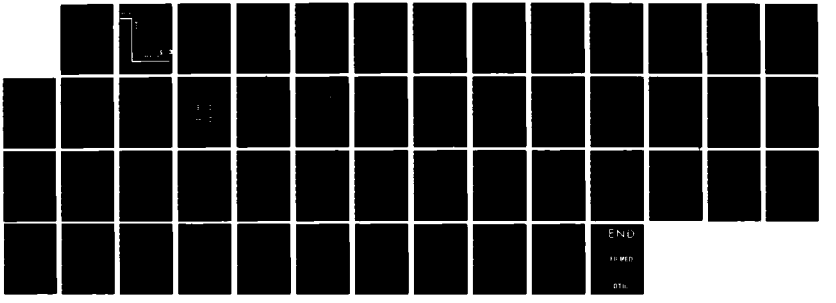
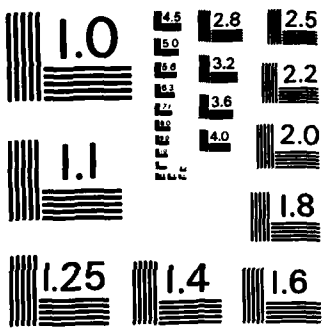
AD-A161 981 LOGISTICS ENGINEERING ANALYSIS TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS(U) AIR FORCE HUMAN RESOURCES LAB BROOKS AFB TX J C MCMANUS NOV 85 1/1

UNCLASSIFIED AFHRL-TR-84-60 F33615-82-C-0002 F/G 1/4 NL





AFHRL-TR-84-60

(12)

AIR FORCE HUMAN RESOURCES LABORATORY

AD-A161 981

LOGISTICS ENGINEERING ANALYSIS TECHNIQUES FOR FAULT-TOLERANT AVIONICS SYSTEMS

Michael H. Veatch
Alberto B. Calvo
John F. Myers

The Analytic Sciences Corporation
One Jacob Way
Reading, Massachusetts 01867

James C. McManus

LOGISTICS AND HUMAN FACTORS DIVISION
Wright-Patterson Air Force Base, Ohio 45433-6503

November 1985

Final Report for Period March 1982 - March 1984

AIR FORCE SYSTEMS COMMAND
BROOKS AIR FORCE BASE, TEXAS 78235-5601

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely Government-related procurement, the United States Government incurs no responsibility or any obligation whatsoever. The fact that the Government may have formulated or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication, or otherwise in any manner construed, as licensing the holder, or any other person or corporation; or as conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

The Public Affairs Office has reviewed this report, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This report has been reviewed and is approved for publication.

WILLIAM B. ASKREN, Acting Technical Director
Logistics and Human Factors Division

DENNIS W. JARVI, Colonel, USAF
Commander

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS AD-A161 981
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) AFHRL-TR-84-60	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION The Analytic Sciences Corporation 6b. OFFICE SYMBOL (*If applicable*)	7a. NAME OF MONITORING ORGANIZATION Logistics and Human Factors Division
6c. ADDRESS (*City, State, and ZIP Code*) One Jacob Way Reading, Massachusetts 01867	7b. ADDRESS (*City, State, and ZIP Code*) Air Force Human Resources Laboratory Wright-Patterson Air Force Base, Ohio 45433-6503
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Air Force Human Resources Laboratory 8b. OFFICE SYMBOL (*If applicable*) HQ AFHRL	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F33615-82-C-0002
8c. ADDRESS (*City, State, and ZIP Code*) Brooks Air Force Base, Texas 78235-5601	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. 62205F; PROJECT NO. 1710; TASK NO. 00; WORK UNIT ACCESSION NO. 26
11. TITLE (*Include Security Classification*) Logistics Engineering Analysis Techniques For Fault-Tolerant Avionics Systems	
12. PERSONAL AUTHOR(S) Veatch, Michael H.; Calvo, Alberto B.; Myers, John F.; McManus, James C.	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM Mar 82 TO Mar 84	14. DATE OF REPORT (*Year, Month, Day*) November 1985 15. PAGE COUNT 52
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
communication, logistics analysis, fault-tolerant avionics, mean time between critical failure, identification, mean time between failure, (Continued)

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

This report presents a technique which performs reliability, supportability, and survivability (RSS) analysis of fault-tolerant, dynamically reconfigurable systems during early design. Implemented in the Mission REliability Model (MIREM) computer program, this method analyzes the structure of functional components in a system. Use of MIREM will allow design engineers to apply RSS analysis before the design is fixed.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL Nancy A. Perrigo, Chief, STINFO Office	22b. TELEPHONE (*Include Area Code*) (512) 536-3877 22c. OFFICE SYMBOL AFHRL/TSR

18. (Concluded)

mean time to repair
mission completion success probability

SUMMARY

In the past, logistics engineering disciplines have been applied to new avionics designs in the later stages of development. To ensure that avionics designs are reliable, supportable, and survivable in the operating environment, effective logistics engineering techniques are needed early in the development cycle. This technical report presents a technique which performs reliability, supportability, and survivability (RSS) analysis of fault-tolerant, dynamically reconfigurable systems during early design. Implemented in the MIssion REliability Model (MIREM) computer program, this method analyzes the structure of functional components in a system.

Specifically, MIREM determines a value for the Mean Time Between Critical Failure (MTBCF), along with other fault-tolerance indices. Given conditions specified by the user, MIREM will compute the probability that a critical function will operate at the time it is needed.

Use of the MIREM program in the analysis of the ICNIA architectures produced interesting findings. Increased reconfigurability between components that are already redundant does not necessarily improve reliability. Also, all reliability results depend to a large extent on the functional requirements of the specified mission.

The techniques in the MIREM program have been developed to perform RSS analysis of fault-tolerant systems. Application of these techniques to the ICNIA architectures demonstrated that they can be used to address redundancy, component quality, dynamic reconfigurability, and maintenance concepts during the early stages of design.

PREFACE

This report documents research and development work in reliability, supportability, and survivability prediction techniques for fault-tolerant avionics and their application to Integrated Communication, Navigation, and Identification Avionics. This work is jointly supported by the Air Force Human Resources Laboratory and the Air Force Wright Aeronautical Laboratories. The guidance and support of Messrs. Daniel V. Ferens and Robert L. Harris of these organizations are greatly appreciated.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

This report describes research and development (R&D) in the Impact Analysis of Integrated Communication, Navigation, Identification Avionics (ICNIA) program, an overview of which is depicted in Figure 1. The program has the goals of:

1. Developing logistics analysis methods that are appropriate for integrated, fault-tolerant systems early in the development cycle.

2. Investigating traditional and innovative maintenance concepts, in particular, evaluating deferred repair policies that would exploit fault tolerance to increase sustainability in limited repair environments.

3. Applying these techniques to the two ICNIA architectures under development.

4. Influencing the ICNIA designs to improve reliability and supportability.

5. Documenting the R&D results in a form amenable for use by design engineers.

R&D in the reliability, supportability, and survivability areas was preceded by front-end analyses to determine the applicability of existing techniques. The output of the R&D in each area consists of documented methods for evaluation of integrated, fault-tolerant designs and the associated logistics options, as well as specific evaluations and design feedback for the ICNIA designs.

1.2 BACKGROUND

The growing requirement for tactical aircraft Communication, Navigation, and Identification (CNI) avionics in the presence of volume, weight, power, and cost constraints is currently forcing avionics designers to consider system integration (Harris, 1981). Fault tolerance is one feature that an ICNIA system must have if reliability and support cost benefits are to be realized.

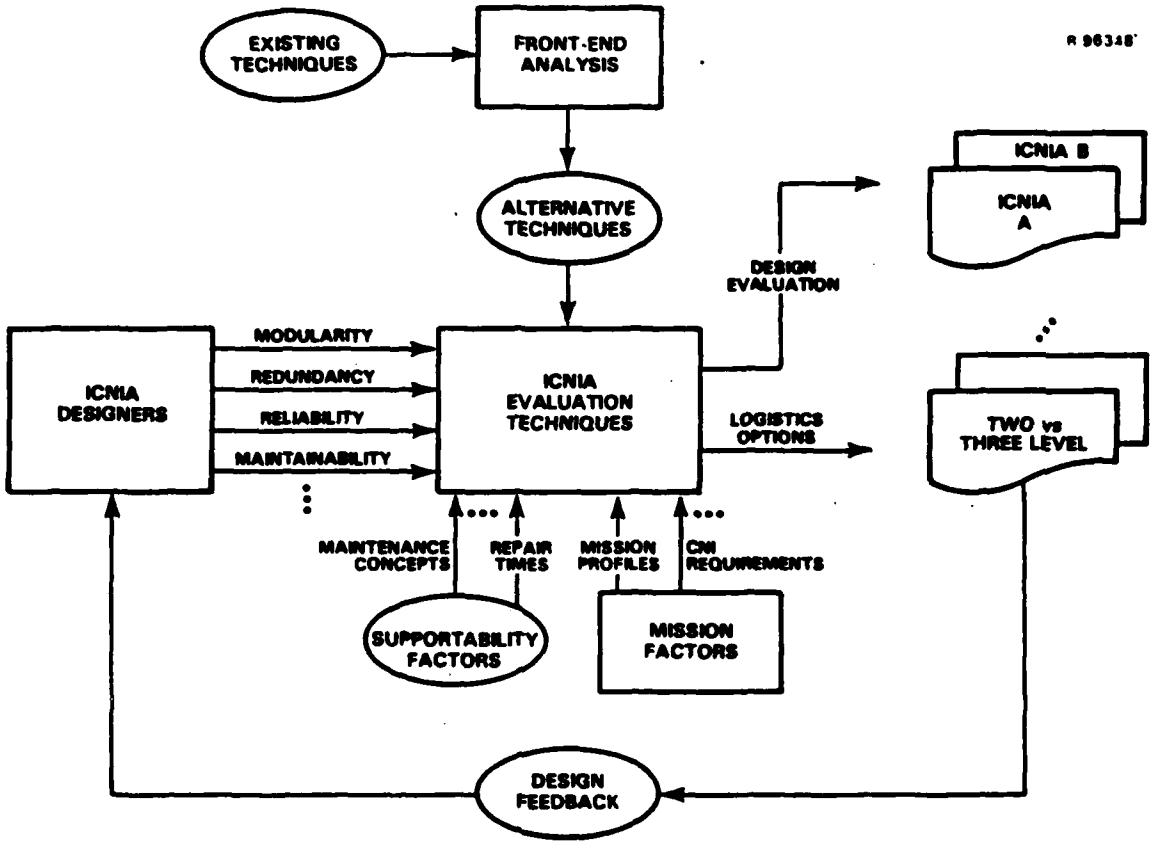


Figure 1. Overview of Impact Analysis of ICNIA Research Program Structure

Exploring the reliability, supportability, and survivability implications of an integrated, fault-tolerant architecture requires new techniques (Camana & Campbell, 1982).

Historically, logistics engineering disciplines have been applied to new avionics designs in the later stages of development. To ensure that avionics designs are reliable, supportable, and survivable in the operating environment, logistics engineering techniques are needed that can be effectively implemented during the advanced design phase of the system development cycle. Techniques employed in this phase will challenge design engineers to provide logistics support, reliability, and survivability capabilities before the design is fixed. In particular, logistics engineering techniques are needed that do not impose unrealistic detailed data requirements during the earlier stages of design.

The combination of these two factors creates a need for new and innovative logistics engineering techniques. The need currently exists in the two ICNIA system development programs that are being pursued at the Air Force Wright Aeronautical Laboratories. One program (System A) uses transversal filter technology, and the other (System B) employs analog large-scale integration technology. The Impact Analysis of ICNIA program was initiated to address this need.

1.3 FAULT-TOLERANT SYSTEM ELEMENTS

Fault tolerance in advanced integrated avionics systems, such as ICNIA, is achieved through dynamic fault detection, fault isolation, and reconfiguration. This dynamic process allows failed components to be replaced during a mission by backups or components that were originally assigned to other functions. Fault detection/isolation is performed by Built-In Test (BIT) equipment, which isolates faults to the lowest "failure unit," referred to as a component. A system control processor tracks function requirements and system health in terms of failed or good components. When a failure occurs or requirements change, the controller will reconfigure the system in an attempt to meet the function requirements. Function priorities may be preprogrammed for each mission phase and type of mission, or may be altered by the pilot according to the situations encountered during the mission. These system elements interact as shown in Figure 2.

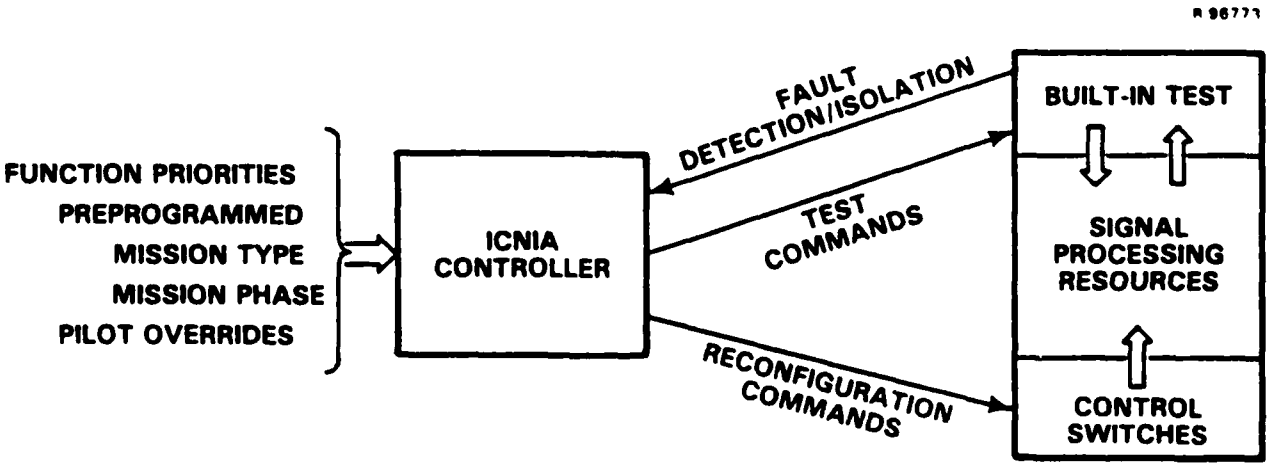


Figure 2. ICNIA Fault Tolerance Elements

The ICNIA architectures integrate 16 radio functions and contain reconfigurability that will allow a high degree of resource sharing between functions. This approach can provide high fault tolerance with few redundant components.

1.4 ORGANIZATION OF THIS REPORT

This report addresses methodology in the three major program areas: reliability, logistics support, and survivability. Chapters 2 and 3 present the analysis methodology for reliability and logistics support, respectively. In Chapter 2, the system architecture model, which is relevant to both areas, is also presented and an example introduced. Chapter 4 presents the survivability analysis, which included a feasibility study, methodology development, and generic findings. Conclusions relative to fault-tolerant systems in general are summarized in Chapter 5.

Veatch (1984a) analyzes the ICNIA system "A" system definition study architecture. It includes chapters on the data collection process, the network reliability model formed for this system, results in the areas of reliability and logistics support, and a summary of findings and recommendations. Veatch (1984b) analyzes the ICNIA system "B" system definition study architecture. It follows the same format as Veatch (1984a).

2. RELIABILITY ANALYSIS

The fault tolerance of ICNIA, achieved through dynamic reconfigurability, makes the analysis of system reliability more complex than for traditional systems. The integration of many radio functions creates interdependent failure modes that are not well described by existing measures of reliability. As a result, new measures of effectiveness are needed.

The applicability of previous work is examined in Section 2.1. A reliability methodology is then presented that includes development of fault tolerance indices and identification/classification of failure modes in a mission scenario. Mission scenarios are discussed in Section 2.3. An example architecture is presented in Section 2.4 and analyzed in Section 2.5. Some conclusions are drawn in Section 2.6.

2.1 FRONT-END STUDY FINDINGS

A front-end study was conducted to ascertain the applicability of existing reliability analysis techniques to ICNIA-type systems. The primary focus was to review the features of reliability models and procedures currently in use by the military services. Following is a brief summary of the techniques surveyed.

MIL-HDBK-217D Reliability Prediction of Electronic Equipment

This handbook is used for reliability estimation of individual components. Failure rates are estimated based on parts count and a stress analysis. Although this procedure is applicable to individual components, it does not address system structure, which is the key to fault tolerance.

MIL-STD-756 Reliability Prediction

This standard is used for system reliability prediction. Conventional combinatoric probability is used to relate series/parallel structures to mission, or system, reliability. The reconfigurable aspect of ICNIA-type systems is not captured.

DEPEND

The Determination of Equipment Performance and Expected Nonoperational Delay (DEPEND) (Air Force Wright Aeronautical Laboratories, 1978b) models reliability and availability for redundant systems with backup modes of operation. The model

considers the fault tolerance achieved through redundancy but not through the sharing of resources in an integrated system. As a result, the analysis of dynamically reconfigurable systems is limited.

AEP

The Avionics Evaluation Program (AEP) (Air Force Wright Aeronautical Laboratories, 1977) estimates mission success and abort rates, as well as costs. The model is essentially a Monte Carlo simulation of flight operations in a specified scenario. Redundancy is modeled at the subsystem level. Component redundancy, integrated systems and dynamic reconfiguration are not addressed. In addition, the magnitude of the model makes it inappropriate as an interactive design tool.

None of the models reviewed appear adequate in the area of representing integrated, reconfigurable systems. The literature on reliability theory of complex systems was also reviewed. The framework of structural reliability as developed algebraically by Birnbaum. (Birnbaum, Esary, & Saunders, 1961), or the equivalent fault-tree approach (Barlow & Proschan, 1975), applies to these systems. However, existing computational techniques, such as those in (Birnbaum & Esary, 1965), seem inadequate for dealing with the complex system structures needed to realistically model the ICNIA systems.

One approach that was taken to avoid the computational limits on reliability structures is Monte Carlo analysis. Even this approach requires the mapping from point failures into system failure. No suitable approach to defining this mapping for detailed ICNIA-type systems is available. Some progress in this area has been made by the ICNIA System A and B contractors. In particular, construction of the mapping has been avoided by the System B contractor by building a Monte Carlo simulation around the system control algorithm, which would determine whether a system failure occurred for each point failure that occurred. However, this approach does not lend itself to use as a reliability design tool in the early phases of development. The need for detailed data concerning the dynamic operating environment and the system controller, coupled with high computer run times, makes such a model cumbersome to use.

The primary conclusion of the front-end study was that the existing reliability techniques did not satisfy all of the analysis requirements for ICNIA-type systems. As a consequence, an essentially new methodology was developed and is described below.

2.2 METHODOLOGY

This section introduces the methodology for analyzing reliability of integrated, fault-tolerant systems. First, measures of effectiveness are defined. Next, a method of representing such systems by a structural reliability model is presented. Finally, computational techniques for the structural reliability model are developed. An overview of the model is provided at the end of the section.

Measures of Mission Reliability

Because of the multiplicity of functions supported by ICNIA and their varying importance to different missions, a combined measure of effectiveness for mission reliability is needed. Mission Completion Success Probability (MCSP) is the probability that a given set of critical functions is available throughout a given mission. A related measure is Mean Time Between Critical Failure (MTBCF), where a critical failure is a failure or a combination of failures that make a critical function unavailable. These measures are meaningful in a mission context where a set of CNI functions are considered critical for mission success. It is assumed that no repair action is taken between critical failures. When a single function is being considered as critical, MTBCF will be referred to as Mean Time Between Function Failure (MTBFF). Thus, the two measures are interchangeable when only a single function of the complete set of CNI functions is considered critical. A useful index of fault tolerance is failure resiliency, defined as the ratio of MTBCF (or MTBFF) to the traditional Mean Time Between Failure (MTBF). Since MTBF refers to the first failure in the system, failure resiliency is greater than or equal to one. Larger failure resiliency values correspond to systems with a higher degree of fault tolerance.

A single function is considered available if the system controller can select a configuration to bring the function up, with a specified level of performance. The availability of a set of functions is complicated by the competition between functions for resources. System resources are modeled as discrete "failure units" or components. A component fails as a unit and is monitored individually by the system controller for reconfiguration purposes. Component requirements vary over time depending on the presence of a signal or pilot input. The time history of component utilization can also be scheduled by the controller within certain tolerances. Thus, dynamic reconfigurability makes it difficult to determine whether functions conflict.

Structural Reliability Formulation

A practical approach to determining function availability is to classify components based on their dynamic features and then represent them accordingly in a static model structure. This approach makes rapid reliability computations possible and is taken in this study.

Three types of component utilization have been identified:

1. Contending: The functions are available if there is a configuration in which separate components are used to perform each function.

2. Timesharing: Each function utilizes a component a fraction of the time. A set of functions is available if there is a configuration in which no component is overloaded.

3. Noncontending: The functions are available if there are sufficient components for each individual function.

Components are contending with respect to certain functions if the components must be dedicated constantly, or at rigidly scheduled times, to supporting the functions (e.g., receivers used to monitor communication channels). Components are timeshared if they are utilized by a function at flexibly scheduled times such that several functions can be interleaved (e.g., data processors). Resources that can be used by any number of functions simultaneously, such as power supplies, are always noncontending.

The classification of components as contending, noncontending, or timesharing also depends on the times during a mission at which each function is required. If functions are not required simultaneously, all components are noncontending.

Within the context of these definitions, dynamic reconfigurability can be represented by a structural model which gives meaningful measures of reliability for a specific mission type. The mission is characterized by the functions required and the simultaneity of these functions.

Structural Reliability Computations

In order to compute MCSP for a given mission scenario with specified function requirements, the mapping from system health (the state of each component) to functional capability is needed. Unfortunately, traditional approaches to evaluating this mapping (Birnbaum & Esary, 1965) are practical only

for systems with a certain modular structure that does not apply to ICNIA architectures. Furthermore, it is desirable to represent this mapping for individual functions rather than complete missions, so that a variety of missions can be constructed from a single data base.

For the ICNIA architectures that have been examined, it is possible to take advantage of the special structure of this mapping to compute MCSP efficiently. The computations, as implemented in the MIssion REliability Model (MIREM), are detailed in Appendix A. The basic approach is to assume a structure corresponding to two levels of reconfigurability or switching. This type of structure is illustrated in Figure 3.

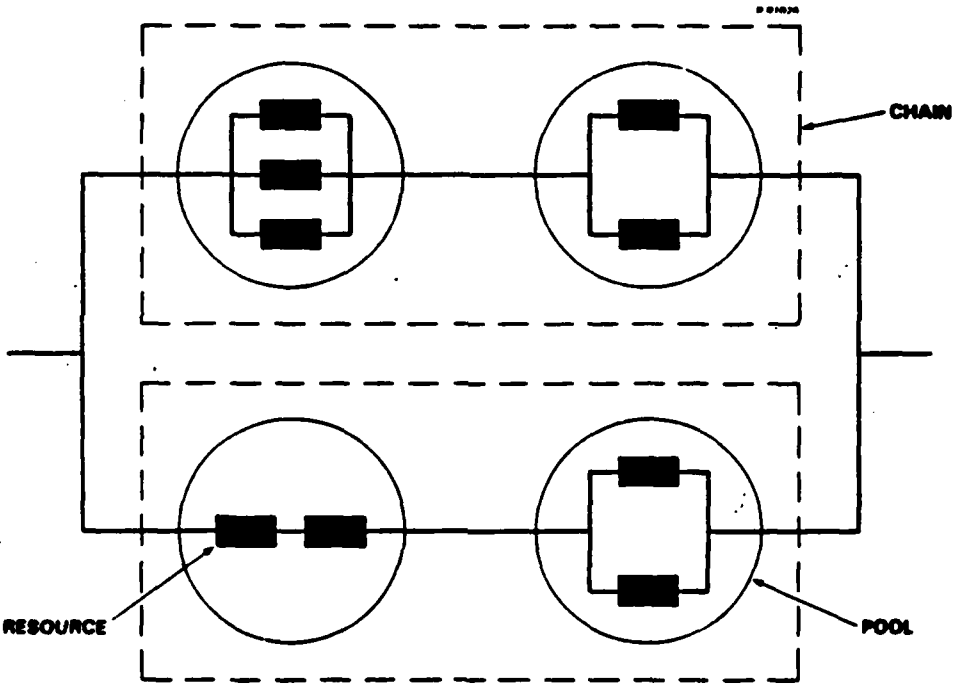


Figure 3. A Two-Level Structure for System Architecture Representation

At the lowest level, pools of interchangeable components are identified. Each function utilizes a certain number of components (or fraction of a component) in a pool. For pools of contending or timeshared components, the total requirement for a pool is the sum of the utilizations of each required function; for noncontending components, the total requirement is the maximum function utilization. If functions are not required simultaneously, all pools are considered noncontending.

MCSP is the product of the probabilities of each pool having sufficient components operating.

The second level of reconfiguration is between parallel chains. A chain is a set of pools that is switched (reconfigured) as a group. In many cases a chain will correspond to a Line Replaceable Unit (LRU), because LRUs have separate power supplies and limited inter-LRU connections. A set of functions is available on parallel chains if there is an allocation of functions to chains such that each chain can support its allocated functions. The approach to evaluating MCSP on parallel chains consists of enumerating all possible allocations of functions to chains (see Appendix A). This approach is computationally feasible, whereas the traditional enumeration of component states is not; the difference being that there are many more components than required functions.

Total system MCSP is the product of the MCSP for each chain/parallel chain set. Other measures of effectiveness can be derived from MCSP. Of particular importance are MTBCF, which is computed by evaluating and numerically integrating MCSP for different mission durations, and failure resiliency, which is defined as the ratio of MTBCF to MTBF.

The reliability analysis methodology is summarized in Figure 4. System structure data are converted to files containing the pool and chain data needed by MIREM. With the additional inputs of failure rates, mission requirements and initial system health, MIREM computes measures of effectiveness plus LRU failure probabilities for use in the logistics analysis.

2.3 MISSION SCENARIOS

A mission can be described by a time sequence of CNI radio system or function requirements. Several factors affect whether the operational requirements of a mission can be met in a given state of system health:

1. The set of critical functions (CF) required for the mission.

2. The combinations of these functions that are required simultaneously.

3. The time slots during which resources must be used to process signals within the interval when a function is required.

4. The time response required when a functional requirement is received compared with the reconfiguration speed of the system.

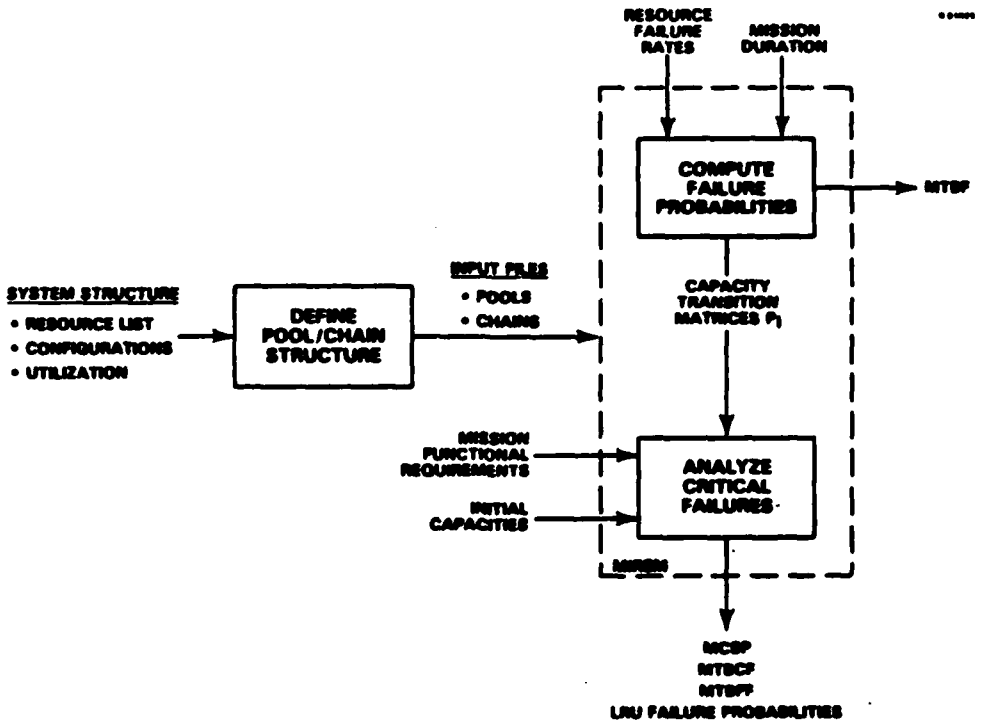


Figure 4. Reliability Analysis Methodology Overview

The last two factors can generally be modeled by appropriate classification of pools as contending or noncontending and by the selection of pool capacity requirements. The first two factors have been dealt with in previous efforts (Long, 1982) by dividing the mission into phases, each of which has distinct functional requirements. In the current analysis, a single set of functions is considered for two cases of simultaneity:

1. All functions are required simultaneously.

2. Each function is required independently.

These two cases bound the actual mission environment. The first (worst) case is used as the baseline for analysis.

The current analysis could be generalized to consider mission phases by including logical or's in the function requirements; e.g., (A and B) or (A and C and D). Although each phase would have a term in the logical expression, it could be

reduced to a few dominant terms. In this manner, varying mission requirements could be analyzed with a static, structural model.

The mission scenarios which have been identified for analysis are listed in Table 1 (ITT Avionics Division, 1983; Long, 1982; TRW Electronic Defense Sector, 1982). These scenarios will be used to analyze ICNIA systems A and B. Interdiction/Offensive Counter Air will be used as a baseline for analysis.

TABLE 1. MISSION REQUIREMENTS

SCENARIO	CRITICAL FUNCTIONS
Interdiction/Offensive Counter Air	UHF, JTIDS, GPS, IFFT
Close Air Support	HF, VHF, UHF, SEEK TALK, SINCGARS, JTIDS, IFFT
Defensive Counter Air	UHF, VHF, SEEK TALK, IFFI, IFFT
"Generic"	ILS, UHF, A/J VOICE, GPS, TACAN, IFFT
"Most Stringent" Simultaneous Requirements	HF, VHF, VHF (GUARD), UHF, UHF (GUARD), JTIDS, IFFT, IFFI

The functions listed for these scenarios are those necessary for survival/safety and mission success. Alternative requirements keyed only to survival could also be used to assess the impact of the system on aircraft losses.

2.4 APPLICATION TO AN EXAMPLE ARCHITECTURE

A simple example of a fault-tolerant architecture is discussed here to illustrate MIREM capabilities. The structure is shown in Figure 5. Low-band functions require one of the two low-band receive front ends; hence, they form the pool B. Low-band functions also require preprocessors in the set C or D. The UHF and SINCGARS functions, for example, require a total of two of the five preprocessors. Preprocessors in set C can be used only if certain other components in the larger group II are operating. Similarly, the set D depends on components in group III.

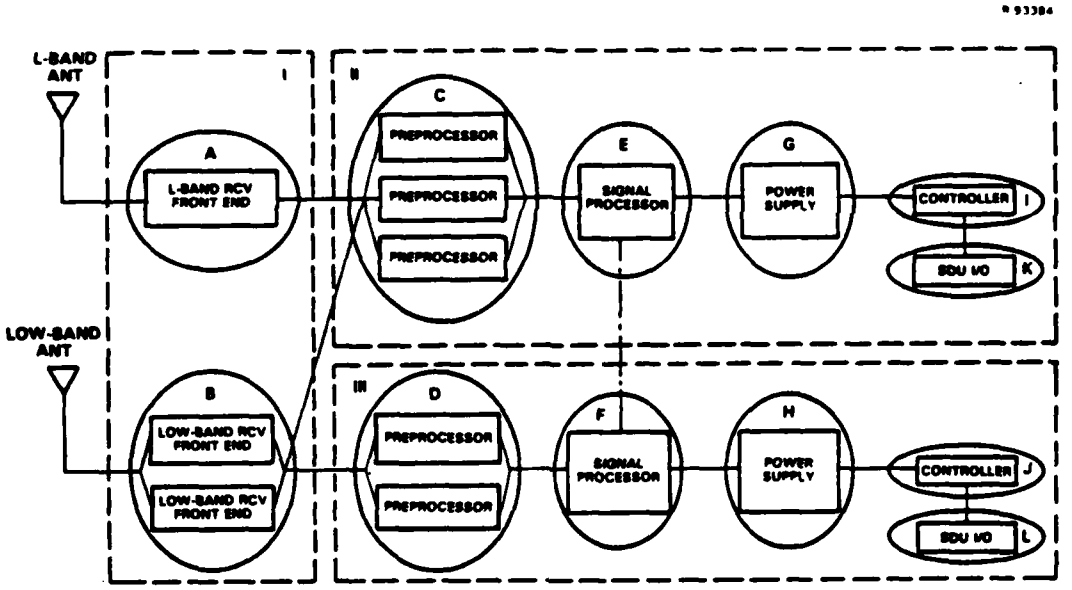


Figure 5. A Simplified Fault-Tolerant Architecture (CNI Receive Functions)

This two-level structure is typical of those found in ICNIA designs (ITT Avionics Division, 1982; TRW Electronics Systems Group, 1982). MIREM classifies C and D as pools and II and III as parallel chains. Pools A and B can be considered a series chain. Connection between these parallel chains is through the series chain (I). Pool boundaries are defined by the first level of reconfigurability; parallel chains are defined by the second.

The input data required by MIREM for each pool are shown in Table 2. The table indicates that GPS, for example, requires one L-band receiver front end, three preprocessors, 80% of the capacity of a signal processor, one power supply, and one controller. The manner in which functions interact is given under pool type. Timesharing and contending pools are listed as type C; noncontending pools are listed as type N. Pool type dictates how utilizations are combined across functions. For example, the combination of UHF and SINCGARS requires two preprocessors but only one front end. Table 2 also shows the number of components, or capacity, and the component failure rate in each pool. Components within a pool are assumed to be identical.

TABLE 2. MIREM INPUT DATA

POOL	CHAIN	DESCRIPTION	UTILIZATION (NO. OF COMPONENTS)			CAPACITY (NO. OF COMPONENTS)	COMPONENT FAILURES PER 10^6 HRS	POOL TYPE
			GPS	UHF	SINC GARS			
A	I	L-Band Receiver Front End	1	-	-	1	100	N
B	I	Low-Band Receiver Front End	-	1	1	2	200	N
C D	II III	Preprocessor	3	1	1	3 2	600	C
E F	II III	Signal Processor	0.8	0.1	0.4	1 1	200	S
G H	II III	Power Supply	1	1	1	1 1	40	F
I J	II III	Secure Data Unit I/O	-	-	1	1 1	40	N
K L	II III	Controller	1	1	1 1	1	200	N

Two other pool types are also considered. A set of pools, one in each parallel chain, is shared (type S) if the pool in one chain can be used by functions allocated to another chain. Chain-fail pools (type F) are those which, upon failure, prevent any of the pools in the chain from being utilized. In this example the signal processors are connected by a data bus, so that they are shared by chains II and III. Loss of a power supply prevents any of the pools in that chain from being used.

Many reconfigurable designs can be modeled by the pool/chain concept. However, care must be taken to represent failure modes properly, particularly for switching and control resources. The interpretation of backup components as a pool (i.e., components that are in parallel) assumes that the backup will take over when a component fails. This is accomplished in ICNIA through Built-In Test (BIT) equipment, RF switching and flexible processor interconnections, all coordinated by a control processor. Failures in these components can be modeled

as an additional pool. The fact that not all failures can be detected by BIT, however, is not modeled.

2.5 RESULTS

Reliability results are presented in this section for the example introduced in Section 2.4. Table 3 shows MTBFF and failure resiliency for each function considered individually and independent of any mission. UHF and SINCGARS both have very good reliability. This is explained by the fact that no single component failure can make these functions unavailable. GPS, being restricted to chain II, has several critical components; thus, it exhibits a low MTBFF. The fault tolerance is best seen in the failure resiliency, which roughly corresponds to the number of failures that occur before a function failure.

TABLE 3. FUNCTION RELIABILITY

FUNCTION	MTBFF (hrs)	FAILURE[a] RESILIENCY
GPS	467	2.08
UHF	2126	9.48
SINCGARS	2042	9.11

[a]FAILURE RESILIENCY = MTBFF/MTBF;
MTBF = 224 hours

System reliability in a mission context, expressed by MTBCF, is considerably lower. Two mission scenarios are considered in Table 4, one requiring all three functions simultaneously, and one requiring only UHF and SINCGARS. Each mission is 3.0 hours in length. For Scenario 1, fault tolerance only extends the MTBF of 224 hours to a MTBCF of 249 hours, whereas for Scenario 2 the increase is dramatic. Hence, failure resiliency is very dependent on the mission scenario. Only 2.5% of the critical failures for Scenario 1 occur in chain I, with the rest occurring in the parallel chains II and III. If the functions are not required simultaneously, the MTBCF for Scenario 1 increases to 389 hours, with a failure resiliency of 1.74.

A major advantage of MIREM as a design tool is its ability to evaluate the impact of proposed design changes. Table 5 shows the sensitivity of MCSP to redundancy levels using the architecture discussed above as the baseline. Adding a second

TABLE 4. MISSION RELIABILITY

MISSION SCENARIO	MCSP (3-hour mission)	MTBCF (hours)	FAILURE[a] RESILIENCY
1 GPS, UHF AND SINCGARS required simultaneously	0.9880	249	1.11
2 UHF and SINCGARS required simultaneously	0.999996	1379	6.15

[a]Failure Resiliency = MTBCF/MTBF; MTBF = 224 hours

TABLE 5. SENSITIVITY OF MCSP TO REDUNDANCY LEVELS FOR SCENARIO 1

REDUNDANCY OPTION		NEW[a] MCSP	% REDUCTION IN MISSION FAILURES
BASELINE ARCHITECTURE	PROPOSED MODIFICATION		
2 Signal Processors	3 Signal Processors (2 in chain II)	0.9892	10
5 Preprocessors (3 in chain II, 2 in chain III)	6 Preprocessors (4 in chain II)	0.9970	75
	6 Preprocessors (3 in chain III)	0.9916	30
1 L-band Receiver	2 L-band Receivers	0.9883	3

[a]Baseline MCSP = 0.9880

signal processor to chain II, for example, reduces the probability of mission failure (1 - MCSP) by 10%. Additional preprocessors improve reliability dramatically because of their high failure rate and because all five are required for this scenario. Other mission scenarios would show different sensitivities.

Table 6 gives the sensitivity of MCSP to the degree of reconfigurability of the system. The primary restriction

TABLE 6. SENSITIVITY OF MCSP TO RECONFIGURABILITY FOR SCENARIO 1

RECONFIGURABILITY OPTION		NEW[a] MCSP	% REDUCTION IN MISSION FAILURES
BASELINE ARCHITECTURE	PROPOSED MODIFICATION		
Share signal processors between chains	Separate signal processor for each chain	0.9880	0
GPS must use chain II	GPS can use chain II or III (add 3rd preprocessors to chain III)	0.9970	75

[a]Baseline MCSP = 0.9880

to reconfigurability is that GPS must use chain II. Adding the appropriate switching and a third preprocessor to chain III, so that GPS can use either chain, has a large reliability payoff. On the other hand, reducing reconfigurability by eliminating the data bus between the signal processors does not significantly degrade reliability.

2.6 CONCLUSIONS

A structural reliability model has been presented which can represent the features of integration and fault tolerance in complex systems. The model focuses on dynamic reconfigurability and does not consider the issues of BIT coverage, software inadequacies or failures and cabling failures. Several conclusions can be drawn from the reliability example that was analyzed:

1. Single components that can cause system failures (critical failures), if they exist, are the single most important factor in Mission Completion Success Probability (MCSP) and a major factor in Mean Time Between Critical Failure (MTBCF).

2. A second level of redundancy (at the LRU level) improves reliability only if all critical functions are supported on both of the LRUs.

3. The determination of which functions are critical for a mission and whether they are required simultaneously can drastically affect MCSP.

4. Reconfigurability (e.g., inter-LRU connections) between components that are already redundant does not necessarily enhance reliability.

Efficient computation of reliability measures is possible with this model. Furthermore, the model has the advantage of not requiring highly detailed design inputs.

3. LOGISTICS SUPPORT ANALYSIS

The potential advantages of integrated, fault-tolerant CNI avionics from the logistics support perspective are readily apparent. Some of the larger impacts are expected in:

1. Adoption of two-level maintenance.

2. Faster turnaround at the flight-line level.

3. Greater number of sorties between corrective maintenance actions.

These changes offer payoffs in both Life-Cycle Cost (LCC) and operational readiness. Integrated, fault-tolerant architectures exhibit the potential for increasing readiness levels above those of existing discrete systems at equal or lower LCC. This feature has added meaning with the emerging requirements of sustained combat capability under a bare base (i.e., no repair capability) environment with limited spares budgets. To achieve this objective, however, emphasis needs to be placed not only on hardware/software reliability and system architecture, but also on BIT, modularity, and support strategies.

This section presents a method of evaluating the operational readiness payoff of integrated, fault-tolerant avionics. The method can evaluate alternative repair strategies and is consistent with the limited data available during the early stages of system design. An overview of the methodology is shown in Figure 6. The applicability of previous work is discussed in Section 3.1. The logistics support scenario to be modeled is described in Section 3.2. Section 3.3 presents the modeling methodology. Model inputs for an example architecture are defined in Section 3.4, and results are given in Section 3.5. Some conclusions are drawn in Section 3.6.

3.1 FRONT-END STUDY FINDINGS

Several logistics analysis techniques were assessed as to applicability to analysis of integrated, fault-tolerant architectures using both conventional and innovative maintenance concepts. In particular, eight models were evaluated in some depth. Brief discussions of these eight models, their principal features and applicability to the ICNIA analysis requirements, are provided in the following paragraphs:

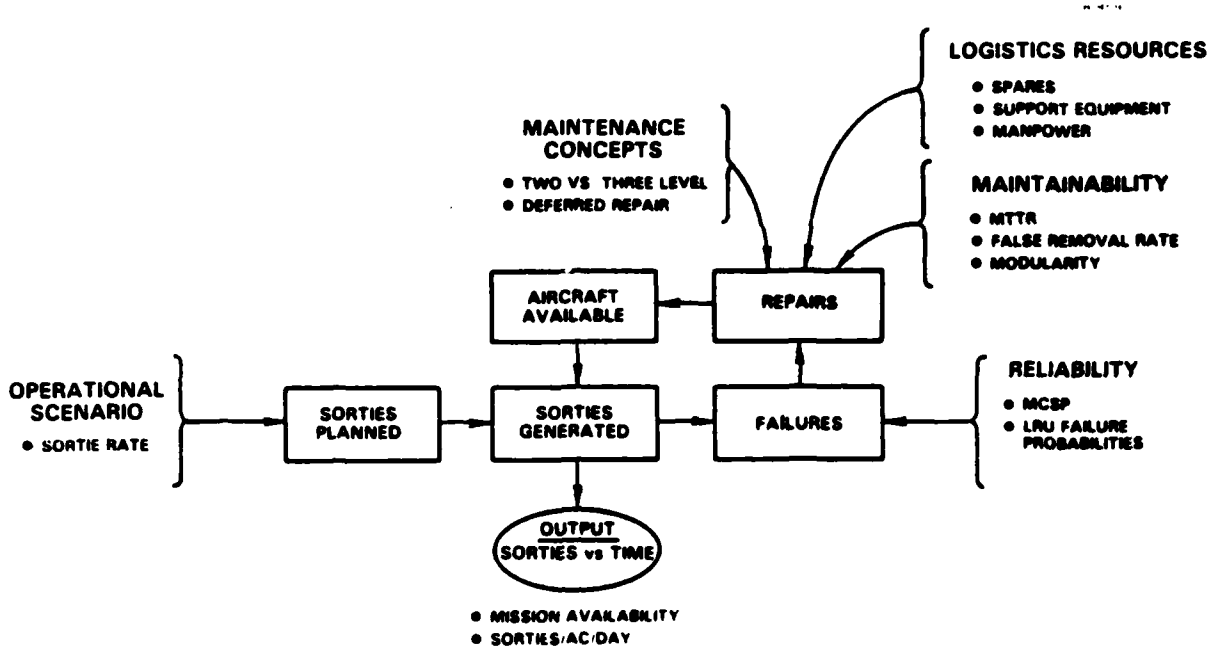


Figure 6. Readiness Methodology Overview

1. ALPOS - The Avionics Laboratory Predictive Operations and Support model (Air Force Wright Aeronautical Laboratories, 1978a) is a parametric operations and support cost model based on historical data. It was derived using multiple regression techniques. It does not capture the integrated fault-tolerant characteristics of ICNIA nor can it model the innovative maintenance concepts applicable to ICNIA.

2. LCOM - The Logistics Composite Model (Air Force Management Engineering Agency, 1982) is a discrete event simulation model based on Monte Carlo techniques which captures in very fine detail the logistics structure of the maintenance scenario and the hardware structure (typically of a major weapon system). It does not lend itself to early design work, where the data are limited, although it could be streamlined with some effort.

3. ORLA - Optimum Repair Level Analysis (Air Force Logistics Center, 1971) is an expected value model for determining optimum (least-cost) policies for repairing/discarding LRUs and/or Shop Replaceable Units (SRU's) at the intermediate or depot level. Determinations are based on spares, support equipment, and other support costs. The technique does not capture

the fault-tolerant characteristics of ICNIA since it is driven largely by MTBF and traditional support factors.

4. LSC - The Logistics Support Cost (Air Force Logistics Center, 1976) model consists of 10 equations which address support costs. The model does not explicitly capture innovative maintenance concepts applicable to ICNIA.

5. LCC2 - The Life-Cycle Cost Model Version 2 (Gates et al., 1976) is based on LSC equations. Although it provides flexibility as to maintenance concept modeling, it does not capture readiness factors and is not applicable to the early design phase.

6. MOD-METRIC - The MOD-METRIC model (Air Force Logistics, 1975) is a set of sparing algorithms that treats the multi-item, multi-echelon, and multi-indenture inventory problem in an optimization framework. The model is limited to spares and does not capture the relevant logistics factors impacting system readiness.

7. Dyna-METRIC - The Dyna-METRIC model (Hillestad, 1982) incorporates dynamic queueing equations that extend the MOD-METRIC capabilities to transient behavior under time-varying operations. Like MOD-METRIC, the model addresses optimal sparing and spares availability, but does not capture other logistics factors impacting system readiness.

8. SOAR - The Simulation of Operational Availability/ Readiness model (The Analytic Sciences Corporation, 1981) is a continuous-flow simulation model based on system dynamics techniques that capture the reliability and maintainability parameters of a system with the dynamics of logistics support at a single base in order to evaluate mission availability at the squadron or wing level. It is applicable to early system design, and its network flow framework can be extended to capture innovative maintenance concepts for ICNIA.

The main conclusion drawn from this front-end study is that no single technique captures all of the ICNIA analysis requirements. These models were developed with specific objectives in mind and address some of the ICNIA analysis needs but not all. The SOAR model appeared to be the technique closest to the ICNIA logistics support analysis requirements. This technique was selected for analysis of operational readiness with some modification for capturing innovative maintenance concepts.

3.2 LOGISTICS SUPPORT SCENARIO

The logistics support scenario being modeled incorporates the dynamics of aircraft sortie and maintenance operations at a single site (e.g., air base) from the perspective of the equipment under study. Weapon system sortie requirements, expressed in terms of desired number of sorties per day, are generated over a given time period. The weapon system is viewed in terms of the equipment under study and the rest of the aircraft with their associated reliability and maintainability parameters and support resources. Maintenance operations and logistics support at the organizational- intermediate- and depot-level maintenance sites are represented. Figure 7 presents an overview of the logistics support scenario for two- and three-level maintenance used in this analysis. This framework is used to

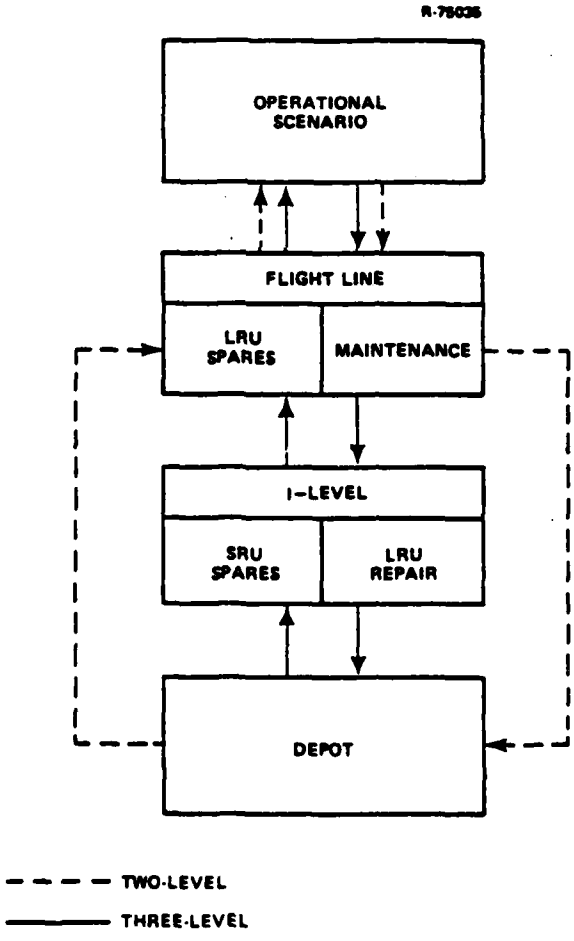


Figure 7. Logistics Support Scenario

explore maintenance and support issues associated with fault-tolerant systems:

1. Repair policies which include immediate versus deferred maintenance.

2. Two versus three levels of maintenance.

3. Conventional and advanced support scenarios.

Immediate and Deferred Repair Policies

The flight-line, or organizational-level, maintenance activities consist primarily of removal and replacement (R/R) of LRUs. For fault-tolerant system applications, R/R actions may take place when the first failure occurs or may be deferred until system critical failures occur (i.e., loss of a critical function). These two repair policies will be referred to as immediate and deferred repair, respectively. Deferred repair is an innovative maintenance concept that would require significant institutional changes to implement. The procedure would rely heavily on BIT equipment to determine system health and an intelligent system to make the repair/defer decision based on system health and the type of mission to be flown. Compromise maintenance policies, which would defer repair of some noncritical failures and repair others, could be developed based on the increased risk of additional failures causing a critical failure in a degraded system. For the mission scenarios and system architectures considered to date, however, the increase in risk is generally small.

Two Versus Three Levels of Maintenance

After flight-line removal, faulty LRUs then enter the intermediate, or I-level, maintenance shop under a three-level maintenance policy where they are repaired by R/R of the faulty SRUs. If a two-level maintenance policy is considered, then the LRUs are sent directly to the depot for repair. The depot activities consist of repair of the faulty LRUs or SRUs, depending on the maintenance concept.

The maintenance resources available at each level depend on the type of base at which operations are being modeled. Two scenarios have been identified. These scenarios will be used in the analysis of the ICNIA systems A and B in (Veatch, 1984a, 1984b), respectively.

Conventional and Advanced Support Scenario

The conventional support scenario is representative of a fixed-site main operating base. The following maintenance resources are available for a squadron of 24 aircraft and systems:

1. Initial spares levels set at one spare for each LRU.

2. I-level shop for LRU repair, including one Automatic Test Equipment (ATE) work station available 12 hours each day and sufficient manpower.

3. Depot replenishment for SRUs (three-level maintenance) or LRUs (two-level maintenance).

A tactical fighter sortie schedule and an immediate repair policy are used as a baseline for this scenario. This 60-day schedule consists of a 7-day surge or wartime sortie rate, a sustaining rate for days 8 to 30, and a peacetime sortie rate of 0.7 sortie/aircraft/day for the last 30 days. Immediate repair is a reasonable baseline assumption for this scenario, since maintenance resources are not unduly stressed.

The advanced support scenario represents a dispersed operating location, known as a bare base or austere site. The following maintenance resources are available for a squadron of 24 aircraft and systems:

1. Initial spares levels set at one spare for each LRU.

2. An Industrial Maintenance Facility, which possesses depot repair capabilities, co-located with a Main Operating Base ("Queen Bee" base).

3. Depot SRU/LRU replenishment available only after the initial 7-day surge.

A maximum sortie schedule is used as a baseline for this scenario, putting maximum stress on the maintenance resources. Under this schedule, each ICNIA-equipped aircraft is launched as soon as it becomes available after rearm/refuel or repair. Deferred repair has the potential for sustaining more sorties in this limited-resource scenario and is used as a baseline.

3.3 METHODOLOGY

Perhaps the most operationally significant dimension of logistics support, and one that is meaningful early in the

development cycle, is operational readiness. For fighter aircraft, readiness can be viewed as the ability to satisfy an immediate or short-term requirement for sorties. To evaluate the operational readiness payoffs of integrated, fault-tolerant CNI systems, a logistics model that captures these issues and is consistent with existing data during the early stages of system design is needed. The Analytic Sciences Corporation (TASC) has developed the Simulation of Operational Availability/Readiness (SOAR™)[1] model to study readiness issues for advanced avionics systems (Calvo, 1982). SOAR has been applied to avionics systems such as the AN/ALQ-131, Airborne Self-Protection Jammer (ASPJ) and Low-Altitude Navigation and Targeting, Infrared for Night (LANTIRN). It has now been extended to accommodate deferred repair policies applicable to integrated, fault-tolerant avionics.

SOAR analyzes the dynamics of aircraft sorties and maintenance operations at a single site that are described in the logistic scenarios of Section 3.2. A system of linear differential equations is established for the expected flow rates into and out of major system states. Aircraft, systems, LRUs, and SRUs move through ready, failed, and under repair states. These equations are solved by Euler's single-step method, starting from specified initial conditions. Different system states and flow diagrams are used for the cases of immediate and deferred repair.

Immediate Repair Model

The basic SOAR flow diagram for immediate repair is shown in Figure 8. Sorties are generated to meet the planned sortie rate or until the available aircraft and systems are exhausted. The expected number of LRUs returning faulty are routed to a repair queue, are repaired, and finally are reissued. Additional repair states and delays for LRUs and SRUs that depend on the level of repair are not shown.

Deferred Repair Model

The SOAR flow diagram for deferred repair is shown in Figure 9. Unlike immediate repair, deferral of repair until a critical failure occurs results in a changing mission reliability. For highly fault-tolerant systems, reliability decreases as a system continues to be flown without repair. Hence, the age or operating time since repair of each system must be tracked by the model. Six categories of system age are counted as separate states in the model, with varying Mission Completion Success Probability (MCSP). Age also impacts

[1] SOAR is a trademark of The Analytic Sciences Corporation.

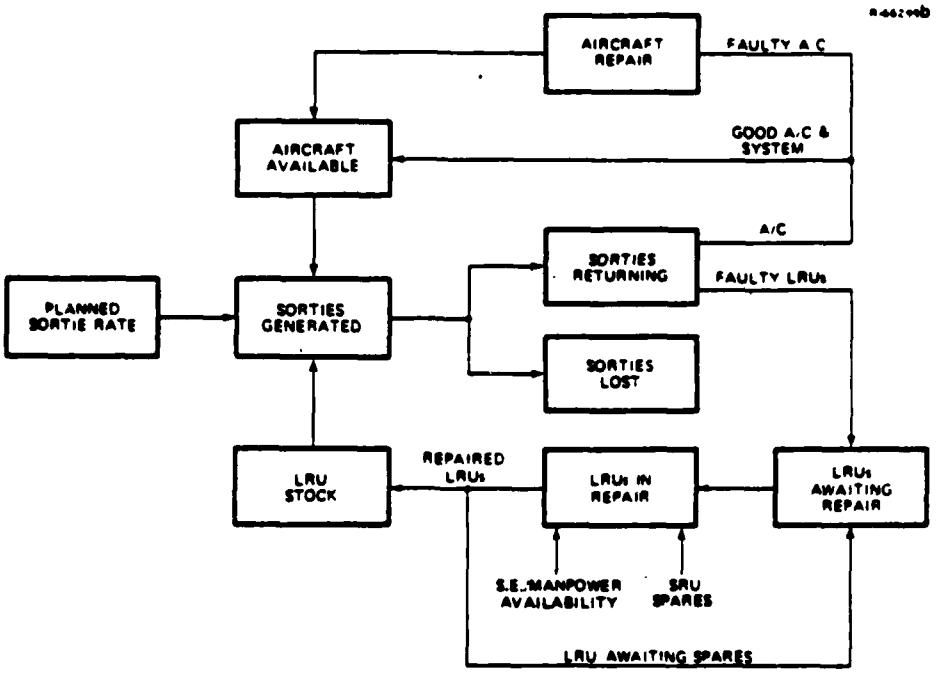


Figure 8. SOAR Avionics Model (Immediate Repair)

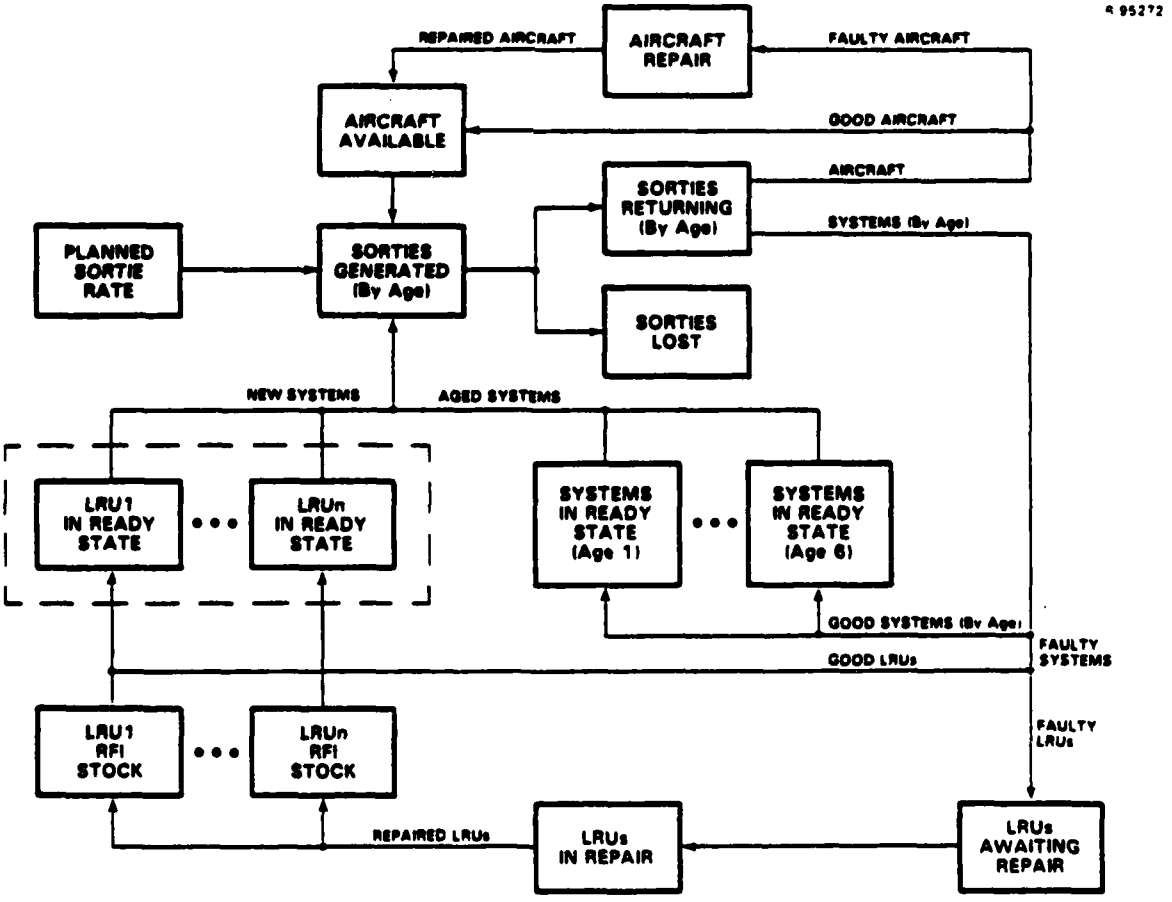


Figure 9. SOAR Deferred Repair Avionics Model

which LRUs are pulled from systems returning faulty. On the average, more LRUs will be pulled from "old" systems.

Once the faulty LRUs are pulled, the remaining LRUs return to "new" status. When they are combined with other Ready For Issue (RFI) stock, a new (age zero) system reenters the cycle.

The remainder of the model is equivalent to the immediate repair model.

Measures of Effectiveness

The time sequence of any state variable or rate in the model can be obtained as an output from SOAR. Two primary measures of operational readiness have been identified as useful outputs:

1. Mission Availability: The ratio of the actual number of sorties generated to the desired number.

2. Sortie Generation Rate: The number of sorties generated per day per aircraft. The Primary Aircraft Authorization (PAA) is used as the number of aircraft; less aircraft may be available because of attrition. This measure is of interest when a maximum sortie generation schedule is being used.

3.4 MODEL INPUTS FOR AN EXAMPLE ARCHITECTURE

The inputs required by SOAR are listed in Tables 7 and 8. The values listed in these tables are for the baseline case reported in Section 3.5. Parameters that differ from these values for the conventional and advanced deployment scenarios are defined in Section 3.2. The architecture-dependent inputs are for the example architecture of Section 2.4. A three-LRU packaging is assumed, with one LRU for each chain as depicted in Figure 5.

The reliability inputs in Table 8 were generated by MIREM using the equations derived in Appendix A. The architecture of Section 2.4 and the mission requirements of Scenario 2 were used. These inputs pertain to deferred repair; conventional MTBF reliability measures are used as inputs for immediate repair. Each age interval in Table 8 corresponds to 100 hours of operation without repair. For new systems, an average of just over one LRU contains a failure when a repair action occurs, whereas for systems of age 6, two LRUs contain failures. In addition,

TABLE 7. SOAR MODEL INPUTS

DESCRIPTION		NAME	VALUE
Mission Related			
Desired Sortie Rate (sorties/aircraft/day)	Surge	SX	a
	Intermediate	IX	a
	Peacetime	PX	0.7
Interval Between Sorties (hours)		SINTVL	1
Attrition Rate (fraction of sorties)	Surge	WARF	0
	Peacetime	PARF	0
Start of Surge Period (hours)		STWAR	0
End of Surge Period (hours)		ENDWAR	168
Start of Peacetime Period (hours)		STPEAC	720
Scenario Length (hours)		LENGTH	1440
Mission Length (hours)		ML	3
Aircraft Related			
Initial Number of Aircraft		INAC	24
Aircraft Returning Faulty (fraction)		DF	0
Turnaround Time for Faulty Aircraft (hours)		ATAT	9
Rearm/Refuel Time for Good Aircraft (hours)		FLDEL	2†
System Related			
Initial Number of (Age 1) Systems		PIRS1	24
LRU Turnaround Time at the I-Level Shop (hours)		MTAT	4
LRU False Removal Rate (fraction of LRU failures)		UFP	0.1
Support System Related			
I-Level Support Equipment and Manpower Availability (fraction of total time)		SAVAIL	0.5
Number of I-Level Testers		NSE	1
Number of Ready For Issue (RFI) Spares	LRU 1	RFI1	1
	LRU 2	RFI2	1
	LRU 3	RFI3	1
Base to Depot Shipping Time (hours)		BDST	360
Depot to Base Shipping Time (hours)		BRST	240

[a]Value is classified.

†A 1-hour rearm/refuel time applies to the conventional and advanced deployment scenarios defined in Section 3.2.

TABLE 8. SOAR RELIABILITY INPUTS (DEFERRED REPAIR)

LRU \ AGE[a]	1	2	3	4	5	6
PROBABILITY OF CRITICAL FAILURE DURING MISSION						
-	0.0001	0.0004	0.0007	0.0010	0.0013	0.0016
PROBABILITY THAT LRU IS FAULTY AT REPAIR						
1	0.11	0.15	0.19	0.22	0.26	0.29
2	0.92	0.94	0.95	0.96	0.97	0.98
3	0.26	0.40	0.50	0.57	0.63	0.68
EXPECTED NUMBER OF FAULTY LRUs	1.30	1.49	1.64	1.76	1.86	1.95

[a]Age of a system refers to the number of missions flown or hours of operation without undergoing repair. Six age ranges are established, each representing 100 hours or 33 missions.

the distribution of faulty LRUs shifts toward those with fault tolerance (LRUs 2 and 3) as time since repair increases. The mission failure probability also increases with age. This increasing "failure rate" is due to the high fault tolerance of the architecture for this mission.

3.5 RESULTS

Readiness results are presented in this section for the architecture introduced in Section 2.4 and the logistics parameters listed in Section 3.4. A maximum sortie schedule and a high aircraft mission capable rate are used for this analysis to stress the maintenance resources. Figure 10 shows the sortie generation rate as a function of time for three-level and two-level maintenance concepts. With three-level maintenance, the spares and intermediate-level shop throughput are sufficient to maintain maximum readiness. Thus, the system under study has no impact on aircraft availability. The maximum rate of 4.8 sorties/aircraft/day is determined by the 5-hour cycle of mission length plus rearm/refuel time. Under two-level maintenance, readiness decreases as faulty LRUs are tied up in the longer repair pipeline and spares are exhausted. Equilibrium

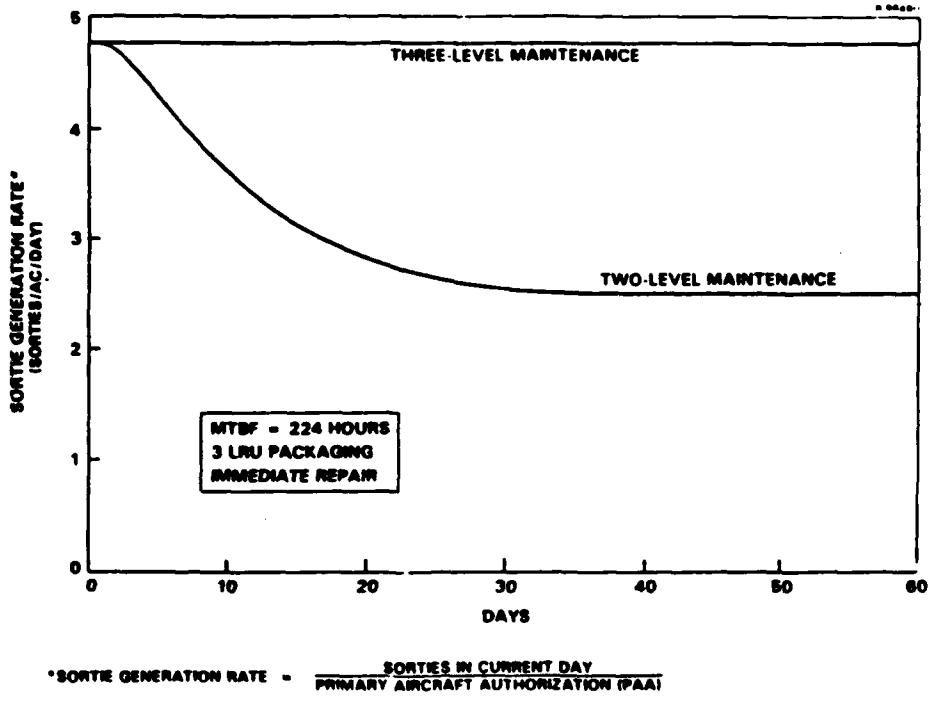
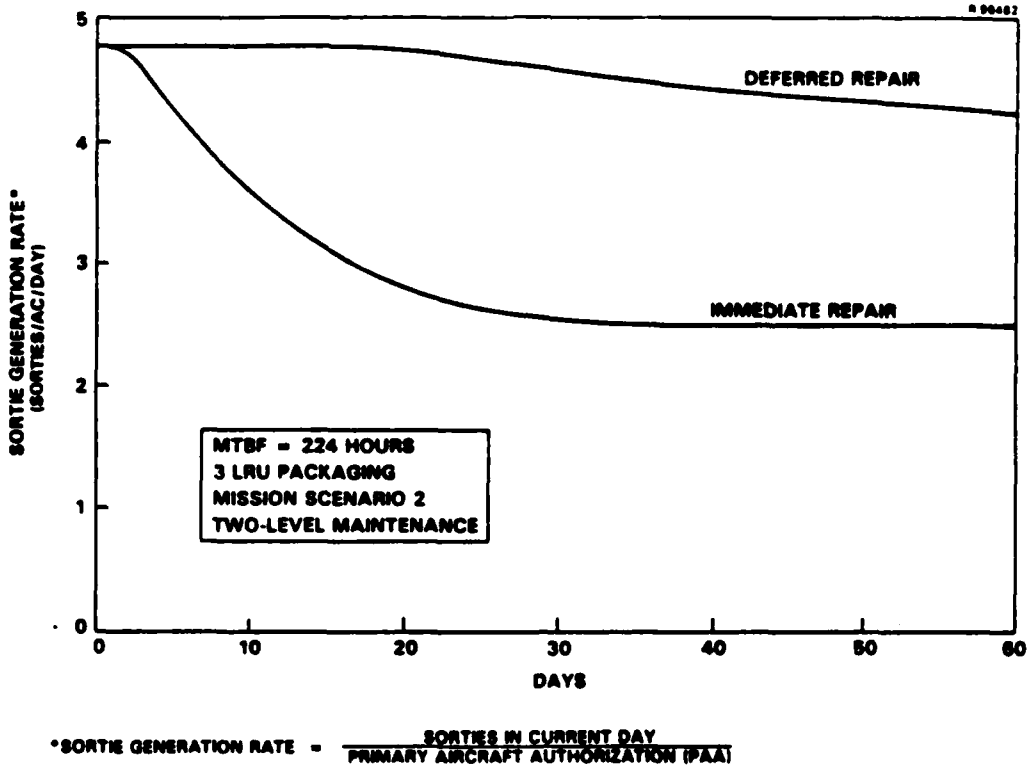


Figure 10. Maximum Sortie Generation by Level of Repair

is reached at 2.3 sorties/aircraft/day when the LRU failures match the LRUs returning from depot.

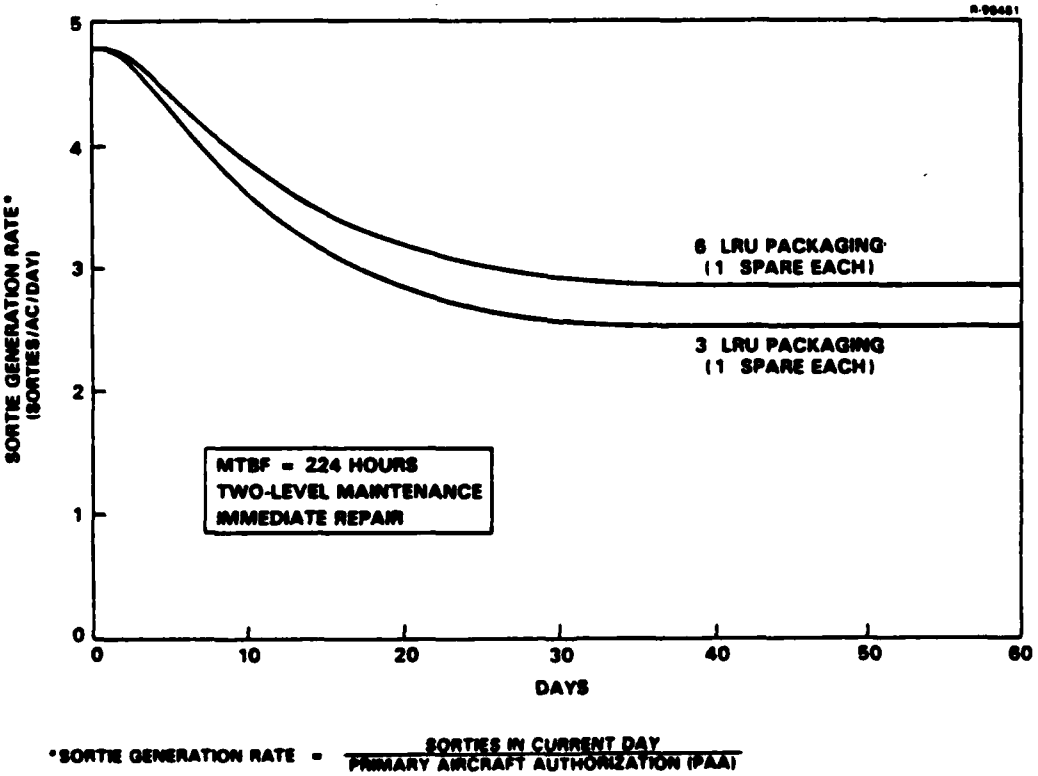
Sortie generation rate can be increased under the two-level concept by providing more spares at the organizational level or by adopting a deferred repair policy. In Figure 11, immediate and deferred repair policies are compared under two-level maintenance. The deferred repair policy can sustain many more sorties than the immediate repair policy and nearly matches the sorties achieved under three-level maintenance. Even when the systems age and repair actions start to build up, the high MTBCF places less demand on the LRU repair pipeline and a higher sortie rate is maintained.

A six-LRU packaging arrangement is compared with the baseline of three LRUs in Figure 12. Immediate repair is assumed so that only the traditional reliability inputs are required for the six LRUs. The six-LRU configuration (increased modularity) provides a higher system availability at the base and thus a higher sortie rate, since a smaller piece of the system is tied up in the repair pipeline for each failure.



*SORTIE GENERATION RATE = $\frac{\text{SORTIES IN CURRENT DAY}}{\text{PRIMARY AIRCRAFT AUTHORIZATION (PAA)}}$

Figure 11. Maximum Sortie Generation by Repair Policy



*SORTIE GENERATION RATE = $\frac{\text{SORTIES IN CURRENT DAY}}{\text{PRIMARY AIRCRAFT AUTHORIZATION (PAA)}}$

Figure 12. Maximum Sortie Generation by Modularity

The readiness benefits of three-level maintenance and increased modularity must be traded off against the associated increased costs. The readiness benefit of deferred maintenance, on the other hand, is really only traded against the slight increase in mission failure probability (assuming that BIT and resource management features are already included for reasons of fault tolerance).

3.6 CONCLUSIONS

A technique has been presented for assessing the readiness impact of integrated, fault-tolerant systems. The readiness impact of two- versus three-level maintenance, modularity and deferred repair have been illustrated. Two conclusions can be drawn from the supportability example which was analyzed:

1. Deferral of repair until a critical failure occurs allows a high sortie rate to be sustained for a longer period without repair. The payoff is substantial for highly fault-tolerant systems, particularly under a two-level maintenance policy. However, some penalty is paid in MCSP for flying systems that contain failed components (less redundancy).

2. High reliability, deferred repair policies and increased modularity all provide impetus to use two-level maintenance, eliminating expensive intermediate-level test equipment.

This analysis technique is applicable to ICNIA architectures during the early stages of design. Specific sortie rate capabilities for ICNIA will depend on the system's reliability parameters.

4. SURVIVABILITY ANALYSIS

The integration and resource-sharing characteristics of ICNIA could lead to the conjecture that ICNIA is more vulnerable to projectile threats than a suite of discrete CNI avionics. The argument would be that although a single discrete subsystem (one or two LRUs) might be lost to such a threat, substantial loss of CNI capability would seem less likely than for a more centrally configured ICNIA system. On the other hand, volume reduction, through system integration, makes ICNIA a smaller target. The system vulnerability question also includes consideration of which LRUs ICNIA can afford to lose and yet still retain a specified capability.

One objective of the ICNIA study was to address these system Survivability/Vulnerability (S/V) issues with respect to projectile threats. The primary focus involved assessing whether ICNIA was more or less vulnerable than were the discrete systems. In view of the variety of threats and the details of specific system protection possibilities, a top-level analysis effort aimed at first-order-type results was considered appropriate. A long term-concern was the S/V evaluation of ICNIA system alternatives.

The plan for the S/V study included a front-end survey for data and analyses applicable to these objectives; identification and implementation of relevant analytic techniques; a decision point as to whether or not to proceed with ICNIA-specific systems evaluations; and, if possible, this eventual evaluation.

4.1 SURVEY RESULTS

The front-end study was designed to obtain S/V techniques and a CNI baseline vulnerability analysis for typical tactical aircraft.

A variety of Joint Technical Coordinating Group/ Aircraft Survivability (JTCG/AS) documents (Belote & Severence, 1977; Joint Tactical Coordinating Group/Munitions Effectiveness, 1975, 1977; Mowrer, Walther, Mayerhofer, & Schumacher, 1977) were reviewed. These sources indicated that a typical aircraft or system S/V methodology consists of computer analysis using the FASTGEN and COVART programs to generate both projectile or fragment shotlines (FASTGEN) and the associated penetration history (COVART) of threat impacts. The output of this analysis is in terms of vulnerable area, a concept defined as an aircraft or system kill probability integrated over projected area -- those

portions of the aircraft or system which are perpendicular to the threat shotline.

Air Force Aeronautical Systems Division (ASD) personnel, active in the S/V community, were queried with regard to a CNI baseline vulnerability assessment for tactical aircraft. It was learned that since CNI contributes typically less than 5 percent to total tactical aircraft vulnerability, analyses of this system are not performed.

The survey concluded that a possible avenue to approach an S/V evaluation of the projectile or fragment threat, in lieu of the data and computer time-intensive FASTGEN-COVART analysis, was to extract the shotline and penetration methodology into a set of smaller programs. A comparison of ICNIA to a discrete system baseline would then be generated, using the avionics configuration for a tactical aircraft.

4.2 METHODOLOGY

CNI system S/V to a projectile or fragment threat was pursued through shotline and penetration analysis. The objective was to assess system vulnerability as a function of threat penetration (dependent on weight, velocity, threat-type and threat-density parameters) and system configuration including LRU size, placement and redundancy. The methodology envisioned is shown in Figure 13.

In addition to physical characteristics of the LRUs and aircraft structures, the attack geometry and threat characteristics are needed to perform the S/V analysis. A prototype scenario was defined as an attack on the aircraft from a forward aspect off the avionics bay. These parameters, with the baseline values from Belote & Severence, 1977, are defined in Table 9.

The number of LRUs and structures penetrated by the threat is determined using the following penetration equations. A target is penetrated if the threat possesses at least the ballistic limit velocity (Mowrer, Walther, Mayerhofer, & Schumacher, 1977):

$$V_{bl} = C_1 \left(\frac{\rho_f T A_p}{W}\right)^{C_2} (\sec w)^{C_3} \left(\frac{\rho_f T A_p}{W_o}\right)^{C_4} \qquad (1)$$

Residual velocity upon exiting a target is computed as:

$$V_r = (V^2 - V_{bl})^{1/2} \Big/ \left(1 + \frac{\rho T A_p}{W \cos w}\right) \qquad (2)$$

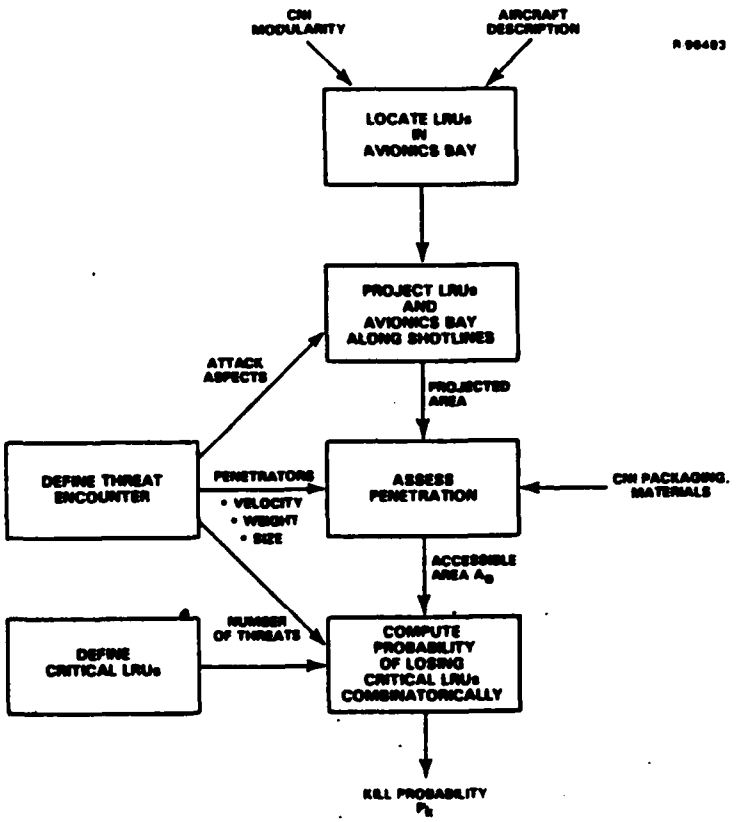


Figure 13. Overview of S/V Methodology

where V is the relative velocity of the penetrator before impacting the target:

$$V = V_{a/c} \cos\theta \cos\phi + [V_p^2 - V_{a/c}^2(1 - \cos^2\theta \cos^2\phi)]^{1/2} \quad (3)$$

Metric units are used for the computations. Alternative units which may be more familiar to the reader are also listed in Table 9. This penetration assessment can be combined with the other procedures shown in Figure 13 to determine kill probability.

4.3 CONCLUSIONS

Initial projectile/fragment attack aspect and velocity lead to a particular aircraft penetration sequence in which the housing materials (aircraft and LRU skin, shelving protusions and shielding) and the baffling effect of the LRU contents act as resistance to penetration.

TABLE 9. SURVIVABILITY PARAMETERS

SYMBOL	DESCRIPTION	VALUE		UNITS
	Attack Aspect			
θ	Attack Azimuth	10, 20, 30		degrees
ϕ	Attack Elevation	-5, -10		degrees
ω	Shotline Obliquity Angle	varies		degrees
	Threat (Steel)			
V_p	Projectile/Fragment Velocity	1,200		m/sec
ρ_f	Specific Weight of Penetrator	7,600		gmwt/cm^3
A_p	Presented Area of Penetrator	$\pi d^2/4$		cm^2
d	Diameter of Penetrator	0.12		cm
W	Weight of Penetrator	7.8		gmwt
		120		grain
W_o	Empirical Constant	6.48		grwt
		100		grain
	Target	A/C Skin, A/C Fixtures, LRU Skin (Aluminum)	LRU Interior	
ρ	Specific Weight of Target	2,600	varies	gmwt/cm^3
C_1	Target Material Constants (Empirical)	413	varies	m/sec
C_2		0.941	varies	-
C_3		1.098	varies	-
C_4		-0.038	varies	-
T	Target Thickness			
	A/C Skin	0.64		cm
	A/C Fixtures	0.64		cm
	LRU Skin	0.22		cm
	LRU Interior	varies		cm
$V_{a/c}$	Aircraft Velocity	0.9		Mach
		300		m/sec

Preliminary exercising of the penetration equations for typical LRU configurations in an avionics bay under assumed threat profiles revealed that, with intervening protrusions, penetration through two LRUs was likely. Since ICNIA houses redundant components in at most two LRUs, these penetration results indicate that CNI system kill (loss of both RF or both digital LRUs) will be highly dependent on explicit protection concepts and particular LRU placement, even for simple threat engagements. Because of the dependency on these as-yet-undetermined factors, further S/V analysis and exercising of the rest of the S/V methodology at this time does not appear fruitful.

When compared to discrete systems, the volume and weight reduction payoffs of ICNIA (production) architectures provide the key to any decreased vulnerability. These payoffs can be transformed into various protective measures such as increased shielding and harder LRUs. The effects of these measures, their combination and optimization require an intensive, detailed analysis more fitting to consideration as actual installation nears.

5. SUMMARY AND RECOMMENDATIONS

A methodology has been presented which can represent the features of integration and fault tolerance in complex systems. Techniques for assessing the reliability and logistics support impacts of such an architecture were developed. These techniques are applicable to ICNIA architectures during the early stages of design. The reliability example illustrates the ability of the model to assess redundancy, reconfigurability and component quality in terms of mission reliability. The logistics support model demonstrated the readiness impact of two- versus three-level maintenance, deferral of repair actions until a critical failure occurs, and modularity.

Several conclusions can be drawn from the example which was analyzed. For reliability,

1. Single components that can cause system failures (critical failures), if they exist, are the single most important factor in Mission Completion Success Probability (MCSP) and a major factor in Mean Time Between Critical Failure (MTBCF).

2. A second level of redundancy (at the LRU level) improves reliability only if all critical functions are supported on both of the LRUs.

3. The determination of which functions are critical for a mission and whether they are required simultaneously can drastically affect MCSP.

4. Reconfigurability (e.g., inter-LRU connections) between components that are already redundant does not necessarily enhance reliability.

In terms of supportability,

1. Deferral of repair until a critical failure occurs allows a high sortie rate to be sustained for a longer period without repair. The payoff is substantial for highly fault-tolerant systems, particularly under a two-level maintenance policy. However, some penalty is paid in MCSP for flying systems that contain failed components (less redundancy).

2. High reliability, deferred repair policies, and increased modularity all provide impetus to use two-level maintenance, eliminating expensive intermediate-level test equipment.

The techniques developed have the advantage of not requiring highly detailed design and logistics inputs and of being relatively streamlined. The computerized models are amenable to interactive use and could be hosted on a minicomputer. As a result, the techniques could be applied early in the design phase as a design tool to aid the engineer in building reliability and supportability into an integrated system.

In the survivability area, the reduced volume and weight of ICNIA, compared to discrete systems, provide the key to decreased vulnerability by providing a margin for employing increased protective measures. A method was developed for assessing the Survivability/Vulnerability (S/V) of fault-tolerant avionics. Preliminary analysis of CNI system S/V to a projectile or fragment threat indicated that, even with intervening protrusions, penetration through two LRUs was likely. These results suggest that ICNIA system kill will be dependent on explicit protection concepts and LRU placement; therefore, detailed analysis appears more fitting when actual installation nears.

Several areas of additional research are suggested by this study. The reliability model developed here does not include the effects of incomplete or faulty BIT coverage, which could cause incorrect switching by the system controller. For highly fault-tolerant systems, this effect is likely to be significant. Software reliability and fault tolerance, which will become increasingly important in these systems, also needs further research. Maintenance concepts that rely on smart systems to schedule and reduce the number of repair actions pose another major issue. The implications of attempting to institutionalize such a concept need to be explored. Finally, the enhancement and possibly integration of the models developed here into an interactive, user-friendly package is required if they are to be used by design engineers.

REFERENCES

Air Force Logistics Center, 1971, "Optimum Repair Level Analysis (ORLA)," AFLCM-800-4.

Air Force Logistics Center, 1975,"Recoverable Inventory Control Using MOD-METRIC," AFLCP 57-13.

Air Force Logistics Center, 1976, "Logistics Support Cost Model User's Handbook," Air Force Logistics Center/Acquisition Logistics Division (AFLC/ALD), Report.

Air Force Management Engineering Agency, 1982, "Logistics Composite Model (LCOM) Simulation Software Users Reference Guide," AFMSMMET Report 81-1.1.

Air Force Wright Aeronautical Laboratories, 1977, "Avionics Evaluation Program: Multiple Aircraft, Multiple Sorties, and Cost Accumulation," AFAL TR-76-196.

Air Force Wright Aeronautical Laboratories, 1978a, "The Avionics Laboratory Predictive Operations and Support (ALPOS) Cost Model," AFAL TR-78-49, Vol. II.

Air Force Wright Aeronautical Laboratories, 1978b, "Ku-band Reliability Improvement -- User's Manual for TASA/DEPEND Program," AFAL-TR-78-135, Vol. 3.

Barlow R.E., and Proschan, F., 1975, "Importance of System Components and Fault Tree Events," Stochastic Processes and Their Applications, Vol. 3, pp. 153-172.

Belote, G.E., Severence, J.D., 1977, "FASTGEN II Target Description Computer Program," Booz-Allen Applied Research, ASD-TR-77-24.

Birnbaum, Z.W., Esary, J.D., and Saunders, S.C., 1961, "Multi-Component Systems and Structures and their Reliability," Technometrics, Vol. 3, pp. 55-77.

Birnbaum, Z.W., and Esary, J.D., 1965, "Modules of Coherent Binary Systems," SIAM Journal, Vol. 13, pp. 444-462.

Calvo, A.B., 1982, "Techniques for System Readiness Analysis," IEEE NAECON 82 Proceedings, pp. 628-634.

Camana, P.C., and Campbell, M.E., 1982, "Integrated CNI Avionics Maximizes Reliability," IEEE NAECON 82 Proceedings, pp. 42-45.

REFERENCES (Continued)

Gates, R.K., et al., 1976, "Program LCC Documentation Version 2," The Analytic Sciences Corporation, Technical Report TR-747-3.

Harris, R.L., 1981, "Future Directions in CNI Integrated Avionics," IEEE NAECON 81 Proceedings, pp. 338-344.

Hillestad, R.J., 1982, "Dyna-METRIC: Dynamic Multi-Echelon Technique for Recoverable Item Control," The Rand Corporation, Report No. R-2785-AF.

ITT Avionics Division, 1982, "Integrated Communications, Navigation and Identification Avionics Systems Definition Study, Interim Technical Report," ITT Avionics Division.

ITT Avionics Division, 1983, personal communications, March 3.

Joint Tactical Coordinating Group/Munitions Effectiveness, 1975, "COVART II, Analyst Manual".

Joint Tactical Coordinating Group/Munitions Effectiveness, 1977, "Penetration Equations Handbook for Kinetic Energy Penetrators," Report No. JTCG/ME-77/16,.

Long, W.S., 1982, "Mission Scenario/ICNIA Prioritization Development," General Dynamics presentation.

Mowrer, Walther, Mayerhofer, Schumacher, 1977, "Aircraft Vulnerability Assessment Methodology, Vol. 1," U.S. Army Ballistic Research Laboratories, BRL Report 1796 (JTCG/AS-76-V-004).

The Analytic Sciences Corporation, 1981, "Simulation of Operational Availability/Readiness (SOAR) Model Overview," Report No. EM-2194.

TRW Electronic Systems Gruop, 1982, "Integrated Communications, Navigation and Identification Avionics Project, Interim R&D Status Report".

TRW Electronic Defense Sector, 1982, "Preliminary Prime Item Development Specification for Integrated Communication Navigation Identification Avionics (ICNIA) Terminal".

Veatch, M.H., 1984a, "Impact Analysis of ICNIA System A," The Analytic Sciences Corporation, Technical Report TR-4128-1-1B.

Veatch, M.H., 1984b, "Impact Analysis of ICNIA System B," The Analytic Sciences Corporation, Technical Report TR-4128-1-1C.

APPENDIX A

GLOSSARY

A/J	Anti-jam
ALPOS	Avionics laboratory predictive operations and support model
BIT	Built-In Test
CNI	Communication, navigation and identification
GPS	Global positioning system
HF	1. High frequency, 2. HF clear voice communication set, AN/ARC-190
ICNIA	Integrated communication, navigation and identification avionics
IFFI	Identify friend-or-foe, interrogator set, AN/APX-76B
IFFT	Identify friend-or-foe, transponder set, AN/APX-101
ILS	Instrument landing system, AN/ARC-108
I/O	Input/output
JTIDS	Joint tactical information distribution system
LCC	Life-cycle cost
LCC2	Life-cycle cost model version 2
LCOM	Logistics composite model
LRU	Line replaceable unit
LSC	Logistics support cost model
MCSP	Mission completion success probability
MIREM	Mission reliability model
MTBCF	Mean time between critical failure
MTBF	Mean time between failure

MTBFF	Mean time between function failure
MTTR	Mean time to repair
ORLA	Optimum repair level analysis
RF	Radio frequency
RFI	Ready for issue
R/R	Removal and replacement
SDU	Secure data unit
SEEK TALK	UHF anti-jam voice communication set (to be replaced by HAVE CLEAR)
SINCGARS	Single-channel ground and airborne radio subsystem
SOAR	Simulation of operational availability/readiness
SRU	Shop replaceable unit
S/V	Survivability/vulnerability
TACAN	Tactical air navigation set, AN/ARN-118
UHF	1. Ultra-high frequency, 2. UHF clear voice communication set, AN/ARC-164
VHF	1. Very high frequency, 2. VHF clear voice communication set, AN/ARC-186

END

FILMED

1-86

DTIC