View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by NASA Technical Reports Server

NASA
CP
2167
c.1

NASA Conference Publication 2167

Validation Methods Research for Fault-Tolerant Avionics and Control Systems Sub-Working Group Meeting -

CARE III Peer Review

COPY
ECH
KIRTLAND
0099875
TECH LIBRARY KAFB, NM

*Proceedings of a sub-working
group meeting held at
Research Triangle Institute
Research Triangle Park, North Carolina
September 15-16, 1980*

NASA

TECH LIBRARY KAFB, NM

0099875

NASA Conference Publication 2167

Validation Methods Research for Fault-Tolerant Avionics and Control Systems Sub-Working Group Meeting -

CARE III Peer Review

Kishor S. Trivedi and James B. Clary, *Editors*
Research Triangle Institute

Proceedings of a sub-working group meeting
held at Research Triangle Institute
Research Triangle Park, North Carolina
September 15-16, 1980

NASA
National Aeronautics
and Space Administration

Scientific and Technical
Information Office

1980

PREFACE

The Langley Research Center has been actively pursuing the synthesis of a reliability assessment capability for fault-tolerant computer-based systems for several years. This work has culminated in the development of CARE III (Computer-Aided Reliability Estimation), a product of the Raytheon Company at Sudbury, Massachusetts. The Langley-sponsored CARE III is a general purpose reliability assessment tool for highly reliable fault-tolerant systems.

The CARE III sub-working group meeting represents the first formal step in the validation of CARE III and is a sequal to previous working group meetings I and II entitled "Validation Methods Research for Fault-Tolerant Avionics and Control Systems" (NASA CP-2114 and CP-2130).

The enormous success of the sub-working group meeting must be attributed to the diligence and hard work of Kishor S. Trivedi, the principal investigator of NASA grant NAG1-70, under which this work was sponsored. Acknowledgement must also be given to James B. Clary, co-organizer and co-editor of this report, to all participants who did an earnest evaluation, and to the Langley Research Center, where the working group meetings were conceived and sponsored.

Salvatore J. Bavuso
NASA Technical Manager for NASA Grant NAG1-70 and
CARE III Project Engineer

TABLE OF CONTENTS

1.0 INTRODUCTION

On 15-16 September 1980, a sub-working group meeting was held at the Research Triangle Institute, Research Triangle Park, North Carolina to:

1. Conduct a peer review of CARE III, including an examination of the assumptions on which CARE III is based and the fundamental probabilistic notions behind it.

2. Evaluate CARE III's effectiveness in meeting its goals; namely, to model accurately the behavior of ultrareliable systems required by flight-critical avionics and control systems.

3. Recommend tests that explore and validate the capabilities of CARE III.

To achieve these objectives, four major areas of the CARE III reliability model were considered: 1) the mathematical model itself, 2) the numerical methods employed, 3) the modeling requirements of fault-tolerant architectures, and 4) the tests employed to determine the usefulness and validity of the model. During a presentation of CARE III capabilities and the ensuing technical discussions, sub-working group attendees were asked to focus their efforts on those areas involving their particular expertise, while at the same time maintaining a broad overview of the CARE III reliability modeling process. Following the technical discussions, subgroups were formed to consider and document further the particular concerns in each of these areas.

The participants in this sub-working group praised the CARE III reliability model. They unanimously agreed that the model is mathematically sound and the method is valid. Areas where further work was recommended focused upon the need for a better exposition of the method and an explanation of the user interface.

The detailed conclusions and recommendations of the CARE III sub-working group are presented in the following sections. Section 2.0 addresses the mathematical model, Section 3.0 discusses numerical methods, Section 4.0 considers CARE III from the fault-tolerant architect's viewpoint, and Section 5.0 discusses approaches to CARE III validation.

2.0 MATHEMATICAL MODELS

Professor U. Bhat, Professor W. Smith, Professor K. Trivedi,
Dr. A. White, and Mr. S. McConnel

2.1 Introduction

The design of fault-tolerant avionics and control systems needs to be supported by an assessment of whether the systems possess the level of reliability for which they were designed. Because ultrahigh reliability requirements exist for such systems, an experimental approach based on lifetesting techniques cannot be used to evaluate the systems [1,2]. Analytical models based on stochastic assumptions must then be developed to help predict and validate the reliability of such systems.

Early approaches to reliability prediction were based on a combinatorial method first discussed by Mathur and Avizienis [3]. Their method assumed that the system is a series of subsystems in which a subsystem was modeled to be of hybrid NMR type. The reconfiguration mechanism was assumed to be perfect. Bouricious and his colleagues extended this model to allow the reconfiguration mechanism to have an imperfect coverage [4]. As an embodiment of this notion, the CARE program was developed at JPL as a computer-based reliability evaluation package. This was later modified by Raytheon and was named CARE II [5].

Not all systems of interest can be broken down into a series of smaller subsystems. In such cases, combinatorial methods have been superseded by more general Markov chain methods. Ng and Avizienis [6] have developed a unified model for the reliability evaluation of nonmaintained (closed) fault-tolerant systems based on a Markov approach. These ideas have been incorporated into a computer-based reliability evaluation package known as ARIES [7].

Several limitations of the early approaches became evident with their use in modeling ultrareliable, fault-tolerant systems such as SIFT [8] and FTMP [9]. First, fault coverage was assumed to be a single number, whereas in practice, the times to detect, isolate, and recover from a fault are nonzero random variables. Furthermore, these quantities do depend on the current state of the system. The implication is that the fault-handling behavior of the system needs to be modeled and one or more parameters need to be derived capturing the coverage aspects. Such a coverage model is already a part of CARE II and will continue to be an integral part of CARE III [10].

The second limitation was the assumption that all random variables of interest are exponentially distributed. In practice, this is seldom the case. CARE III is a major departure from conventional approaches in that it purports to support nonexponential distributions.

The third limitation was the assumption that fault-occurrence and fault-handling behavior are simultaneously accounted for by a single Markov model of system behavior. This implies a combinatorial explosion in the state space of the Markov chain, resulting in computation difficulties. It may be recognized, however, that the time constants of the fault-handling processes are several orders of magnitude smaller than those of the fault-occurrence events. It is therefore plausible to analyze separately the fault-handling behavior of the system (the coverage model) and later incorporate the outputs of the coverage model, together with the fault-occurrence behavior, in an overall reliability model. This is the approach used in CARE III.

Although the sub-working group had a number of comments, including some criticisms, it is important to precede a discussion of these comments with a commendation of the CARE III creators for a very competent and thorough job.

2.2 The CARE III Approach

As pointed out in the last section, two major concerns with any advanced reliability prediction model are:

1) the problem of very large state spaces, and
2) the desire to include nonexponential holding times.

The solution adopted for the first problem is the state aggregation (or decomposition) method. One possible approach to the solution of the second problem is to use the Coxian method of stages [11]. Indeed, this approach has been used in other reliability models [12] and in queueing theoretic models for computer performance evaluation [13]. However, the use of the method of stages for the second problem increases the size of the state space, thus further compounding the first problem. The approach to non-exponential holding times adopted in CARE III avoids this pitfall. CARE III uses a combination of sample path enumeration techniques (at the coverage model level) and time-dependent transition parameters resulting in a nonhomogeneous Markov chain (at the aggregate model level).

The CARE III sub-working group attendees were instructed to analyze the following simple example: a two-unit standby redundant system with the failure rate of the spare as zero. The reliability model of this system is shown in Figure 1.

Initially, the system is in the state labelled 0, where both the units are healthy; one of the units is operating while the other is in the standby mode. While in this state, the rate of fault occurrence is assumed to be $\lambda(t)$. Note that, in general, $\lambda(t)$ is time dependent, which allows the holding time in state 0 to be modeled with a distribution other than exponential distribution. When a fault occurs, the system goes through a complex recovery phase modeled by the states and state transitions within the dashed lines in Figure 1. The structure of the recovery model corresponds exactly to the current single-fault coverage model used in CARE III. As one possibility at the end of the recovery phase, the fault is detected and recovery occurs, resulting in continued operation of the system in state 1. The faulty unit is isolated and the good unit switches into operation. Another possibility is that the recovery process is unsuccessful and the system lands in the failure state F. If the system is operating in state 1, a failure can cause the system to finally land in the failure state F.

Figure 2 illustrates what occurs if this multistate transition diagram in Figure 1 is reduced to a simple three-state diagram. The template corresponding to the coverage model within the dashed lines will occur many times in the reliability model of a more complex system; therefore, if a technique is developed for state aggregation of this template, the computation time can be reduced greatly. The intuitive reason for the proposed state aggregation is that there is a natural separation between the fault-occurrence model and the fault-recovery model [1], because faults are relatively rare events, while events in the coverage phase (once entered) occur quite rapidly.

It should be noted that all the states in the coverage model of Figure 1 are collapsed into state 0 of that figure producing state 0' of the aggregate model of Figure 2. It follows that the holding time in state 0' will not be exponentially distributed, even in the simple case where all holding times in the process of Figure 1 were exponentially distributed. The implication is that even if the original Markov chain were homogeneous (i.e., constant transition parameters), the reduced chain would be nonhomogeneous with time-dependent transition parameters.

In order to use the aggregate model of Figure 2, the transition parameters $\lambda_1(t)$ and $\lambda_2(t)$ must be derived from the original model of Figure 1. This computation is done within the COVRGE module in CARE III. The approach, referred to as sample path enumeration by Professor U. N. Bhat, accounts for nonexponential holding times within the coverage model. Once these transition parameters are determined, the aggregate model is solved using the Kolmogorov approach (within the CARE3 module), as outlined in the CARE III document [10].

Having dealt with the problem of large state spaces using the state aggregation method, let us return to the problem of nonexponential holding times. As noted earlier, nonexponential holding times within the coverage model are handled using the sample path enumeration method. In order to deal with nonexponential holding times in states outside the coverage model, let us examine the approach of nonhomogeneous Markov chains. Even if all holding times are assumed to be exponentially distributed in the original model, derived transition parameters of the aggregate model are time dependent, hence the temptation occurs to use time-dependent transition parameters to model nonexponential holding times in the fault-occurrence model.

One problem occurs in using this approach. The time dependency of transition parameters can be easily handled, provided the time is measured from the beginning of system operation (global time). However, nonexponential holding times in a state naturally give rise to time-dependent transition parameters associated with all arcs emanating from the state, with time measured from the point of entry into that state (local time). For example, in Figure 1 three different "clocks" are encountered, labelled respectively by t, t', and τ.

The argument to be used in favor of CARE III here is that all failure processes can be assumed to start at the beginning of system operation; hence, the global time can be used to assign time-dependent transition rates to all arcs due to failure events. Of course, this argument breaks down if renewals (repairs) take place.

The following additional points are to be noted with respect to CARE III:

1. The nonhomogeneous Markov model can only model systems that have fault rates dependent on global time. This follows from the discussion above.

2. The preferred recursion in CARE3 is the unreliability recursion for $Q_j(t)$ (based on equation (10) in [10]). However, this involves the knowledge of $P_j(t)$, the probability of being in state j at time t. The problem has been solved by approximating $P_j(t)$ by $P_j{}^*(t)$ (the same probability assuming perfect coverage). This approximation may not be good when one models either systems with lower reliability or systems with longer mission times.

3. The coverage model is intended to be a universal diagram. It assumes that everything can be modeled by a specific combination of states and state transitions. In this report only the single-fault model has been discussed, but CARE III also includes a comprehensive double-fault model.

4. In calculating the transition parameters of the aggregate model (e.g., $\lambda_1(t)$ and $\lambda_2(t)$ in Figure 2), convolution-type equations such as

$$\int_0^t f(t-\tau)\ g(\tau)\ d$$

are encountered. The quantity f represents the failure probability density function (pdf), while the quantity g represents a pdf within the recovery model. The global time is represented by t, while τ is the local time for the recovery process. It is natural to assume that f varies slowly with respect to τ; hence, it has been approximated as a second-order polynomial in τ. This approximation works because the "failure rates" are orders of magnitude smaller than the "recovery rates".

5. It is not apparent how nonunity dormancy factors can be handled with the present model. For example, in Figure 1 it was assumed that the spare unit did not fail; the corresponding failure process was timed from the instant the spare unit was switched into operation. Thus, if $\mu(t)$ is to be a function of time, it cannot be naturally cast as a function of global time t.

2.3 Recommendations

(1) As noted earlier, the approach used in CARE III is novel and quite difficult to grasp. It is therefore recommended that a tutorial document be prepared in order to explain more completely the techniques used in CARE III. It is recommended that the proposed document first describe the coverage model and then the reliability model in both the original (or overall) and the aggregated versions. One example of a confusing point in the current document [10] is the use of the transition parameter

$$\lambda_{j\ell}(t)\ C_{j\ell}(t)$$

in equation (3). This product-form separation, though appealing from the traditional point of view, is ill-advised mathematically.

(2) CARE III assumes that a system consists of a series of subsystems which in turn consist of a set of modules. A module is considered an atomic unit whose failure characteristic is known. In practice, the module itself may be internally redundant, and a reliability model needs to be formed for the module itself. A hierarchical modeling technique in the context of CARE III needs to be investigated.

(3) The process of reliability modeling involves several levels of approximations and assumptions whose accuracy and correctness need checking. Therefore, validation of the model should be an integral part of modeling. Even if the model cannot be validated in its entirety at one time, it is recommended that validation be attempted in parts. This recommendation is closely related to the overall validation-methods research [1,2].

(4) It is recommended that the Laplace transform method be investigated as an alternative to complex integral equations within COVRGE. This may be particularly effective since the behavior of functions near the time origin within the coverage model is of interest.

3.0 THE CARE III NUMERICAL METHOD

Professor M. Patrick and Professor R. Geist

3.1 The Computer Program

3.1.1 Structured Design

There is evidence that the software implementation of the CARE III model could be considerably strengthened through a review by professional software engineers. Long-range marketing plans necessitate a modularity of design and a clear, concise documentation, as well as run-time efficiency.

3.1.2 Program Testing

A modular design would further allow an exercising of all portions of the code and thus lend a robustness to the entire program without undertaking the formidable task of proving the program correct.

3.1.3 Validation of Output

In addition to the comparison of output with results obtained from other programs of other models, a validation of machine independence seems in order. Will the results obtained on a 64-bit machine remain unaffected by a switch to a 32-bit machine, given that sensitivities of order $< 10^{-9}$ are likely? For example,

$$10^{-14} + 10^{-7} - 10^{-7} = 10^{-14} \qquad \text{64-bit}$$

$$10^{-14} + 10^{-7} - 10^{-7} = 0 \qquad \text{32-bit}$$

3.2 The Reliability Model

3.2.1 Differential Equation Solution

The single-step quadrature methods seem to have been ignored; specifically, differential equation (4) could be solved through application of a classical Runge-Kutta routine. (An adaptive version, RKF45 is suggested. See reference [14].) Though the results may prove less satisfactory than those obtained through methods RM3 and RM4, the classical methods appear superficially to be at least as promising (no evaluation of exp(x) is required) and should not be rejected without sufficient experimentation.

3.2.2 Current Integration Method

Should RM3 and RM4 remain the most viable methods, the use of adaptive quadrature numerical integration is suggested, such as QUANC8, in place of Simpson's and trapezoidal rules. Such routines were designed to yield results to specified levels of accuracy with a minimum of computation time.

3.2.3 Sensitivity of Solution of Reliability Model to Variations in Coverage Coefficients

Small coefficient variation in linear systems of differential equations (such as equation (4)) is a standard setting for introducing computationally ill-conditioned problems. Though real-world examples may not suffer from these ill effects of finite precision arithmetic, the possibility of an ill-conditioned case warrants sensitivity analysis.

3.2.4 Approximation of f(t-τ)

As a function of τ, f(t-τ) is approximated as a second-degree polynomial. Since many polynomial approximations can be made, some justification for the particular choice should be given.

3.3 The Coverage Model

The coverage model appears to be the computationally intensive portion of the program. To the extent that sensitivity analysis (3.2.3) proves the reliability model insensitive to small variations in the coefficients, computation time can be reduced through introduction of approximations in coefficient calculation. Further, efficient methods for solution of Volterra-type equations (see reference [15]) might well prove useful in this model, even in the absence of such approximations.

3.4 Markov Approach (Finding Eigenvalues)

3.4.1 QR Method Versus Hyman-Laguerre

Computational experience indicates that the QR algorithm for finding eigenvalues of a Hessenberg matrix is far superior to using the Hyman-Laguerre methods proposed in Volume II of the CARE III Final Report for Phase I. The results indicate that, for matrices of order ranging from 8 through 64, the QR method is better (in terms of computational time) by factors ranging from 30 to 40. If the Markov approach becomes a part of CARE III, the QR method should replace the Hyman-Laguerre method currently used.

3.4.2 QR Method Versus Lanczos's Method for Sparse Matrices

For large sparse systems there is some evidence that Lanczos's algorithm is the method to use. A comparison of the QR method and Lanczos's method should be carried out.

4.0 FAULT-TOLERANT ARCHITECTURE MODELING REQUIREMENTS

Professor J. Hayes, Mr. S. Elkind, Mr. J. Clary, and
Lt. D. Loudermilk

The objective of CARE III is to develop a computer program for estimating the reliability of fault-tolerant avionic systems. In light of this objective, the following comments, conclusions, and recommendations are offered from a user's point of view. The discussion focused on three major areas: 1) user input requirements, 2) the system model, and 3) the program output.

4.1 User Input Requirements

In reference to user input specifications, four major areas of interest were deemed important:

- CARE III Documentation
- User Design Aids
- User Input Format
- Preprocessing Programs/Modules

4.1.1 Care III Documentation

Due to the complexity of the CARE III model, more explicit documentation should be provided to the user in order to insure a proper understanding of the input specifications required for model operations. The documentation should include, at a minimum, all known constraints and application limitations of the model, a precise definition of all system input requirements, and copious, detailed examples. Examples should include, in explicit detail, techniques and methodologies for both novice and experienced users of CARE III to understand some of the more esoteric input parameters rather than blindly resorting to default values.

4.1.2 Design Aids

Due to the absence of some types of input data and because of certain modeling constraints imposed by the program itself, provisions should be made to allow the user to use the model effectively at his level of understanding. In particular, default values should be provided in the case of unknown parameters (e.g., error propagation rate), or data functions supplied that provide input data within reasonable bounds. Because some modules experience failure processes other than Weibull, a facility for special processes should be included. One possibility could be the capability for the user to supply a subfunction which returns a hazard rate as a function of time.

4.1.3 User Input Format

In order to exploit the utility of the CARE III model to the greatest possible extent, the user's input requirements could be specified in a hardware description language (HDL). This approach offers a potential increase in the fidelity of the input data rather than limiting it to block diagram system descriptions. In terms of user simplification and input accuracy, interactive operation will enhance the model's potentiality for broader use and can provide the user a menu of options, definitions, and requirements necessary for proper model operation.

4.1.4 Preprocessing Modules

In order to model real systems, including interrelationships of system modules, the CARE III model presently requires that a fault tree analysis be run. This information should be specified to the user within the documentation, as well as detailed instructions on the modeling requirements of the fault tree. Also, CARE III does not possess the capability of deriving failure rates for modules of an unknown reliability. As a solution to this problem, it was suggested that a MIL-STD-217-like model be incorporated into CARE III as a preprocessing module.

4.2 System Modeling

CARE III emphasizes certain implicit limitations on the types of systems it can model. These limitations need to be spelled out clearly. Areas of concern include hardware versus software modeling, the allowable description levels in model formulation, and model sensitivity to parameter changes.

4.2.1 Hardware/Software Considerations

While the use of software modules and stages are included in the scope of CARE III, it appears to have been primarily influenced by the needs of hardware system models. The extent to which CARE III can be used to model software systems, or combined hardware-software systems, needs to be clarified. For example, how does the user recognize or define the module boundaries in such systems? Is adequate data on software failure rates, software error propagation rates, etc., likely to be available in a form that can be readily used in a CARE III system model? If not, then the appropriate restrictions on the use of CARE III should be made explicit. It would be very helpful to provide examples illustrating the construction and use of CARE III models in software-dependent ultrareliable systems. The problem of integrating hardware and software modules in the same model must be explicitly addressed.

4.2.2 Multilevel Models

The CARE III reliability model can be viewed as a means of analyzing a system that is described at a single complexity level. In practice, systems are multilevel and hierarchical in nature. Thus, it is possible that the user's input reliability data and output requirements may refer to several different, and perhaps mutually incompatible, levels. This may necessitate considerable preprocessing of input data by the user. Alternatively, he may be forced to construct a sequence of CARE III models at different complexity levels. The user should be made aware of these limitations, and appropriate remedies should be defined. The identification of complexity levels may be more difficult in the case of software systems.

4.2.3 Sensitivity Studies

CARE III could be made much more useful by providing facilities to support the analysis of reliability and coverage as various input parameters of the model are viewed. This would provide the user with a means of identifying aspects of the model that require redesign. Sensitivity analysis can determine the relative importance of various parameters in the modeling process. This information could then be used to simplify the model by deleting areas of low sensitivity, while the model could be made more detailed in highly sensitive areas. Knowledge of the range of values for which a particular parameter is valid can also be computed, allowing use to be made of inexact, worst case, or otherwise poor data. Sensitivity analysis may be particularly useful for estimating the impact of software failures, since software failure data is usually very difficult to obtain. It may be desirable to include features in CARE III that generate sensitivity data automatically.

4.3 Program Output

The CARE III system has the potential for producing outputs useful for the two stages in system design. The first stage is system design, where CARE III should be useful in guiding the design process. The second stage is the final assessment of a design, where a more detailed model is probably used. The outputs considered are: 1) R(t), system reliability as a function of time, 2) data on failure mode frequencies, and 3) sensitivity studies. It is felt that all three are useful and desirable adjuncts to the CARE III system.

4.3.1 Reliability Function

CARE III currently provides system reliability as a function of time.

4.3.2 Coverage Data

CARE III currently outputs the probabilities of occurrence of different coverage failure situations. This information provides a potentially valuable design tool, since it provides a basis for determining the weak points in a system design. This information should be output to the user in a form which can be easily interpreted in terms of the design and can be used to provide feedback to a system designer who does not necessarily understand how CARE III works.

4.3.3 Sensitivity Studies

Currently, CARE III must be run repeatedly to perform studies of a system's sensitivity to changes in input parameters. An automatic sensitivity analysis function should be added to avoid this. It would aid in both the design and assessment stages of system design. In both cases, the analysis shows which parts of a system design are particularly vulnerable to small changes in input parameters. In the design process it gives indications of a possible reliability problem. In the assessment stage, the analysis has a double use. First, if the parameter change produces an unexpected change in reliability, an invalid model or even invalid application of CARE III may be indicated. Second, the analysis shows where a refinement in or expansion of the model may provide a significantly tighter upper bound on the predicted system reliability.

As in the coverage data outputs, this analysis should be reported in a way easily interpretable by someone not intimately familiar with CARE III's internal workings.

4.4 Fault-Tolerant Architecture Modeling Conclusions and Recommendations

The objective of this section is to outline briefly the major conclusions of the CARE III sub-working group participants from a fault-tolerant architect's viewpoint.

4.4.1 Conclusions

The sub-working group believes that CARE III represents the state of the art in models for evaluating ultrareliable electronic systems. Specifically, CARE III addresses user needs for predicting and analyzing the reliability of systems whose probability of failure is $< 10^{-9}$ in 10 hours.

However, limitations in the use of CARE III do exist; these limitations must be made clear to potential users. Of major concern to this group are the limitations of applicability of the model to:

1. systems whose probability of failure is $> 10^{-9}$ in 10 hours, and

2. system software, including executive software and applications software.

4.4.2 Recommendations

The following recommendations are deemed important:

1. The user input interface needs additional work (e.g., more aids to help the user understand and derive input parameters).

2. The input requirements should be more closely coupled to the program output.

3. A "quick-look" capability is needed (e.g., for ball park reliability estimates).

4. A future user workshop should be held to define other desirable input/output characteristics.

5. The potential for expanding CARE III to other, less reliable, fault-tolerant computing requirements needs to be explored.

6. Incorporate, as an integral part of CARE III, the ability to automatically perform sensitivity analyses.

7. Make provisions in CARE III for explicitly handling software errors.

In conclusion, CARE III is an ultrareliable fault-tolerant computing system reliability estimation model. The conclusions and recommendations made here are intended to foster further the transition of CARE III to the user community.

5.0 CARE III TEST CASES

Professor J. Gault, Dr. D. Jessep, and Mr. R. Joobbani

5.1 Introduction

5.1.1 Objectives

The material in this section reflects the contributions of members of a sub-working group with diverse backgrounds and experience. The objectives of this section are to reflect the opinions of the working group concerning the assessment of CARE III. Assessment comprises the following activities:

- model validation,
- implementation validation,
- capability characterization, and
- usability evaluation.

Each of these assessment activities will be defined in more detail and a set of tasks for each activity recommended.

5.1.2 Scope

The assessment activities were viewed as including tests, experiments, analysis, and proof techniques. Proof techniques were discarded as inappropriate due to the numerical nature of CARE III, and the necessity of a formal specification and the high man-hour requirement. The remaining three approaches were included in the recommended assessment tasks.

The absence of any discussion of questionable simplifications or assumptions should be noted and is a consequence of conscious omission, since none were identified by the working group.

5.1.3 Organization

Section 5.2 presents a philosophical overview and further definition of the four assessment activities. Section 5.3 lists and describes a more specific set of tasks for each of these activities. Finally, Section 5.4 summarizes the opinions and recommendations of the sub-working group concerning the assessment of CARE III.

5.2 CARE III Testing and Characterization

5.2.1 Model Validation

The CARE III model exists at two levels. The higher level is the block diagram form of the modules CAREIN, COVRGE, and CARE3. The structure of this level is depicted in the CARE III Final Report (Phase I, Vol. I), which defines the function of each of these modules as follows:

CAREIN: (1) interprets user input on structure, system success criteria, fault model and coverage parameters.

(2) generates internal files to be used in the two downstream models.

COVRGE: determines the coverage parameters for each system stage and operating mode from the inputs.

CARE3: uses data from CAREIN and COVRGE to produce system reliability estimates in accord with input success criteria.

Validation of the model at this level can proceed by segmenting the system and demonstrating that each module performs precisely the functions defined for it above. Additional validation at this level may be done to show that the modules, once validated separately, may be interconnected to operate properly as a set of interconnected modules or as a system.

Lower level validation consists of demonstrating that the basic equations (used in the calculations of each module) function properly. For example, the equations used to calculate coverage in COVRGE would be checked to show that they correctly calculate the proper value of coverage over some range of the argument values.

5.2.2 Implementation Validation

Implementation (program) validation demonstrates that the code, or programming, used to implement each module is bug-free. Hence, rather than indicating that correct results from the reliability point of view are produced, this test is used to demonstrate that no conditions might exist, because of the coding that would provide unexpected results due to human errors in coding or code specification misinterpretation, for example.

5.2.3 Capability Characterization

Capability (program) characterization determines how CARE III data processing parameters might be impacted by expected types of ultrareliable systems to be modeled by the program. These parameters would be of interest to potential users who plan to install a system or to estimate run requirements on an individual run basis. Characterization should lead to the ability to estimate storage requirements, CPU time requirements, and elapsed time requirements for a complete run of the system. A breakdown of these same parameters on a module basis would also be useful.

As a subset of this characterization, "stress testing" of the system should be performed to determine what input system configurations or parameter settings constitute adequate need for extended storage or time.

5.2.4 Usability Evaluation

This evaluation is devoted to the user interfaces to the program package. The first phase of this evaluation assumes the user is protected from entering fallacious data to the system. This data may be out of the normally accepted operating range for a particular variable, or it may be out of the reasonable range for a particular variable. As an example, a coverage of 0.2 may be abnormally low and can simply be flagged by CAREIN. A coverage of 2.0 is unreasonable and the run may be aborted by CAREIN. A check on these kinds of program responses should be made.

The second phase of this evaluation determines the degree to which the CARE III system is portable and maintainable and determines a program baseline for measuring performance. Portability considerations refer to:

1. the degree to which an identified programmer is required to install and bring up the system, and

2. the type of hardware-software support required in a data center to run the program.

Maintainability refers to the evaluation of those changes that can be made in the system without impacting the ability of unchanged portions to perform their function properly. Determination of a test case to be run after a program change would assist in this evaluation. Similarly, a benchmark test case would assist in serving as a program baseline for evaluating performance.

5.3 Test Characterization Tasks

This section presents a more or less specialized set of tests that can be applied to the CARE III package for the purpose of its validity and acceptance. The issues involved are:

a. mathematical model validation,
b. implementation,
c. programming proof,
d. parametric sensitivity,
e. real-life case study for resource requirement, and
f. portability and maintenance test.

Each of these issues will be briefly described.

a. Mathematical Model Validation: Mathematical model validation refers to the proof of correctness of the model applicability and the mathematical transformation. A set of simple, realistic structures and configurations that are easily realized by analytical treatments (such as combinatorial or specialized equations) should be evaluated by CARE III and analytical methods, and the results should be compared.

b. Implementation: In an implementation test, the numerical methods used for the calculations, i.e., integration, are considered. Several numerical methods are applied to the same process and the results are compared to determine the accuracy and, at the same time, the efficiency. In other test programming the numerical methods are compared with analytical methods.

c. Programming Proof: At this stage all the mathematical models and the way they are calculated are translated into a programming language. The programming proof is an attempt to validate and verify the translation process by the use of symbolic simulation or any other program validation (proof-of-software correctness) method. A brute force will exercise all the different paths throughout the program.

d. Parametric Sensitivity: This test is an overall test for all three previous steps. It indicates whether the program generates appropriate derivations due to different system parameter changes. Again, the derivation can be analytically determined.

e. Real-Life Test: A real-life system is chosen as the test bed. The results produced by the CARE III package are compared to the results produced by another reliability evaluator, such as the FTMP model produced by Draper Labs. The real-life test has several benefits. They are:

   1. It proves the correctness of the CARE III package overall.

   2. It studies the performance of the package in terms of care, use, and the system learning cycle.

   3. It specifies a bound on resource requirements, such as time, memory, and storage media.

f. Portability and Maintainability: This test determines the degree to which the CARE III package is system dependent.

5.4 Summary

The CARE III assessment tasks recommended by the sub-working group are summarized in Table 1. To date, the primary examples used to verify CARE III computation have been those obtained by other models, notably those associated with SIFT and FTMP. The sub-working group participants agreed that this comparison was important. In addition, they recommended that other reference points for comparison be generated by:

- using tractable analytic cases,
- creating alternative models of specific cases, and
- segmenting large test cases in order to apply simulation.

Some tasks listed in Table 1 are likely to exceed the requirements of CARE III assessment and may be considered appropriate to more extensive trials beyond the acceptance of the present version of CARE III.

6.0 REFERENCES

1. Trivedi, K. S., J. W. Gault, and J. B. Clary, "The Validation of System Reliability in Life-Critical Applications," Proceedings, Pathways to System Integrity Symposium, National Bureau of Standards, Gaithersburg, MD, June 19, 1980.

2. Gault, J. W., K. S. Trivedi, and J. B. Clary, eds., "Validation Methods Research for Fault-Tolerant Avionics and Control Systems - Working Group Meeting II." NASA CP-2167, 1980.

3. Mathur, F. P. and A. Avizienis, "Reliability Analysis and Architecture of a Hybrid-Redundant Digital System: Generalized Triple Modular Redundancy with Repair," Proc. AFIPS SJCC, 1970.

4. Bouricius, W. G., W. C. Carter, and P. R. Schneider, "Reliability Modeling Techniques for Self-Repairing Computer Systems," Proc. 24th National Conference of ACM, 1969, pp. 295-383.

5. Stiffler, J. J., et al., "An Engineering Treatise of the CARE II Dual Mode and Coverage Models," Final Report, NASA Contract L-18084A, November 1975.

6. Ng, Y. W. and A. Avizienis, "A Model for Transient and Permanent Fault Recovery in Closed Fault-Tolerant Systems," Proc. 1976 Int. Symposium on Fault-Tolerant Computing, June 1976.

7. Ng, Y. W. and A. Avizienis, "ARIES - An Automated Reliability Estimation System," Proc. 1977 Annual Reliability and Maintainability Symposium, January 1977.

8. Wensley, J., et al., "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control," Proceedings of the IEEE, October 1978.

9. Hopkins, A. L., et al., "FTMP - A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft Control," October 1978.

10. Stiffler, J. J., L. A. Bryant, and L. Guccione, "CARE III Final Report, Phase I," NASA Contractor Report 159122, November 1979.

11. Cox, D. R., "The Use of Complex Probabilities in the Theory of Stochastic Processes," Proc. Cambridge Philosophical Society, 1955.

12. Landrault, C. and J. C. Laprie, "SURF - A Program for Modeling and Reliability Prediction for Fault-Tolerant Computing Systems," Information Technology, J. Moneta (ed.), Amsterdam: North-Holland Publishing Company, 1978.

13. Kleinrok, L., Queueing Systems, Volumes I and II, New York, NY: Wiley Interscience, 1975 and 1976.

14. G. E. Forsythe, M. A. Malcolm, and C. B. Moler, Computer Methods for Mathematical Computations, Englewood Cliffs, NJ: Prentice-Hall, 1977.

15. C. E. Froberg, Introduction to Numerical Analysis, Reading, MA: Addison-Wesley Publishing Company, 1965.

TABLE 1.- CARE III ASSESSMENT TASKS

I. Mathematics

a. Go through the math
b. Consider sample cases, solve analytically, and compare the results with CARE III mathematics
c. Use defaulted values and time-independent values to test the math

II. Implementation

a. Compare numerical methods used with analytical methods
b. Compare numerical methods with other numerical methods
c. Exercise as many paths in the program as possible
d. Symbolic execution

III. Parametric Sensitivity

a. Compare the deviations produced as a result of parameter changes with analytical values calculated for deviations

IV. Real-Life Test

a. Compare the results with FTMP
b. Compare the results with SIFT
c. Compare the results with JPL-STAR data

V. Portability

a. Determine the degree of package dependency on the system on which it is first implemented
b. Use the package in different machines and installations

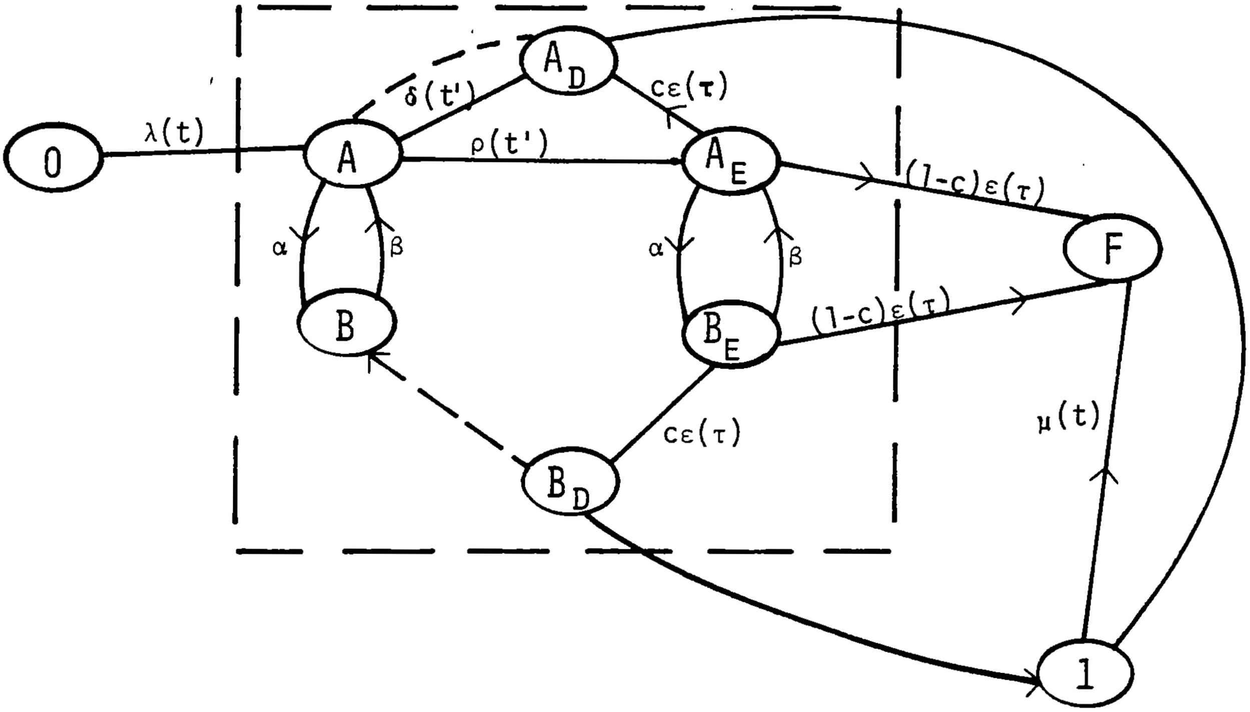

Figure 1.- Overall reliability model of two-unit system.

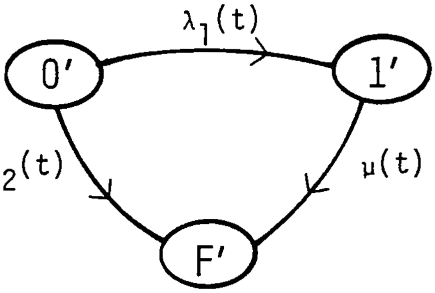

Figure 2.- Aggregated reliability model for a two-unit system.

ATTENDEES

Name	Address
Mr. S. Bavuso	NASA-Langley Research Center Mail Stop 477 Hampton, VA 23665
Dr. U. Bhat	Department of Statistics Southern Methodist University Dallas, TX 75221
Mr. J. Clary	Systems and Measurements Division Research Triangle Institute P.O. Box 12194 Research Triangle Park, NC 27709
Mr. S. Elkind	Department of Computer Science Carnegie-Mellon University Pittsburgh, PA 15213
Dr. J. Gault	Department of Electrical Engineering North Carolina State University P.O. Box 5275 Raleigh, NC 27650
Dr. R. Geist	Computer Science Department Duke University Durham, NC 27706
Dr. J. Hayes	Department of Electrical Engineering-Systems University of Southern California Los Angeles, CA 90007
Dr. D. Jessep	IBM Corporation D/29C B/653-11 101 W. T. Harris Charlotte, NC 28257
Mr. R. Joobbani	Systems and Measurements Division Research Triangle Institute P.O. Box 12194 Research Triangle Park, NC 27709
Lt. D. Loudermilk	AFAL/AAA-3 Wright-Patterson AFB, OH 45433

Name	Address
Mr. S. McConnel	Department of Computer Science Carnegie-Mellon University Pittsburgh, PA 15213
Dr. M. Patrick	Computer Science Department Duke University Durham, NC 27706
Mr. M. Smith	Systems and Measurements Division Research Triangle Institute P.O. Box 12194 Research Triangle Park, NC 27709
Dr. W. Smith	Department of Statistics University of North Carolina Chapel Hill, NC 27514
Dr. J. Stiffler	Raytheon Company Box 3190 528 Boston Post Road Sudbury, MA 01776
Dr. K. Trivedi	Computer Science Department Duke University Durham, NC 27706
Dr. A. White	c/o S. Bavuso NASA-Langley Research Center Mail Stop 477 Hampton, VA 23665

1. Report No. NASA CP-2167	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle
VALIDATION METHODS RESEARCH FOR FAULT-TOLERANT AVIONICS AND CONTROL SYSTEMS SUB-WORKING GROUP MEETING - CARE III PEER REVIEW

5. Report Date
December 1980

6. Performing Organization Code
505-34-43-05

7. Author(s)
Kishor S. Trivedi and James B. Clary, editors

8. Performing Organization Report No.
L-14215

9. Performing Organization Name and Address
Duke University, Dept. of Computer Sciences
Durham, NC 27706
Research Triangle Institute, Systems and Measurements Div.,
Research Triangle Park, NC 27709

10. Work Unit No.

11. Contract or Grant No.

12. Sponsoring Agency Name and Address
National Aeronautics and Space Administration
Washington, DC 20546

13. Type of Report and Period Covered
Conference Publication

14. Sponsoring Agency Code

15. Supplementary Notes
Kishor S. Trivedi: Duke University, Durham, N.C.
James B. Clary: Research Triangle Institute, Research Triangle Park, N.C.

16. Abstract

On September 15-16, 1980, a working group meeting was held at the Research Triangle Institute, Research Triangle Park, North Carolina, to address the following issues:

1. Conduct a peer review of CARE III, including an examination of the assumptions on which CARE III is based and the fundamental probabilistic notions behind it.
2. Evaluate CARE III's effectiveness in meeting its goals; namely, to model accurately the behavior of ultrareliable systems required by flight-critical avionics and control systems.
3. Recommend tests that explore and validate the capabilities of CARE III.

The participants unanimously agreed that the mathematical model is sound and the method valid. Recommendations aimed at enhancing CARE III were presented; in particular, the need for a better exposition of the method and the user interface was emphasized.

17. Key Words (Suggested by Author(s))
CARE III
Reliability
Fault tolerant

18. Distribution Statement
Unclassified - Unlimited

Subject Category 59

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 28	22. Price* A03

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

NASA-Langley, 1980