rate λ.

Purpose

Another basic system.

Solution

$$P(SF) = 1 + 2e^{-3\lambda t} - 3e^{-2\lambda t}$$

Results

t	Direct	ARIES 1	ARIES 7	CARE III
0	0	0	0	0
1	2.999500043E-8	2.999500043E-8	2.999500043E-8	2.9994993156E-8
5	7.4937529682E-7	7.4937529682E-7	7.4937529682E-7	7.4937446470E-7
10	2.99500474671E-6	2.99500474671E-6	2.99500474671E-6	2.9950040243E-6
.01	2.99996139042E-12	2.99996E-12	2.99996E-12	2.9999939165E-12
.10	2.99995001063E-10	2.99995E-10	2.99995E-10	2.9999519535E-10
7000	.50512196468	.50512196468	.50512196468	

TEST CASE 3

Description: M out of N

12 Processors
Perfect Coverage
SF iff 7 or More Faults

7 or More Faults
$\lambda = 10^{-4}$/hour/processor
t = 8000 hours

Purpose

A Basic M Out of N System

Solution

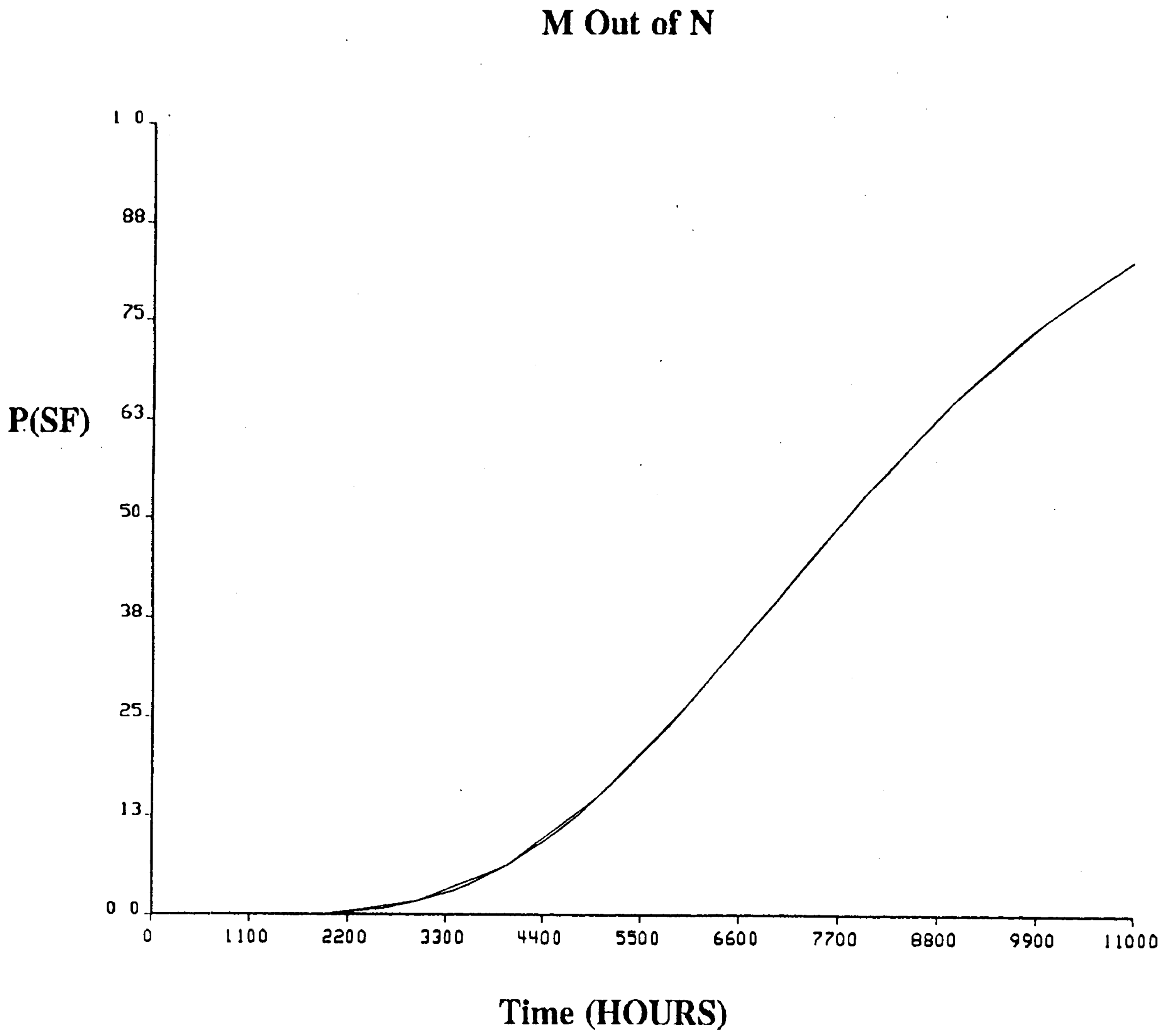
$$P(SF) = \sum_{k=7}^{12} \frac{12!}{k!(12-k)!} p^k q^{12-k}$$

$$\text{where } p = 1 - e^{-\lambda t}$$
$$q = e^{-\lambda t}$$

Results

	Direct Calculation	ARIES Type1	ARIES Type7	CAREIII
t=8000	.5288303411826796	.52883034118268013	.52883034118268137	.52883034118

The initial results for ARIES Type1 were incorrect: perfect reliability was maintained for more than 10,000 hours and then dropped several orders of magnitude. It was determined that ARIES was not correctly computing systems with >1 degradation and no spares. A modification was made to produce correct results.



M Out of N
P(SF)
1 0
88
75
63
50
38
25
13
0 0
0
1100
2200
3300
4400
5500
6600
7700
8800
9900
11000
Time (HOURS)

TEST CASE 4

Description: M out of N

5 processors
$\lambda = 10^{-4}$/hour/processor
Permanent Faults
SF iff

- 4 or more faults

- Faults preclude majority of good processors

Single Fault Model

- A fault is detected immediately as it produces an error

- Single point faults are excluded

- Only 2 concurrent active faults can cause SF

Imperfect Coverage

$P_A = P_B = 1$

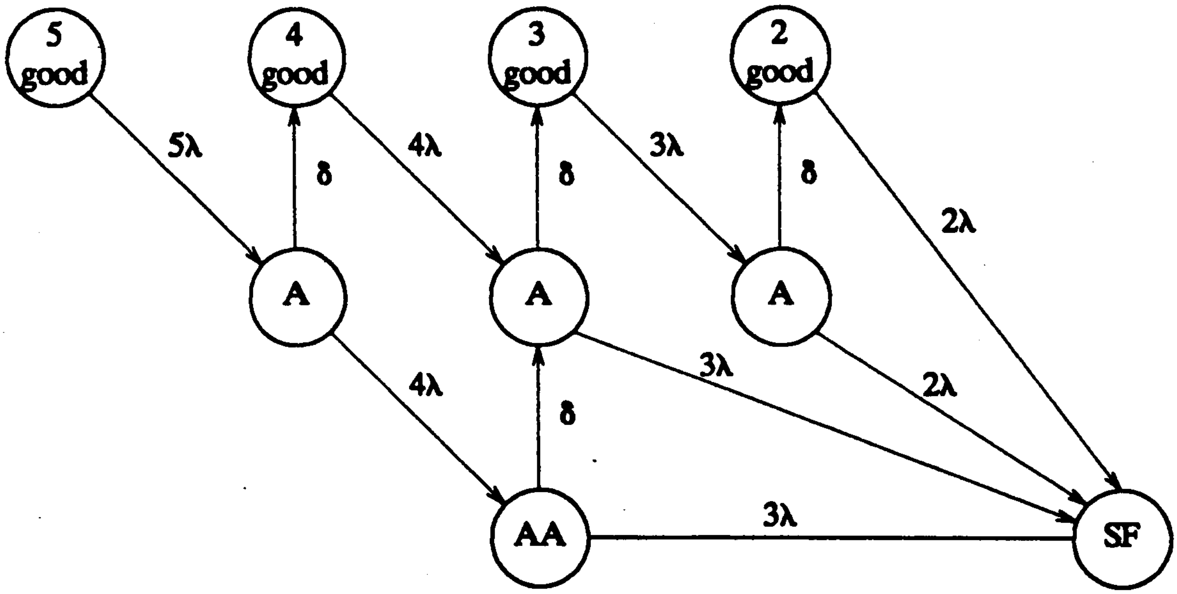
$\epsilon = 0$
$c = 1$
$\rho = 0$
$\delta = 3600$/hour

Purpose

An M out of N System with Triple Fault

TEST CASE 4 (cont'd)

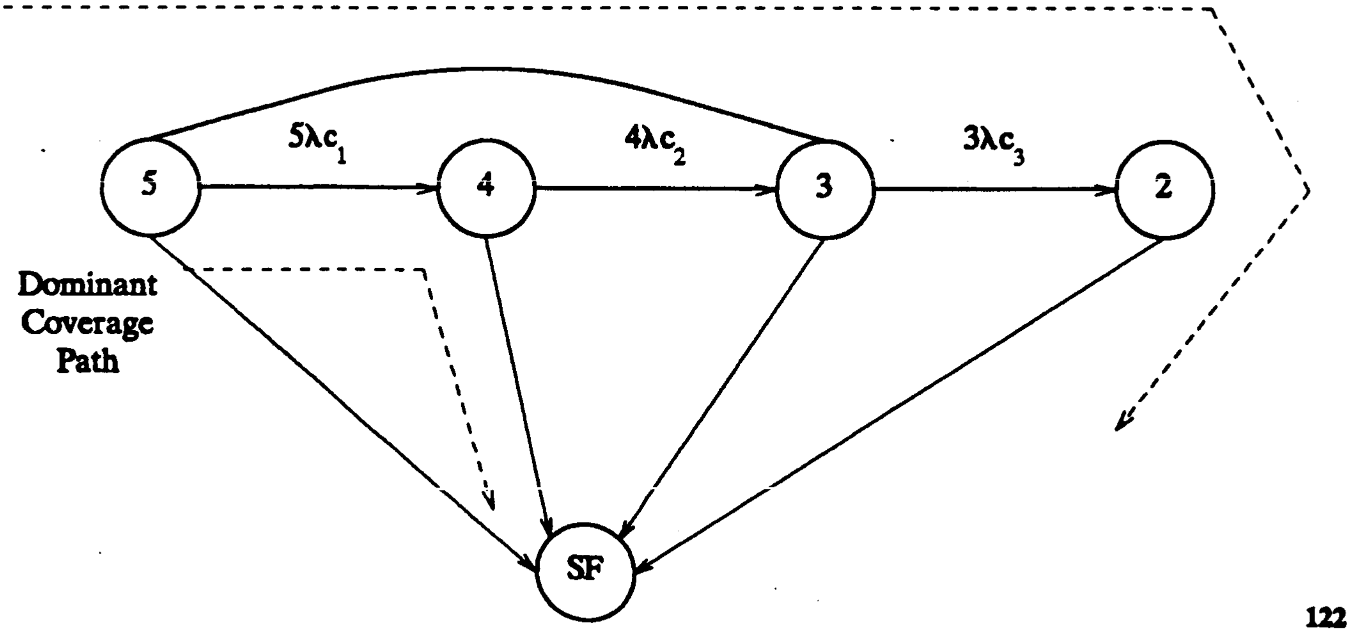
Model



Solution

Since λ/δ is small, instantaneous coverage can be used to simplify the model.

Exhaustion of Components



Test Case 4
(continued)

Dominant Term Due to Lack of Coverage

$$\left[P_{cov,5-4-F}(t)\right] \simeq \frac{1}{S}\left(\frac{5\lambda}{S+4\lambda}\right)\left(\frac{4\lambda}{S+4\lambda}\right)c_1(1-c_2)$$

By Partial Fraction Expansion and $^{-1}$

$$P_{cov,\,5-4-F}(t) \simeq c_1(1-c_2)\left[1-5e^{-4\lambda t}+4e^{-5\lambda t}\right]$$

The Exhaustion of Components Is Approximately the Failure of 4 Out of 5.

Thus,

$$P_{SF}(t) \simeq \frac{3\lambda}{\delta}\left[1-5e^{-4\lambda t}+4e^{-5\lambda t}\right]+5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t}+\left(1-e^{-\lambda t}\right)^5$$

For Small λt

$$P_{SF}(t) \simeq \frac{30\lambda^3 t^2}{\delta}+5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t}+\left(1-e^{-\lambda t}\right)^5$$

Test Case 4
(continued)

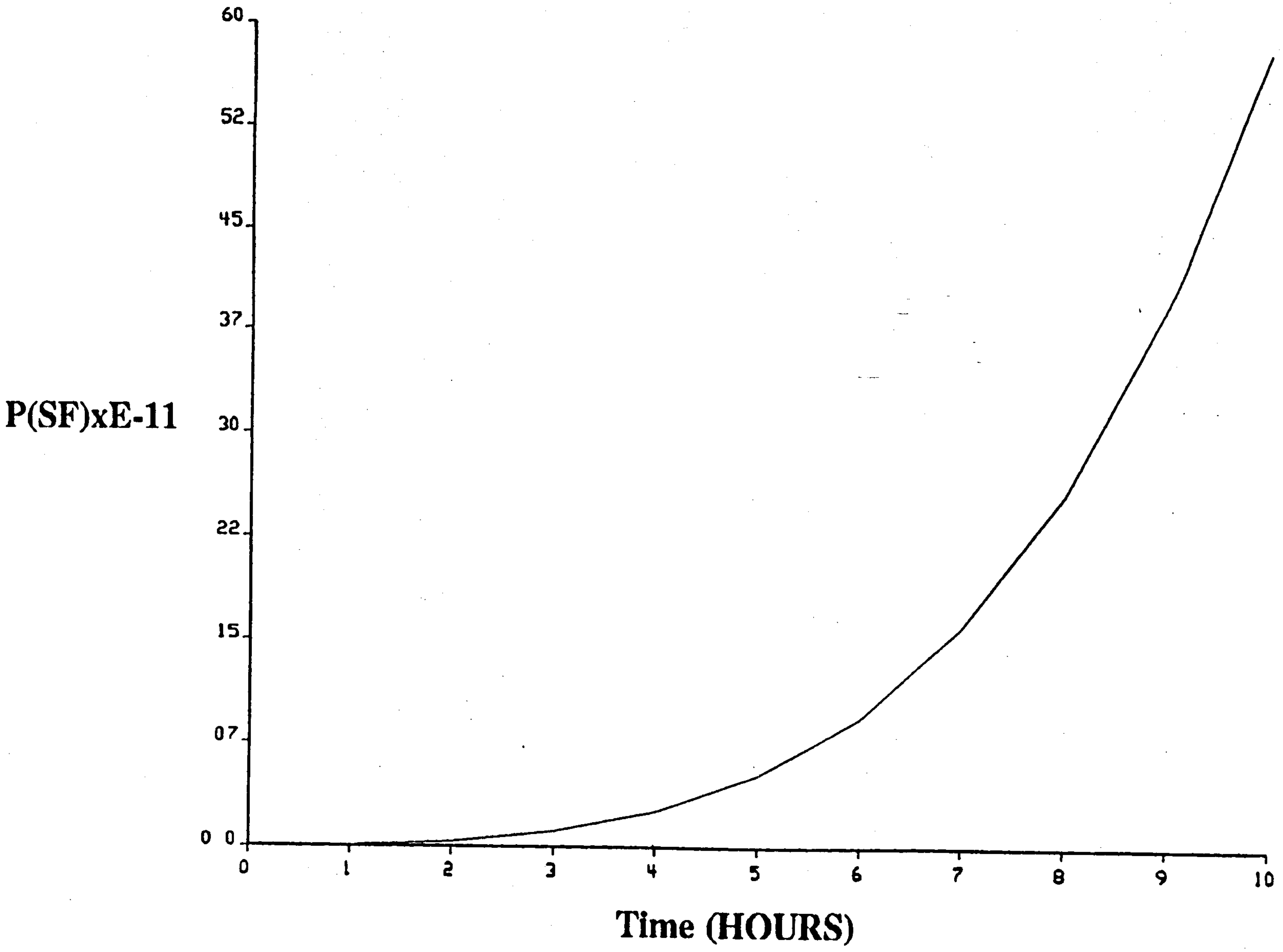
Results

t	Direct	ARIES 1	ARIES 7	CARE III
10	5.81936×10^{-12}	5.81801×10^{-12}	5.81907×10^{-12}	5.81935×10^{-12}

This case is not directly computable by CARE III due to the triple fault. Our result was obtained by using CARE III to solve for the P(SF) due to loss of 4 out of 5 processors and adding the hand-calculated P(SF) due to lack of coverage.

The ARIES Type 1 solution is an approximation made by including the path from 5 good to 3 good in the path from 5 good to 4 good.

M out of N with Triple Fault



TEST CASE 5

Description

TMR with 2 Powered Spares and Permanent Faults
$\lambda = 10^{-4}$/hour/processor
t = 10 hours
Imperfect Coverage
$\rho = 0$
$c = 1$
$\epsilon = 0$
$P_A = P_B = 1$
$\delta = 3600$/hour

Purpose

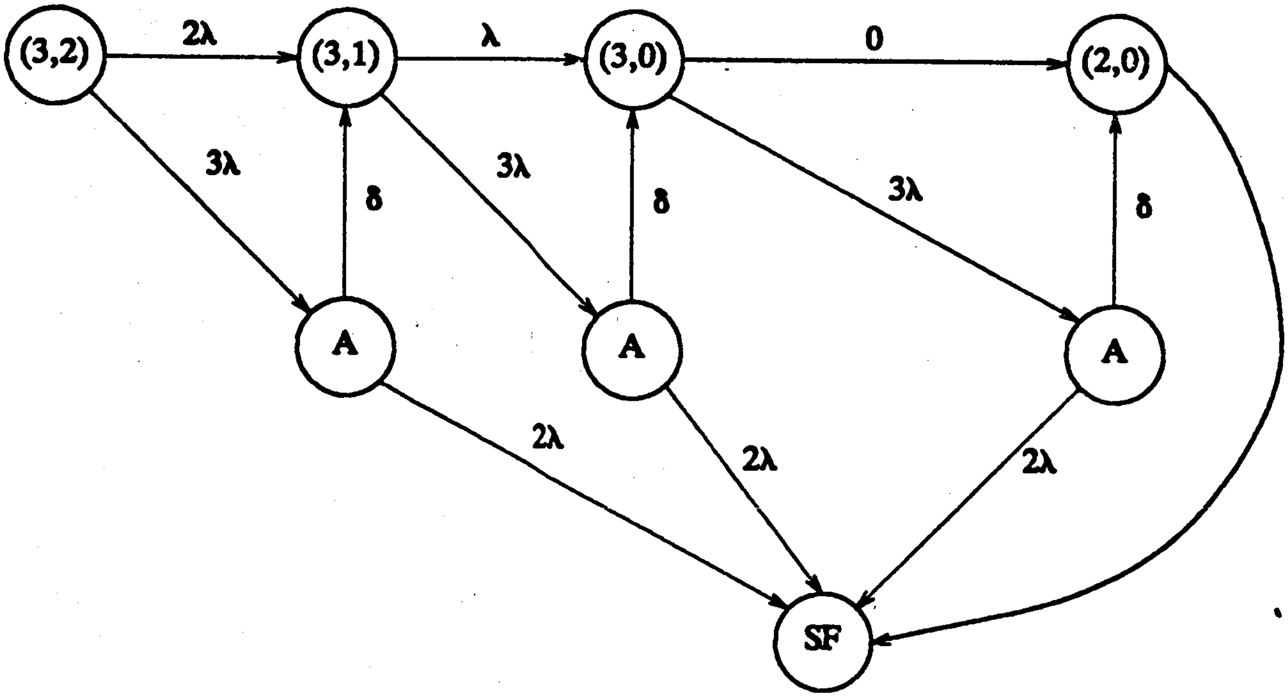
Easily Analyzed Using Instantaneous Coverage
Well Suited for CARE III and ARIES

Results

	Direct	ARIES 1	ARIES 7	CARE III
t=10	$1.7165269 \times 10^{-10}$	$1.7165291 \times 10^{-10}$	1.716543×10^{-10}	$1.7068601501 \times 10^{-10}$

TEST CASE 5 (cont'd)

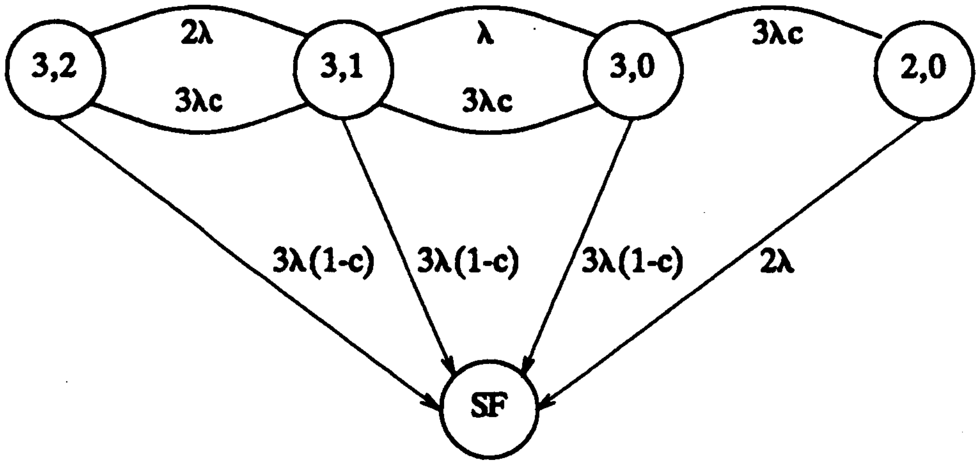
Model



TEST CASE 5

Solution

Since λ/δ is very small, the above model can be simplified by using instantaneous coverage.



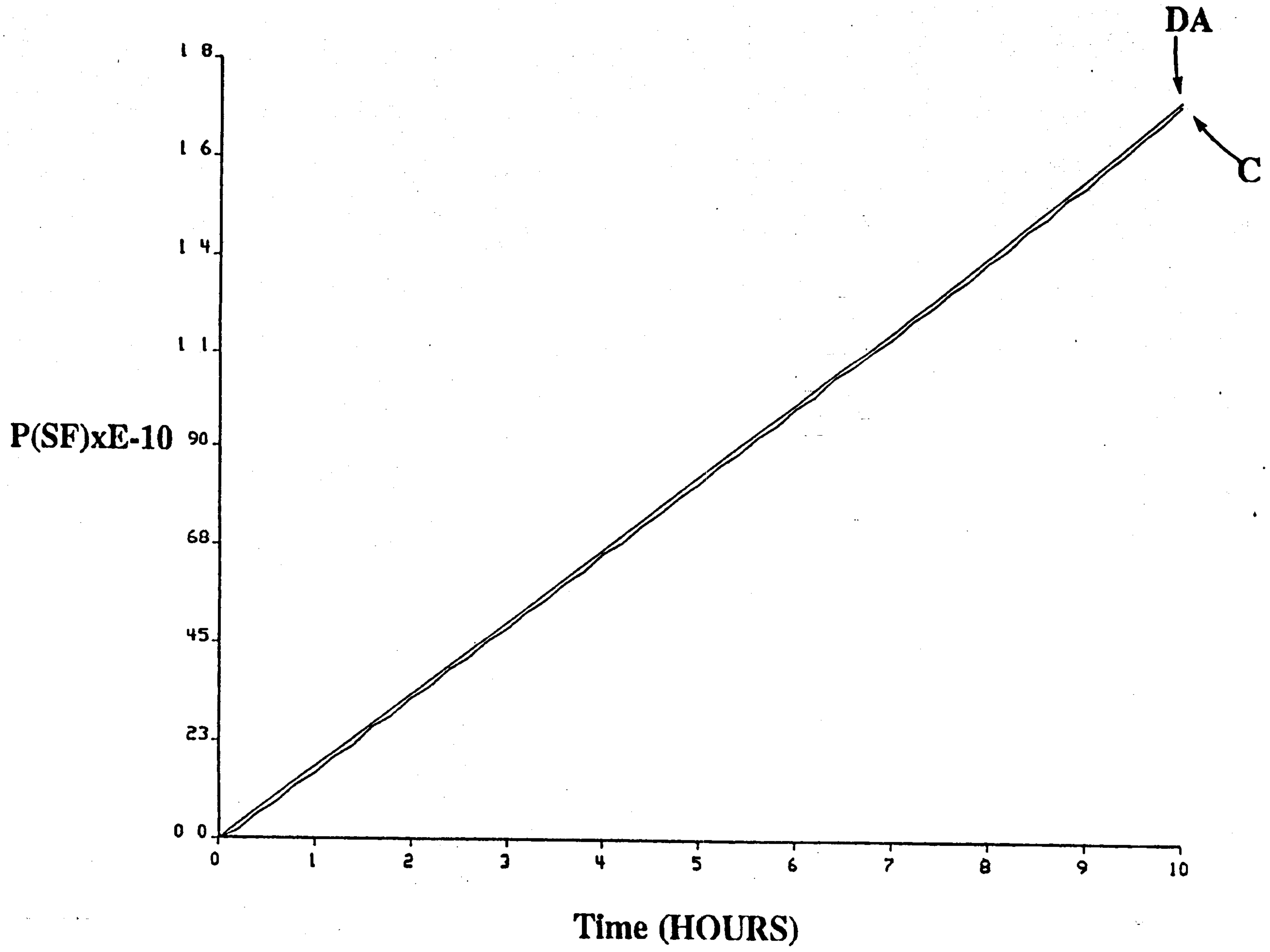
$$P_{SF}[t] \simeq (1-c)\left[1-(e^{-3\lambda t})\right] + 5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t} + \left(1-e^{-\lambda t}\right)^5$$

Coverage

Components (4 of 5)

$$P_{SF}[t] \simeq \frac{6\lambda^2 t}{\delta} + 5\left(1-e^{-\lambda t}\right)^4 e^{-\lambda t} + \left(1-e^{-\lambda t}\right)^5$$

TMR with Powered Spares



TEST CASE 6

Description

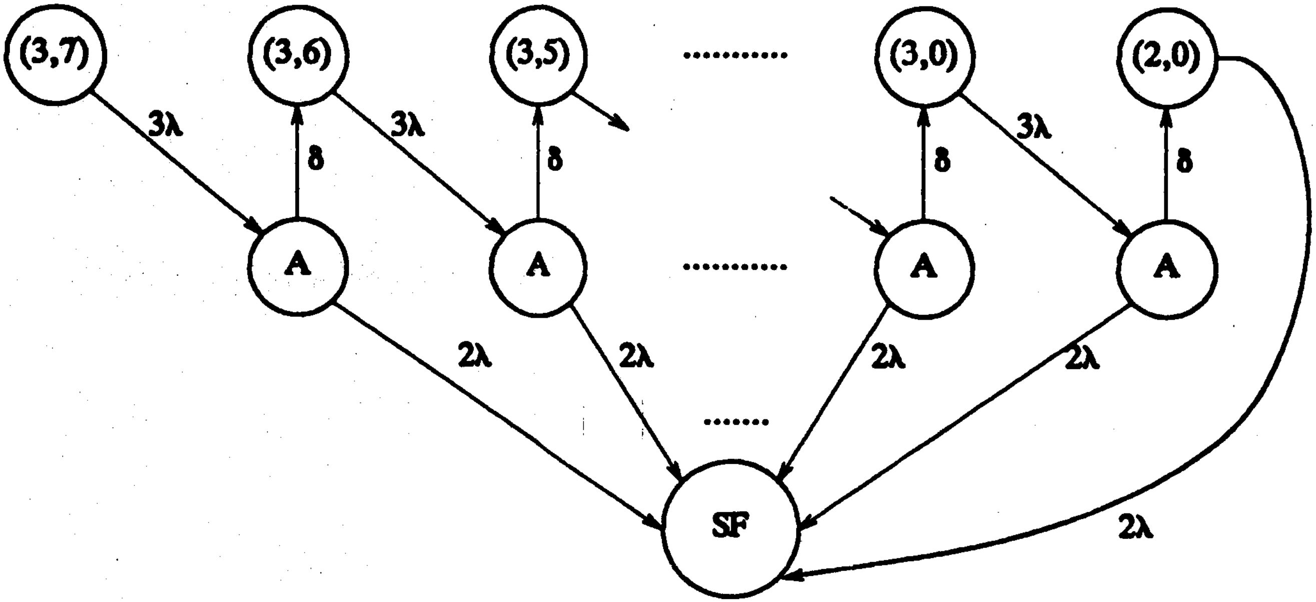
TMR with 7 Unpowered Spares and Permanent Faults
$\lambda = 10^{-4}$/hour
t = 10 years = 87,600 hours
Imperfect Coverage
$\rho = 0$
$c = 1$
$\epsilon = 0$
$P_A = P_B = 1$
$\delta = 3600$/hour

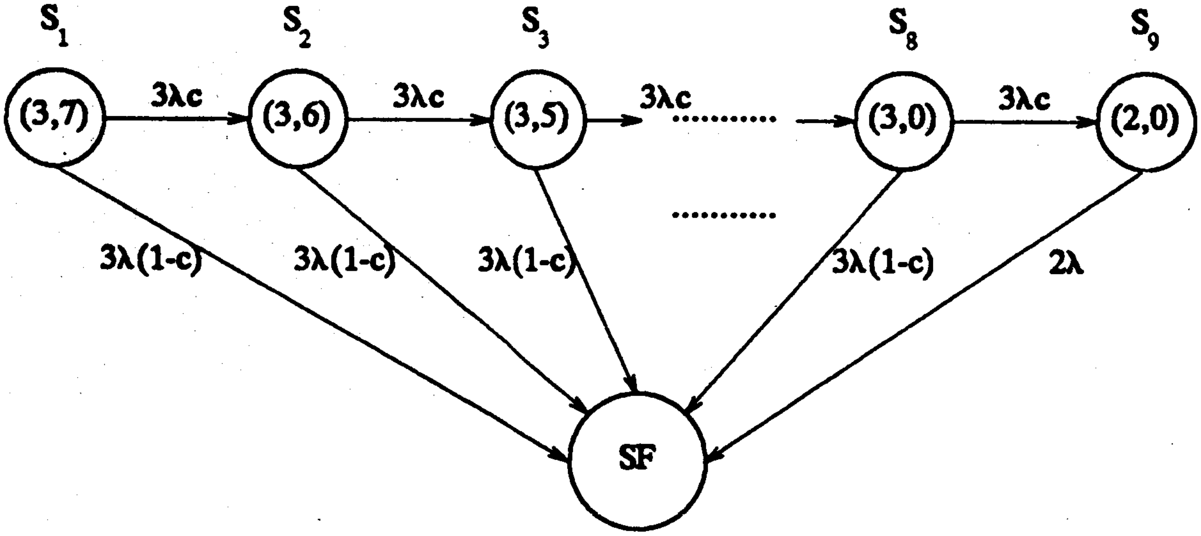
Purpose

Markov Model Has Multiple Eigenvalues

TEST CASE 6

Model





Instantaneous Coverage Markov Model

Solution

Lack of Coverage

$$\left[P_{cov}(t)\right] = \frac{3\lambda(1-c)}{S}\left[\frac{1}{S+3\lambda} + \frac{3\lambda c}{(S+3\lambda)^2} + \cdots + \frac{(3\lambda c)^7}{(S+3\lambda)^8}\right]$$

$$\left[P_{cov}(t)\right] \simeq \frac{3\lambda(1-c)}{S(S+3\lambda)}$$

$$P_{cov}(t) \simeq \frac{2\lambda}{\delta}\left[1-e^{-3\lambda t}\right]$$

Exhaustion of Components

$$\left[P_{CE}(t)\right] = \frac{2\lambda}{S+2\lambda}\left(\frac{3\lambda c}{S+3\lambda}\right)^8$$

By Partial Fraction Expansion for Repeated Roots and $^{-1}$.

$$P_{CE}(t) \simeq 1-3^8e^{-2\lambda t} + e^{-3\lambda t}\left[6560 + 2186(3\lambda)t + 728(3\lambda)^2\frac{t^2}{2} + 242(3\lambda)^3\frac{t^3}{6}\right.$$

$$\left. + 80(3\lambda)^4\frac{t^4}{24} + 26(3\lambda)^5\frac{t^5}{120} + 8(3\lambda)^6\frac{t^6}{720} + 2(3\lambda)^7\frac{t^7}{5040}\right]$$

All Terms Up to the 9th Power Cancel

Source of Computational Problems in First 1000 Hours.

Results

Type 1

Will Not Accept $\mu = 0$

Should Accept $\mu = \frac{\lambda}{10^6}$

Unmodified Version Accepts $\mu = \frac{\lambda}{100}$

Modified Version Accepts $\mu = \frac{\lambda}{10}$

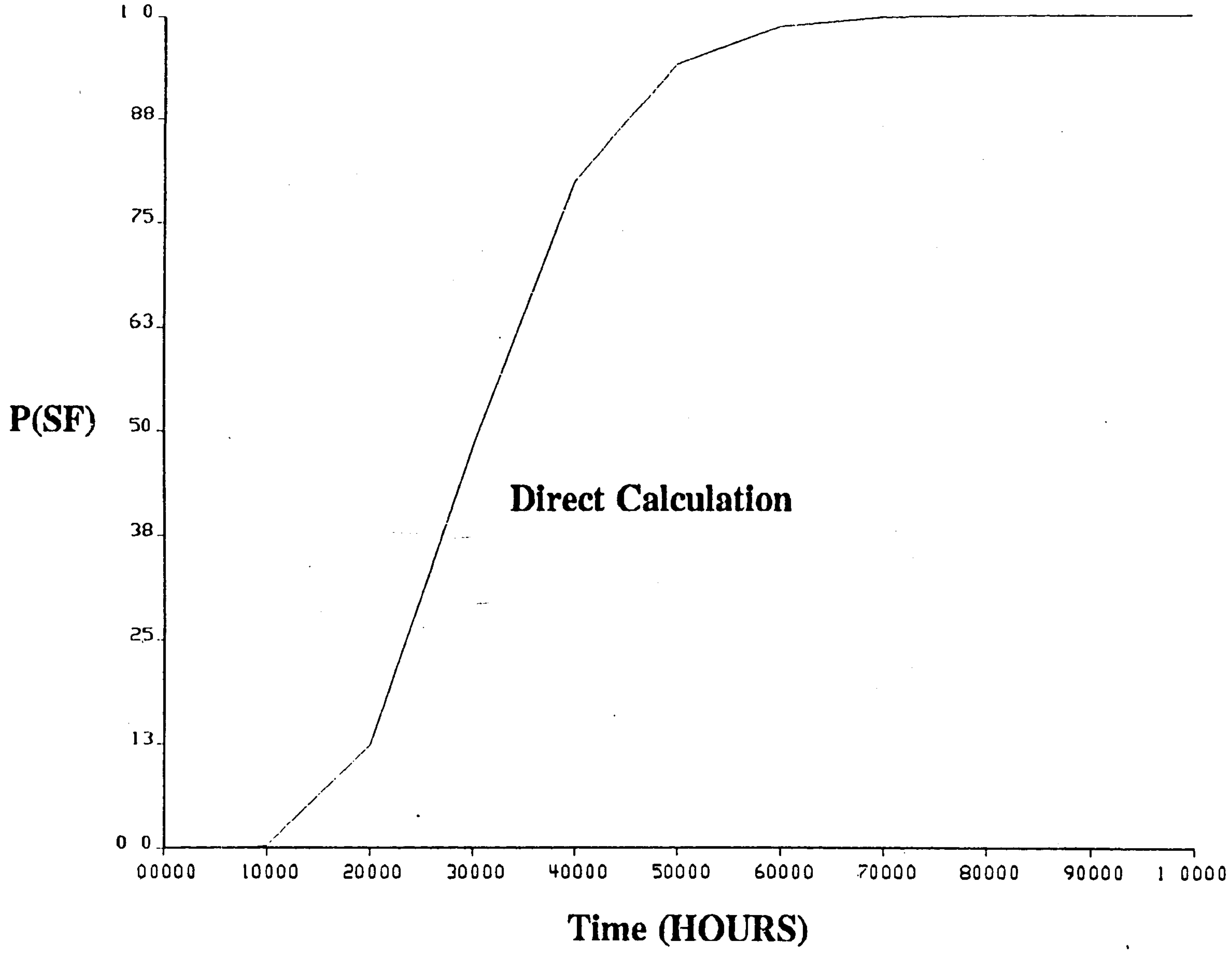
Type 7

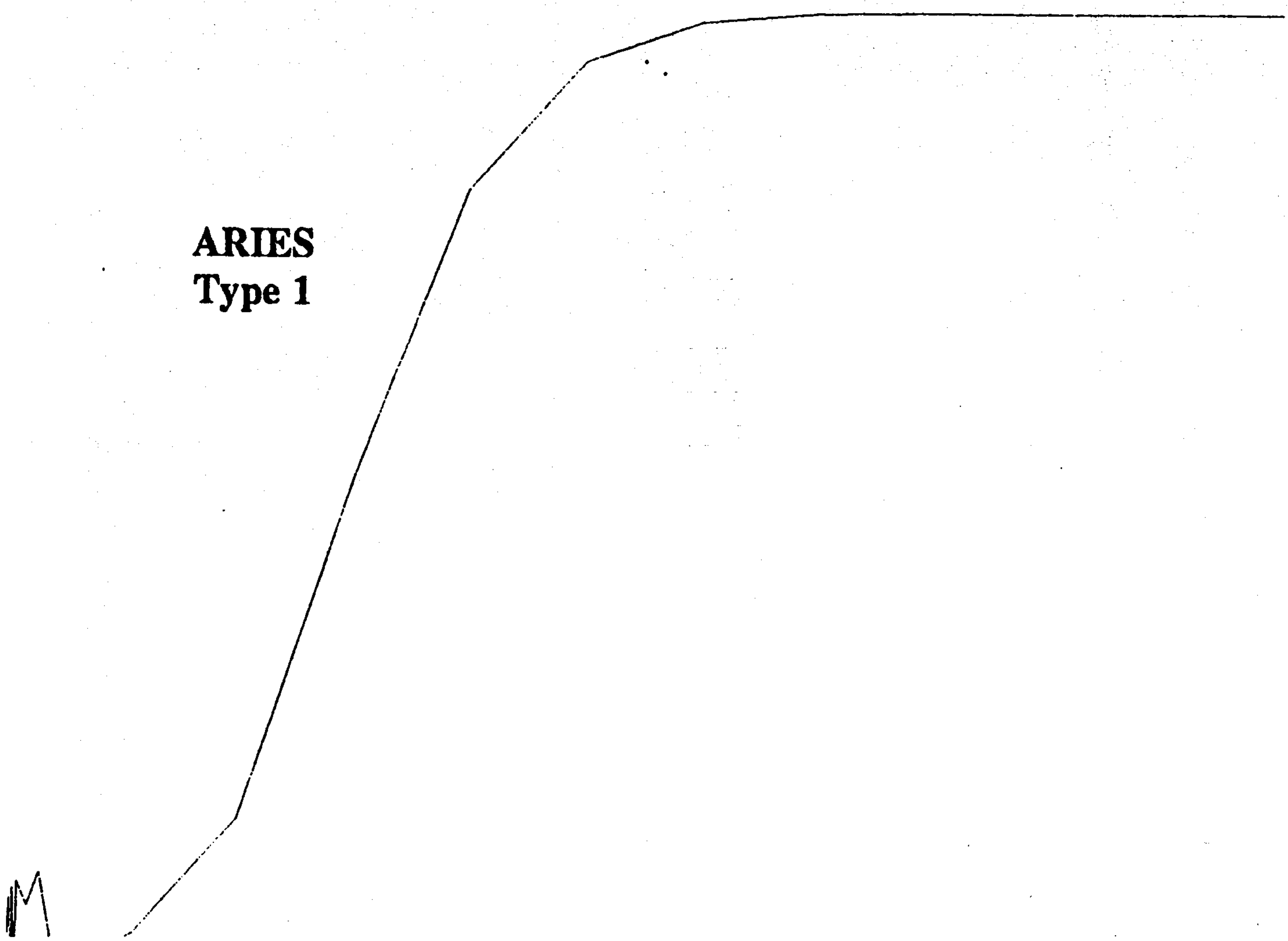
Eigenvalues Are -3λ (8 times and -2λ)

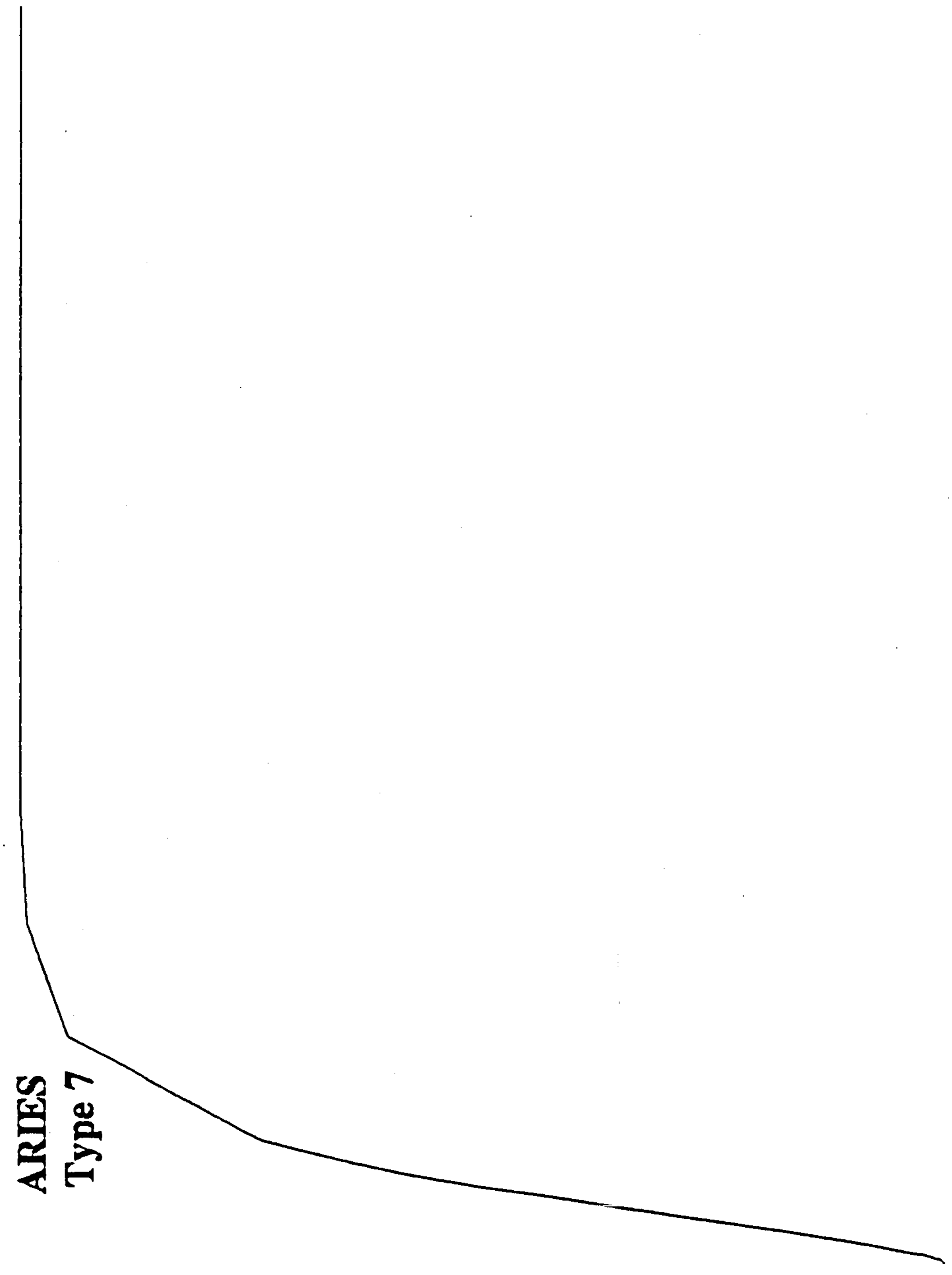
To Solve System, Duplicates Are Dropped So System Is Solved with 2 eigenvalues, -3λ and -2λ

Solution for This System Is Same As For TMR With No Spares

TMR with Unpowered Spares




ARIES
Type 1



ARIES
Type 7

TEST CASE 7

Purpose

To Highlight Assumptions Required to Use ARIES and CARE III for an AIPS-like Architecture

- The Two Triplex Sets Simulate FTMP
- The Reversion to the Second Triplex Set Simulates Functional Migration (Assume Perfect)
- Assumed Network Does Not Impact Reliability
- Triple, Near-Coincident Faults Are Not a Factor in Loss of System. For This, Quintuplex Processors Are Needed. Thus, CARE III Does Not Need to Accommodate More than 2 Near-Coincident Faults.
- Sequence-Dependent Faults Are Not a Factor in Loss of System Because of the Reliabiliy of the Bus Network

Test Case 7
(continued)

Description

- AIPS-Like FCS
  Quad sensors, $\lambda_S = 10^{-4}$/hour/sensor (8 sets)
  Quad Actuators, $\lambda_A = 10^{-4}$/hour/actuator (8 sets)
  Triplex Processors, $\lambda_{P1} = 10^{-3}$/hour/processor (1 set)
  Triplex Processors, $\lambda_{P2} = 10^{-3}$/hour/processor (1 set)
  Permanent Faults
  Perfect Coverage
  $t = 10$ hours

- System Operation

After loss of the triplex processor set, its functions are performed by the second triplex set, provided that it is still functional

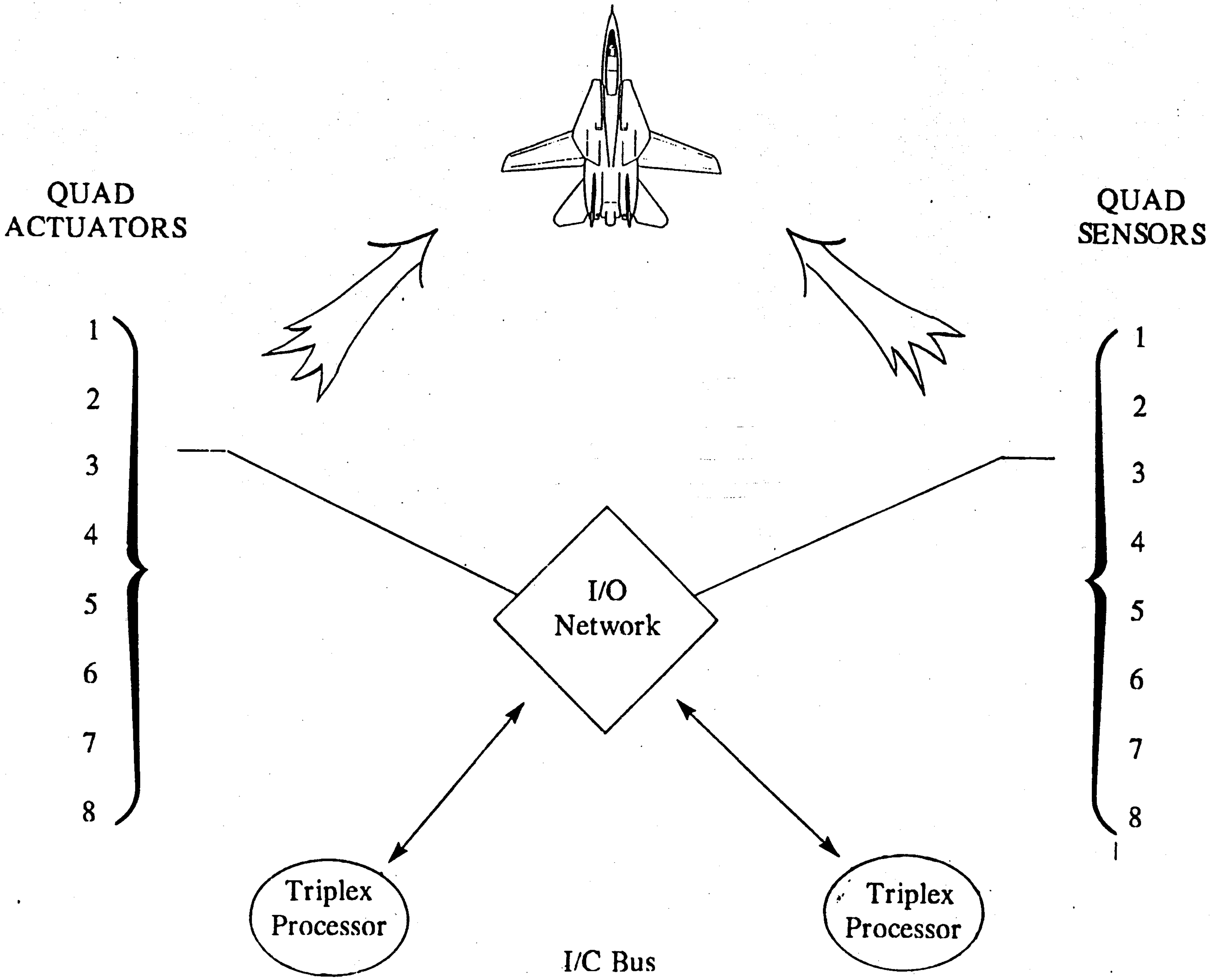
Second triplex set was formerly performing non-critical functions and was not vulnerable to critical fault pairs.

- LOC iff

  Loss of a Sensor Set (1 of 8)

  Loss of an Actuator Set (1 of 8)

  Loss of Processing Function
    Loss of 2 of the First Triplex Set
    Loss of 2 of the Second Triplex Set


QUAD ACTUATORS
1
2
3
4
5
6
7
8
QUAD SENSORS
1
2
3
4
5
6
7
8
I/O Network
Triplex Processor
Triplex Processor
I/C Bus

Test Case 7
(continued)

Solution

Independent Subsystems Leads to Structural Decomposition

$P[SF] \simeq P(E_S) + P(E_A) + P(E_{P1}E_{P2})$

$E_S =$ Loss of Sensor Set (1 of 8)

$E_A =$ Loss of Actuator Set (1 of 8)

$E_{P1} =$ Loss of Primary Processor

$E_{P2} =$ Loss of Backup Processor

$P[E_S] \simeq 32\lambda_S^3 t^3$

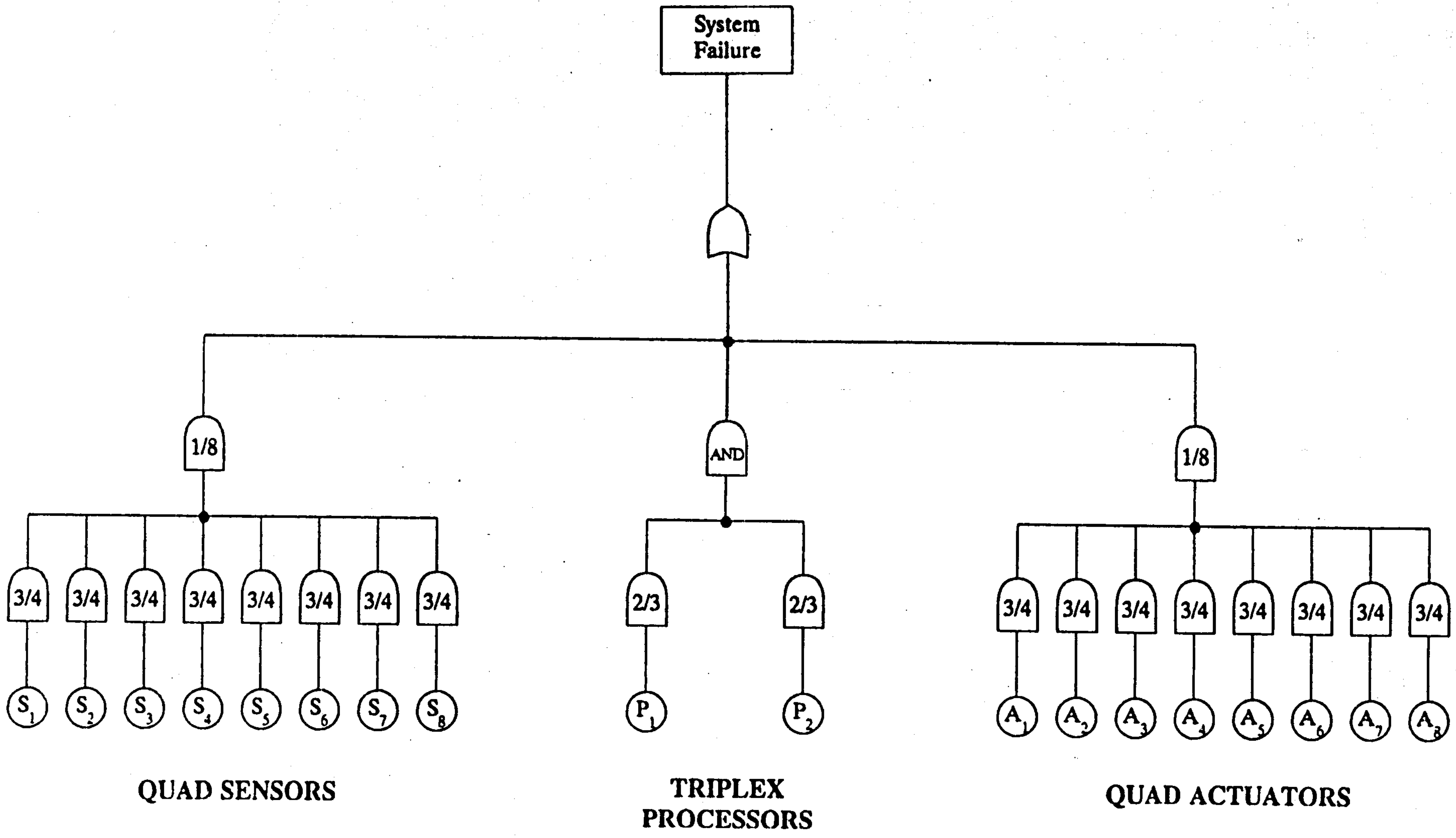
$P[E_A] \simeq 32\lambda_A^3 t^3$

$P[E_{P1}E_{P2}] = P[E_{p1}]P[E_{P2}]$

$\simeq 9\lambda_{pt}^4 t^4$

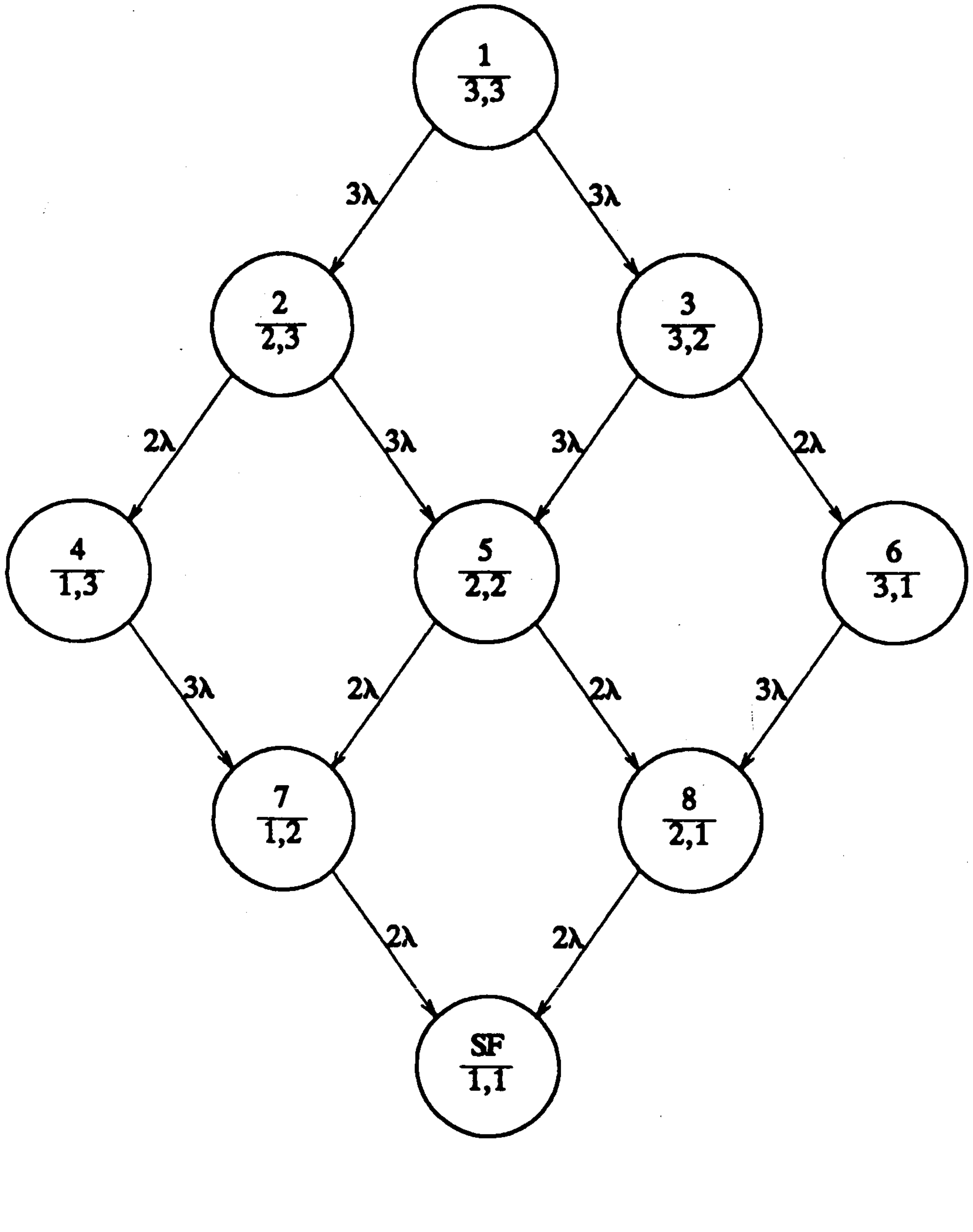
$P[SF] \simeq 32\lambda_S^3 t^3 + 32\lambda_A^3 t^3 + 9\lambda_P^4 t^4$

FAULT TREE


System Failure
1/8
AND
1/8
3/4
3/4
3/4
3/4
3/4
3/4
3/4
3/4
2/3
2/3
3/4
3/4
3/4
3/4
3/4
3/4
3/4
3/4
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
P_1
P_2
A_1
A_2
A_3
A_4
A_5
A_6
A_7
A_8
QUAD SENSORS
TRIPLEX PROCESSORS
QUAD ACTUATORS

TEST CASE 7

Model (Processor sets)



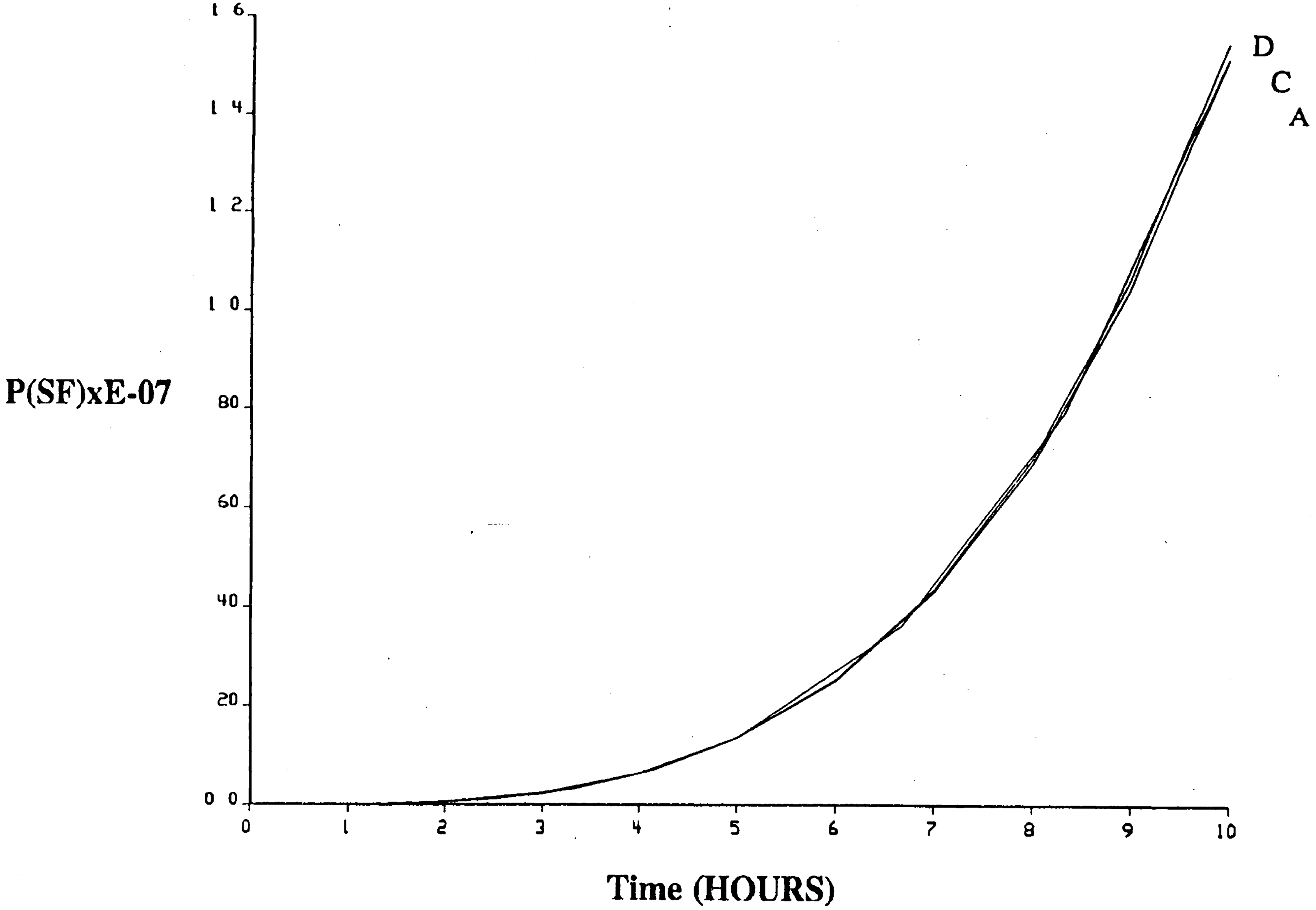
TEST CASE 7
(continued)

Results

	Direct	ARIES	CARE III
t=10	1.54×10^{-7}	$1.5090900654 \times 10^{-7}$	$1.5090886052 \times 10^{-7}$

Each Subsystem Fits ARIES Type 1 Model
Series Configuration of Subsystems Assumed
Processor Subsystems are not Configured Serially — Can Be Combined Into One Type 7 Subsystem
CARE III Fault Tree Allows More Flexibility in Configuring System

AIPS-Like FCS



USER-RELATED

Advantages

Interactive.
Can save and reload a system.
Help facility.
Output in plottable format.
Can create log file.
Can accept input from a command file.

Can Compute Other Performance Measures:

Mean time to first failure.
System failure rate.
Normalized probability of failure.
Reliability improvement factor
(one system vs. another).
Mission time improvement factor
(one system vs. another).
Life-Cycle measures
(for single subsystem).

Disadvantages

Cannot modify a system and reload it.
Cannot exit from define command prompts.
Necessary information scattered throughout
user's guide.
No support.

CARE III USER-RELATED

Advantages

System Fault Tree Input

Easily Modified Input Files

Output Provides Feedback

Output Options

Limited Plotting Capability

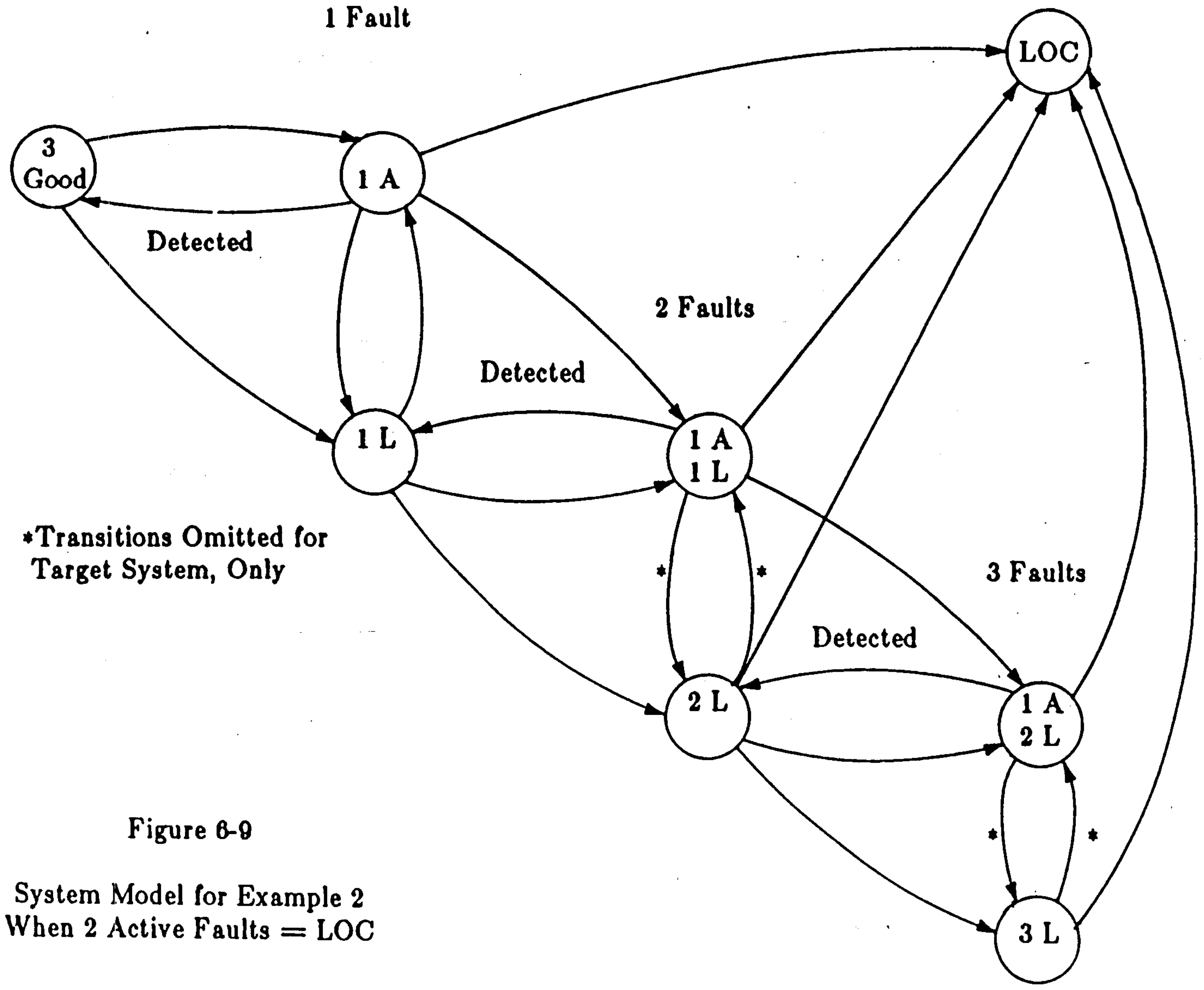
Disadvantages

Not Fully Interactive

OBSERVATIONS REGARDING CARE III

- Does Not Handle Near Coincident Faults for N>2
- Does Not Handle Sequence Dependent Faults
- Double Fault Model Is Conservative
- Designed for Ultrareliable Regime
- Spares Must be Powered
- Fault Handling Model While Somewhat Flexible is Restrictive in Some Respects, e.g., Only One Entry Point Identical Transition Rates on Intermittent States, Does Not Depend on System State, Fault Handling Time Assumed Short Relative to Failure Rate
- Closed System
- Not Fully Interactive

Three Fault Model



*Transitions Omitted for
Target System, Only

Figure 6-9

System Model for Example 2
When 2 Active Faults = LOC

CARE III LIMITATIONS FOR AIPS APPLICATIONS

- Evaluates Closed System
  (Some AIPS Applications Include Maintenance)
- Sequence Dependent Faults Not Directly Evaluated
  (Function Migration, Partial Cross-Strapping)
- Unpowered Spares Not Handled
  (Unpowered Spares A Must for Space)
- AIPS Needs Tool to Evaluate Network Reliability

CARE III FEATURES OF POTENTIAL VALUE TO AIPS

- Fault Handling Model
- Handles Large Systems
- Evaluation of Reliability in Ultrareliable Regime
- Non Constant Failure Rates
- Double Fault Model

ARIES CONCLUSIONS

MODEL

Advantages

Flexible with respect to spares

powered, unpowered, blocked

Parametric instantiation of six predefined system models

Accepts matrix description of systems

Disadvantages

Instantaneous coverage (computed externally by user)

Constant transition rates

Spares can be unpowered but must have a nonzero failure rate no smaller than $\lambda/10^6$ and sufficiently large to insure distinct eigenvalues

ACCURACY

Only reports reliability to seven digits

Unverified and unsupported

Bugs

> Inaccurate results for type1 systems with more than 1 degradation and no spares
>
> Inaccurate copy of subsystems
>
> Various errors in interactive prompts

Calculation of reliability as opposed to unreliability subjects it to computational stress

An accuracy parameter has to be adjusted to get accurate results for type 7 systems

Inaccurate results can occur when eigenvalues are not distinct

CONCLUSION

- Subject to Limitations Previously Stated CARE III Can Be Used to Assess Reliability of AIPS-like Architectures.

- While ARIES Has A Number of Desirable Features, Its Limited Accuracy and its Status with Respect to Validation are Sufficient to Rule Out Its Use For AIPS.

Standard Bibliographic Page

1. Report No. NASA CR-178067	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle

EVALUATION OF RELIABILITY MODELING TOOLS FOR ADVANCED FAULT TOLERANT SYSTEMS

5. Report Date

October 1986

6. Performing Organization Code

7. Author(s)

Robert Baker and Charlotte Scheper

8. Performing Organization Report No.

9. Performing Organization Name and Address

Center for Digital Systems Research
Research Triangle Institute
Research Triangle Park, NC 27709

10. Work Unit No.

11. Contract or Grant No.

NAS1-16489

12. Sponsoring Agency Name and Address

National Aeronautics and Space Administration
Washington, DC 20546

13. Type of Report and Period Covered

Contractor Report

14. Sponsoring Agency Code

505-66-21-05

15. Supplementary Notes

Langley Technical Monitor: S. J. Bavuso
Task 16 Final Report

16. Abstract

Research Triangle Institute undertook an evaluation of the CARE III and ARIES 82 reliability tools for application to advanced fault tolerant aerospace systems. To determine reliability modeling requirements, the evaluation focused on the Draper Laboratories' Advanced Information Processing System (AIPS) architecture as an example architecture for fault tolerant aerospace systems. Advantages and limitations were identified for each reliability evaluation tool.

CARE III was designed primarily for analyzing ultrareliable flight control systems. The ARIES 82 program's primary use was to support university research and teaching. Both CARE III and ARIES 82 were not suited for determining the reliability of complex nodal networks of the type used to interconnect processing sites in the AIPS architecture.

RTI concluded that ARIES was not suitable for modeling advanced fault tolerant systems. It further concluded that subject to some limitations (the difficulty in modeling systems with unpowered spare modules, systems where equipment maintenance must be considered, systems where failure depends on the sequence in which faults occurred, and systems where multiple faults greater than a double near coincident faults must be considered), CARE III is best suited for evaluating the reliability of advanced tolerant systems for air transport.

17. Key Words (Suggested by Authors(s)) Reliability Modeling	18. Distribution Statement Unclassified - Unlimited Subject Category 65

19. Security Classif.(of this report) Unclassified	20. Security Classif.(of this page) Unclassified	21. No. of Pages 159	22. Price A08

For sale by the National Technical Information Service, Springfield, Virginia 22161