Reliability Estimation Procedures and CARE: The Computer-Aided Reliability Estimation Program

F. P. Mathur

Astrionics Division

Ultrareliable fault-tolerant onboard digital systems for spacecraft intended for long mission life exploration of the outer planets are under development. The design of systems involving self-repair and fault-tolerance leads to the companion problem of quantifying and evaluating the survival probability of the system for the mission under consideration and the constraints imposed upon the system. Methods have been developed to (1) model self-repair and fault-tolerant organizations; (2) compute survival probability, mean life, and many other reliability predictive functions with respect to various systems and mission parameters; (3) perform sensitivity analysis of the system with respect to mission parameters; and (4) quantitatively compare competitive fault-tolerant systems—various measures of comparison are offered. To automate the procedures of reliability mathematical modeling and evaluation, the CARE (computer-aided reliability estimation) program was developed. CARE is an interactive program residing on the UNIVAC 1108 system, which makes the above calculations and facilitates report preparation by providing output in tabular form and graphical 2-dimensional plots and 3-dimensional projections. The reliability estimation of fault-tolerant organization by means of the CARE program is described in this article.

Introduction

The task of evaluating system performance of digital system architectures designed for long life or ultrareliability is a recurring one. The state-of-the-art of fault-tolerant computing makes available to the designer various models or schemes which by judiciously using protective redundancy impart greater system probability of survival than would be possible by the use of simplex technology alone. One or more of these fault-tolerant schemes—triple modular redundancy (TMR), *N*-tuple modular redundancy, TMR/simplex redundancy, component redundancy, standby replacement, *K*-out-of-*N* systems, hybrid redundancy, and hybrid/simplex redundancy (References 1–5)—in combination make the architecture of fault-tolerant organizations. The overall reliability model takes into consideration the effect of

variation in individual parameters of the basic schemes on the overall system reliability goals—this relationship being expressed as a mathematical function which is often referred to as the reliability mathematical model of the system. The reliability evaluation task, once the system reliability mathematical model is known, may be: (1) to evaluate the system reliability given the values of the model parameters, or (2) to optimize the reliability objective by selecting optimum values of the model parameters. Since the number of combinations of the basic schemes and the range of possible values that the system parameters may undertake are very large, the decision was taken to automate the reliability evaluation procedure which resulted in the development of a conversational computer program called CARE (computer-aided reliability estimation).

Functional Description of CARE

CARE's purpose is to serve as a computer-aided reliability design tool to designers of ultrareliable fault-tolerant systems by facilitating reliability computation, data generation, and comparative evaluation. CARE consists of 4150 Fortran V statements designed to be run on the UNIVAC 1108 under EXEC 8, version 11C (References 6 and 7). The results of the program are available in three forms: (1) as printouts, (2) as graphical 2-dimensional plots, and (3) as graphical 3-dimensional projections.

CARE has three modes of operation: (1) "conversational" or interactive mode, (2) batch mode, and (3) remote-started batch mode. In the "conversational" mode, CARE may be interactively accessed by users from remote teletypes or other communication consoles to perform reliability analysis in "real time." In the batch mode the job is submitted off-line and necessarily no dynamic changes to the user requirements can be made; this mode is expeditious when the user knows his needs exactly and hence need not spend time sitting at a console to input his queries. The remote-started batch mode is similar to the batch mode except that instead of submitting the job as a deck of punched cards the deck entry may be made via a console.

Essentially, CARE consists of a repository of mathematical equations defining the various basic redundancy schemes. These equations may then, under program control, be interrelated to generate the desired mathematical model to fit the architecture of the system under evaluation. The mathematical model may then be supplied with ground instances of its variables and then evaluated to yield values for the specified independent variable or the mathematical model may be further manipulated so as to yield other reliability theoretic results.

CARE's Repository of Equations

The equations residing in CARE model the following basic fault-tolerant organizations:

(1) *Hybrid-redundant (N,S) systems* (see References 1 and 2).

   (a) NMR (N,0) systems (see References 3 and 8).

   (b) TMR (3,0) systems (see Reference 3).

   (c) Cascaded or partitioned versions of the above systems.

   (d) Series string of the above systems.

(2) *Standby-sparing redundant (1,S) systems* (see References 3 and 4).

   (a) K-out-of-N systems (see Reference 4).

   (b) Simplex systems.

   (c) Series string and cascaded versions of the above.

(3) *TMR systems with probabilistic compensating failures* (see Reference 3).

   (a) Series string and cascaded versions of the above.

(4) *Hybrid/simplex redundant* $(3,S)_{sim}$ *systems* (see References 5 and 9).

   (a) TMR/simplex systems (see Reference 4).

   (b) Series string and cascaded versions of the above.

For the description of the above systems and their mathematical derivations, refer to the cited references. These equations are the most general representation of their systems parameterizing mission time, failure rates, dormancy factors, coverage, number of spares, number of multiplexed units, number of cascaded units, and number of identical systems in series. The definition of these parameters resides in CARE and may be optionally requested by the user (see Figure 1). More complex systems may be modeled by taking any of the above listed systems in series reliability with one another.

These reliability equations may be evaluated as a function of absolute mission time, normalized mission time, nonredundant system reliability, or any other system parameter that may be applicable. Among the various measures of reliability that the user may request for computation are: the system mean-life, the reliability at the mean-life, gain in reliability over a simplex system or some other competitive system, the reliability improvement factor, and the mission time availability for some minimum tolerable mission reliability.

Formulation of a Typical Problem for CARE

A typical problem submitted for CARE analysis may be the following: Given a simplex system with 8 equal modules which is made fault-tolerant by providing two standby spares for each module, where each module has a constant failure rate of 0.5 failures per year and where the spares have an

```
@XQT ATMAN.CARE
HELLO TERMINAL - I AM YOUR RELIABILITY ANALYST WITH THE
CARE (COMPUTER-AIDED RELIABILITY ESTIMATION) PACKAGE
DO YOU WISH TO HAVE YOUR ANSWERS TO THE QUESTIONS PRINTED BACK.
ANSWER YES OR NO
YES
DO YOU WISH TO KNOW THE DEFENITIONS OF RELIABILITY PARAMETERS AND TERMS.
ANSWER YES OR NO
YES
THE DEFENITIONS OF THE VARIOUS RELIABILITY PARAMETERS
AND TERMS ARE AS FOLLOWS.

 T = MISSION TIME.
 R = SYSTEM RELIABILITY.
 S = THE TOTAL NUMBER OF SPARES.
 N = THE NUMBER OF MULTIPLEXED UNITS.
 K = INVERSE DORMANCY FACTOR = (LAMBDA/MU).
 C = COVERAGE FACTOR.
   = CONDITIONAL PROBABILITY OF SYSTEM RECOVERING GIVEN A FAILURE OCCURANCE.
 Q = QUOTA, NUMBER OF IDENTICAL UNITS IN A SIMPLEX SYSTEM.
 W = NUMBER OF CASCADED UNITS.
 Z = NUMBER OF IDENTICAL SYSTEMS IN SERIES.
 P = PROBABILITY OF A UNIT FAILING TO A LOGIC ZERO.
 RV= RELIABILITY OF THE RESTORING ORGAN.
 MU= UNPOWERED FAILURE RATE OF A SIMPLEX SYSTEM = K/LAMBDA.
 LAMBDA = POWERED FAILURE RATE OF A SIMPLEX SYSTEM = K*MU.

 LAMT = NORMALISED TIME = LAMBDA*MISSION TIME.
 ELAMT = EXP(-LAMT).
 REL = SYSTEM RELIABILITY.
 UNREL = SYSTEM UNRELIABILITY = (1 - REL).
 SIMREL = SIMPLEX RELIABILITY = ELAMT.
 SIMGAIN = GAIN IN RELIABILITY WITH REFERENCE TO A SIMPLEX SYSTEM .
         = REL/SIMREL.
 SIMRIF = RELIABILITY IMPROVEMENT FACTOR WITH REFERENCE TO A SIMPLEX SYSTEM.
        = (1 - SIMREL)/(1 - REL).

DO YOU NEED INSTRUCTIONS FOR RUNNING THE CARE PROGRAM
ANSWER YES OR NO
YES
SHORTCOMMENT - THE CARE PROGRAM COMPUTES, WITH RESPECT TO THE
SELECTED EQUATIONS AND PARAMETERS THE FOLLOWING RELIABILITY
FUNCTIONS - THE RELIABILITY (REL), UNRELIABILITY (UNREL),
SIMPLEX RELIABILITY (SIMREL), SIMPLE GAIN (SIMGAIN), SIMPLE
RELIABILITY IMPROVEMENT FACTOR (SIMRIF), MEAN TIME TO FAILURE
(MTF), RELIABILITY AT THE MTF, RELIABILITY DIFFERENCE (DIFF),
RELIABILITY GAIN (GAIN), RELIABILITY IMPROVEMENT FACTOR (RIF),
SIMPLE MAXIMUM MISSION TIME (SIMTMAX), MAXIMUM MISSION TIME (TMAX),
SIMPLE TIME IMPROVEMENT FACTOR (SIMTIF), AND THE RATIO OF
TIME IMPROVEMENT FACTORS (RATIF).

2D AND SOME 3D PLOTS CAN BE OBTAINED FOR THE ABOVE COMPUTATIONS.
VARIOUS PLOTTING OPTIONS TO SPECIFY THE ABSCISSA, THE RANGE
OF ABSCISSA AND ORDINATE VALUES ARE AVAILABLE.ABILITY TO PLOT 3D
INTERSECTIONS OF 3D PROJECTIONS WITH 2D PLANES IS ALSO AVAILABLE.
```

Figure 1. A sample of CARE's question/answer capability

```
 THE CARE PROGRAM ALSO EVALUATES COMPLEX RELIABILITY FUNCTIONS
 FORMED BY TAKING PRODUCTS OF THE BASIC RELIABILITY EQUATIONS.

 CARE HAS A MAXIMUM OF 10 DIFFERENT RELIABILITY EQUATIONS
 THESE ARE TABULATED BELOW.
 1. R(N,S) = F(T,LAMBDA,MU,S,N,K,RV,Z,W)
    THIS IS THE GENERAL RELIABILITY EQUATION OF AN HYBRID-
    REDUNDANT SYSTEM.
 2. R(Q,S) = F(T,LAMBDA,MU,S,K,Q,C,Z,W)
    THIS IS THE GENERAL RELIABILITY EQUATION OF A STANDBY-
    REPLACEMENT SYSTEM.
 3. VOID
 4. VOID
 5. R(3,0) = F(T,LAMBDA,RV,Z,W,P)
    THIS IS THE EQUATION FOR A TMR SYSTEM WHERE THE PROBABILITY
    OF A UNIT FAILING TO LOGICAL ONE OR ZERO IS PARAMETERISED.
 6. R(1,0) = (EXP(-LAMBDA*T))**(Z/W)
    THIS IS A GENERAL EQUATION FOR A SIMPLEX SYSTEM.
 7. DUMMY
 THIS IS A DUMMY EQUATION WHICH IS ALL SET UP TO RECEIVE A NEW EQUATION.
 8. BLANK
 9. BLANK
 10.BLANK

 INSTRUCTIONS WILL BE GIVEN FOR ENTERING INPUT DATA
 AT THE TIME THE INPUT DATA IS NEEDED BY THE PROGRAM.

 DO YOU WISH TO FORM A PRODUCT OF RELIABILITIES
 ANSWER YES OR NO
 NO
 TYPE IN COLUMN 1 THE NUMBER OF THE RELIABILITY EQUATION
 TO BE USED - 1 THRU 7

 1
 INPUT VARIABLES FOR EQUATION  1
 T, LAMT, OR ELAMT MUST BE SPECIFIED AND ITS VALUE
 IS THE MAXIMUM VALUE FOR THAT VARIABLE.  MIN IS THE MINIMUM
 AND STEP IS THE INCREMENT FOR T, LAMT, OR ELAMT.
    SOME VARIABLES THAT ARE NEEDED BY THE EQUATIONS ARE SET
 EQUAL TO A DEFAULT VALUE IF THEY ARE NOT INPUTED.  THESE
 VARIABLES AND THEIR DEFAULT VALUES ARE: S=1, N=1, Z=1, W=1
 Q=1.0D0, C=.999,,D0, P=1.0D0, MIN=0.0D0,
 STEP=1.0D0, AND ELAMT=1.0D0.
    IF B IS INPUTED, THEN THIS VALUE IS USED AS THE FIRST
 GUESS FOR THE UPPER LIMIT OF INTEGRATION IN THE CALCULATION
 OF MTF.
    IF OPTION=1, THEN DIFF, RIF, AND GAIN ARE CALCULATED FOR
 ALL POSSIBLE COMBINATIONS OF THE PARAMETER.  IF OPTION=2,
 THEN DIFF, RIF, AND GAIN ARE CALCULATED FOR THE LAST TWO
 PARAMETER VALUES.  IF OPTION=0 OR IS NOT INPUTED, THEN THE
 PROGRAM WILL ASK  THE USER AS TO WHICH PARAMETER VALUES
 DIFF, RIF, AND GAIN ARE TO BE CALCULATED.
 NOTE: DIFF, RIF, AND GAIN ARE NOT COMPUTED IF THE USER IS
 CALCULATING THE PRODUCT OF RELIABILITIES OR PLOTTING 3-D.
```

Figure 1 (contd)

```
THE VARIABLES FOR EQUATION  1 ARE INPUTED USING
VAR AS THE NAMELIST NAME.  A SAMPLE INPUT FOR EQUATION 5 FOLLOWS:
 $VAR
 T=12.0D0,
 LAMBDA=1.0D0,1.5D0,2.0D0,
 RV=1.0D0,
 Z=1,
 W=1,6,
 OPTION=2
 B=10.0D0
 $END
NOTE: NAMELIST INPUT IGNORES COLUMN 1
THE INPUT VARIABLES ARE TYPED AS FOLLOWS
   DOUBLE PRECISION: T, LAMT, ELAMT, MUT, LAMBDA, MU,
     K, RV, Q, C, P, MIN, STEP, AND B
   INTEGER: S, N, W, Z, AND OPTION
INPUT VARIABLES NOW
DO YOU WISH TO MAKE ALTERATIONS TO THE $VAR LIST
ANSWER YES OR NO
NO
DO YOU WISH TO HAVE 2-D RELIABILITY PLOTS - ANSWER YES OR NO
 YES
INPUT A 1 IN THE COLUMN SPECIFIED BELOW IF YOU WISH
THE CORRESPONDING PLOT OPTION. OTHERWISE INPUT 0.
NOTE: WHEN PERFORMING PRODUCT OF RELIABILITIES, NO OTHER
PLOT OPTION BESIDES PRODUCT OF RELIABILITIES MAY BE SPECIFIED.
COLUMN 1 - PLOTS PRODUCT OF RELIABILITIES
COLUMN 2 - PLOTS RELIABILITY
COLUMN 3 - PLOTS DIFF, RIF, AND GAIN
COLUMN 4 - PLOTS MTF AND RELIABILITY AT MTF
COLUMN 5 - PLOTS UNRELIABILITY
01100
FOR ABSCISSA, INPUT 1 IN COLUMN 1 IF ABSCISSA IS T,
 1 IN COLUMN 2 IF ABSCISSA IS LOG(T) - BASE 10,
 1 IN COLUMN 3 IF ABSCISSA IS LAMT,
 1 IN COLUMN 4 IF ABSCISSA IS LOG(LAMT) - BASE 10,
 1 IN COLUMN 5 IF ABSCISSA IS EXP(-LAMBDA*T),
 1 IN COLUMN 6 IF ABSCISSA IS LOG(EXP(-LAMT)) - BASE 10.
 **1***
 IF YOU WISH TO PLOT A CERTAIN RANGE OF X-AXIS VALUES
FOR THE 2-D PLOTS, ENTER LEFT-END POINT IN COLUMNS 1-8 WITH
FORMAT F8.0 AND RIGHT-END POINT IN COLUMNS 9-16 WITH FORMAT F8.0;
OTHERWISE INPUT NO
NO
IF YOU WISH TO PLOT A CERTAIN RANGE OF Y-AXIS VALUES
FOR THE 2-D PLOTS, ENTER LEFT-END POINT IN COLUMNS 1-8 WITH
FORMAT F8.0 AND RIGHT-END POINT IN COLUMNS 9-16 WITH FORMAT F8.0;
OTHERWISE INPUT NO
NO
DO YOU WISH TO PLOT THE LOCUS OF RV SUCH THAT THE
SYSTEM RELIABILITY EQUALS THE UNIT RELIABILITY.
ANSWER YES OR NO
NO
DO YOU WISH TO HAVE 3-D RELIABILITY PLOTS - ANSWER YES OR NO
NO
DO YOU WISH TO CALCULATE MAXIMUM MISSION TIME AND SIMPLE TIME
FOR GIVEN RELIABILITY - ANSWER YES OR NO
```

Figure 1 (contd)

```
YES
DO YOU WANT PLOTS FOR THESE CALCULATIONS - ANSWER YES OR NO
YES
DO YOU WISH TO CALCULATE MAXIMUM MISSION TIME FOR
GIVEN RELIABILITY AND COMPARE IT AGAINST OTHER PARAMETERS
ANSWER YES OR NO
YES
INPUT IN COLUMN 1 ONE OF THE FOLLOWING THREE OPTIONS:
1. MAXIMUM MISSION TIME IS COMPARED AGAINST ALL POSSIBLE
COMBINATIONS OF THE PARAMETER,
2. MAXIMUM MISSION TIME IS COMPARED AGAINST THE LAST TWO
PARAMETER VALUES,
3. THE PROGRAM ASKS THE USER AS TO WHICH PARAMETER VALUES
MAXIMUM MISSION TIME IS TO BE COMPARED.
1
DO YOU WANT PLOTS FOR THESE CALCULATIONS - ANSWER YES OR NO
NOTE: WHEN EXERCISING OPTION 1, THE PROGRAM PLOTS
ONLY THE FIRST 15 PARAMETER COMPARISONS
YES
INPUT THE FOLLOWING 4 VARIABLES EACH WITH FORMAT F8.0
COLUMNS  1-8  - REFERENCE RELIABILITY R2
COLUMNS  9-16 - MINIMUM RELIABILITY R1
COLUMNS 17-24 - MAXIMUM RELIABILITY R1
COLUMNS 25-32 - RELIABILITY R1 STEP SIZE
   1.000    .000   1.000    .100
DO YOU WISH TO HAVE PRINTED TABLE OF RELIABILITY RESULTS
ANSWER YES OR NO
YES
DO YOU WISH TO HAVE PRINTED TABLE OF DIFF, RIF,
AND GAIN RESULTS - ANSWER YES OR NO
YES
DO YOU WISH MTF AND RELIABILITY AT MTF RESULTS PRINTED
ANSWER YES OR NO
YES
DO YOU WANT PRINTED RESULTS OF THE MAXIMUM MISSION
TIME CALCULATIONS - ANSWER YES OR NO
YES
TYPE IN THE VARIABLE THAT IS TO BE USED
FOR THE FAMILY OF PARAMETERS - MUST BE SPECIFIED
K

      CALCULATIONS FOR EQUATION  1A      (NI MEANS NOT INPUTED)
                        PARAMETER IS K

 LAMBDA          MU          S    N          K          Q
    NI      .0000000         1    1   .1000000+01       NI

    C          RV           Z    W          P         MUT
   NI   .1000000+01          1    1   .1000000+01       NI

 LAMT       REL         UNREL       SIMREL      SIMGAIN      SIMRIF
 .000   1.0000000     .0000000   1.0000000   .1000000+01  .1000000+36
 .100    .9967989     .0032011    .9948374   .1101633+01  .2972798+02
 .200    .9794141     .0205859    .8187307   .1196259+01  .8805495+01

ETC...
```

Figure 1 (contd)

inverse dormancy factor of 10 and the applicable coverage factor being 0.99, it is required to evaluate the system survival probability in steps of 1/10 of a year for a maximum mission duration of 12 years. It is required that the system reliability be compared against the simplex or nonredundant system and that all these results be tabulated and also plotted. It is further required that the mean-life of the system as well as the reliability at the mean-life be computed. It is of interest to know the maximum mission duration that is possible while sustaining some fixed system reliability objective and to display the sensitivity of this mission duration with respect to variations in the tolerable mission reliability.

It is also required that the above analysis be carried out for the case where three standby spares are provided and these configurations of three and two spares be compared and the various comparative measures of reliability be evaluated and displayed.

The above problem formulation is entered into CARE by stating that Equation 2 (which models standby spare systems) is required and the pertinent data (S = 2, 3; Z = 8; K = 10; T = 12.0; LAMBDA = 0.5; C = 0.99; STEP= 0.1; option = 2) is inserted into CARE between the delimiters \$VAR. . .\$END using the VAR namelist.

The above example illustrates the complexity of problems that may be posed to CARE, and the simplicity with which the specifications are entered. The reliability theoretic functions to be performed on the above specified system are acknowledged interactively by responding a YES or NO on the demand terminal to CARE's questions at the time it so requests. A

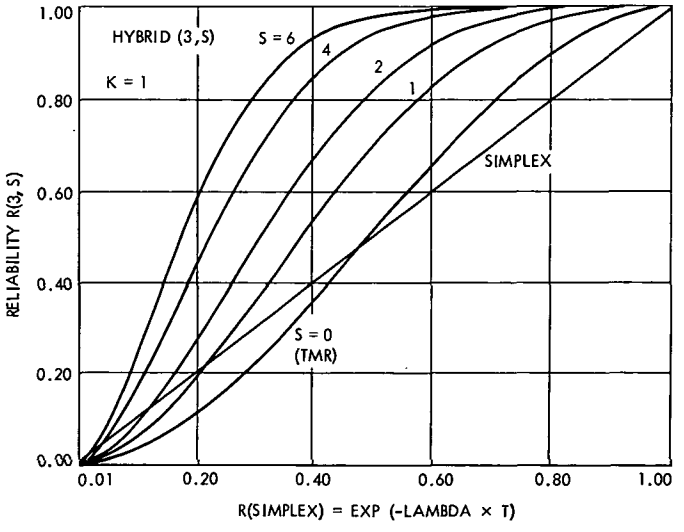

Figure 2. A sample plot by CARE

partial sample run illustrating the question/answer segment of CARE is shown in Figure 1. A sample reliability plot generated by CARE for the hybrid (3,S) system for $S = 6, 4, 2$, and 1 at $K = 1$ is given in Figure 2.

Acknowledgment

The author wishes to acknowledge the support of Mr. G. L. Winje of the Data Systems Division of JPL for much of the programming required in the implementation of the CARE subroutines.

References

1. Mathur, F. P., "Reliability Modeling and Analysis of a Dynamic TMR System Utilizing Standby Spares," *Proceedings of the Seventh Annual Allerton Conference on Circuit and System Theory, University of Illinois, Urbana, October 8–10, 1969*, pp. 243–252.

2. Mathur, F. P., and Avizienis, A., "Reliability Analysis and Architecture of a Hybrid Redundant Digital System: Generalized Triple Modular Redundancy with Self-Repair," *AFIPS Conference Proceedings (Spring Joint Computer Conference), Vol. 36, Atlantic City, May 5–7, 1970.*

3. Mathur, F. P., *Reliability Modeling and Architecture of Ultra-Reliable Fault-Tolerant Digital Computers*, Ph.D. Thesis, University of California at Los Angeles, Computer Sciences Dept., June 1970. University Microfilms, Inc., Ann Arbor, Mich., Reorder No. 71-662.

4. Roth, J. P., Bouricius, W. G., Carter, W. C., and Schneider, P. R., *Phase II of an Architectural Study for a Self-Repairing Computer*, Report SAMSO TR-67-106. International Business Machines Corp., Nov. 1967.

5. Mathur, F. P., "On Reliability Modeling and Analysis of Ultrareliable Fault-Tolerant Digital Systems," to be published in the Special Fault-Tolerant Computing issue of the *IEEE Transaction on Computers*, Vol. C-20, No. 10, Nov. 1971.

6. *Univac 1108 Multi-Processor System: System Description*, Form UP-4046, Rev. 2. Sperry Rand Corp., 1968.

7. *Univac 1108 Multi-Processor System: Fortran V Programmer's Reference Manual*, Form UP-4060, Rev. 1. Sperry Rand Corp., 1969.

8. Mathur, F. P., "Reliability Study of Fault-Tolerant Computers," in *Supporting Research and Advanced Development*, Space Programs Summary 37-58, Vol. III, pp. 106–113. Jet Propulsion Laboratory, Pasadena, Calif., Aug. 31, 1969.

9. Mathur, F. P., "Reliability Modeling, Analysis and Prediction of Ultrareliable Fault-Tolerant Digital Systems," *Digest of the 1971 International Symposium on Fault-Tolerant Computing, Pasadena, California, March 1–3, 1971*, pp. 79–82.