Reliability Analysis Based on a Mathematical Tool

Jahangir Ghajar Dowlatshahi □ Unisys □ Eagan

Key Words: Mathematical Toolbox, Symbolic notation, Coverage, Markov Analysis.

ABSTRACT

The reliability engineering analysis task involves understanding system requirements, modeling the system to respond to these requirements, applying the right mathematical equations that run the model, extracting the results, changing the parameters, and then analyzing them for the optimum design goals (sensitivity analysis, trend analysis, life cycle analysis, growth analysis, and so forth).

One of the most difficult and time–consuming aspects of a system reliability analysis cycle (especially for large,complex, and fault tolerant systems) is the mathematical computations of the system reliability. Personal computers with spreadsheet programs have been successfully used to perform reliability analysis. The mathematical formulas for these applications are usually entered into a macro and exist in the cells of the spreadsheet, or stay in a library of specialized functions to be called to the spreadsheet when required. A new generation of mathematical tools (Mathematical Toolboxes) featuring symbolic notation, a rich source of mathematical functions, graphics and text capabilities, are currently on the market. These tools take the burden of complex and tedious mathematical computations from the reliability engineer and leave the engineer with the basics of reliability engineering design.

This paper describes one such tool that has been used to model systems with redundancy and coverage. Coverage is the probability of automatically recovering from faults within a specified time and without affecting normal system operation.

INTRODUCTION

Those of us in the reliability engineering world have experienced the great value of statistical problem solver software programs and have also experienced situations in which no existing software programs could solve our problems completely.

System reliability analysis (especially for fault tolerant systems) adds another dimension to the difficulty and complexity of analysis techniques. This is because various reliability analysis techniques and procedures must be integrated into one system. In many instances, the reliability engineer puts different procedures and solution strategies together in order to solve a special application, by trying to answer the following questions step–by–step:

1. Are the system modules in series/parallel?
2. Is the system repairable or non–repairable?
3. Are failures in the system mutually independent?
4. Has the system full coverage or is coverage < 1?
5. Is the system time–dependent or failure–dependent?
6. Can the assumption of exponential distribution for failures hold, or should the engineer use a different distribution?

A mathematical reliability model can then be generated to represent the actual operational system. Without a powerful simulation and computation tool, the analysis of the model proves to be very cumbersome in many specialized systems.

Added to these problems is the computation/analysis of software reliability, with numerous approaches to solve them. There is virtually no single statistical/mathematical software package that can resolve every reliability problem that engineers would face.

Mathematical Toolboxes, with symbolic manipulation capability to perform algebraic calculations, are currently used heavily in the scientific and engineering arenas. The mathematical operation is usually performed sequentially starting with the definitions of constants and variables, followed by the application formulas. Text can be inserted at any point to define the assumptions, mathematical approaches, procedures and analysis techniques, etc. Numerical results can be obtained at every step of computation.

Mathematical Toolboxes in the hands of the reliability engineers are valuable tools to perform step–by–step sequential and logical reliability analysis. All steps are clear–cut, readable, and easily understood as the analysis proceeds. There are no hidden formulas/equations, functions, or rules defining the process. Each step can be evaluated (e.g., using sensitivity analysis and plotting the results), validated, and integrated into the system model. The results can then be tested and evaluated for the overall system reliability performance. The final result is an excellent documentation of the processes involved in modeling and analyzing a system reliability problem.

A powerful environment, in which one can build a prototype/simulation of an actual reliability application, allowing rapid change and refinement, is easy to achieve. Standard numerical methods such as integration, solution of differential equations, and matrix/vector operations, so widely used in the Markov reliability modeling, can be very efficiently implemented using Mathematical Toolboxes.

The following examples have been specially selected to demonstrate the capability of one such Mathematical Toolbox, the MathCAD tool, as used by the author to solve and document the reliability problems. The examples presented in this paper assume independence among the subsystems comprising the total system, except for the Markov models where dependencies among lower system units exist.

EXAMPLE 1 - NO-REPAIR SERIAL SYSTEM

Define Constants and Variables:

T := 0 . .100 Mission Duration

Mean Time to Failure (MTTF) for Units A, B, C, and D:

MTTFA := 1000	MTTFB :=2000
MTTFC := 500	MTTFD :=200

Reliability For Each Block:

$$R\_A(T) := e^{-\left[\frac{T}{MTTFA}\right]}$$ First block

$$R\_B(T) := e^{-\left[\frac{T}{MTTFB}\right]}$$ Second block

$$R\_C(T) := e^{-\left[\frac{T}{MTTFC}\right]}$$ Third block

$$R\_D(T) := e^{-\left[\frac{T}{MTTFD}\right]}$$ Fourth block

System Reliability:

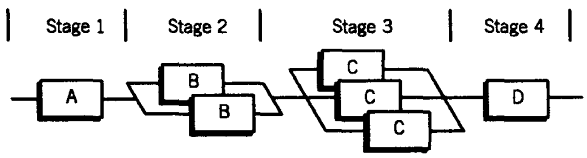
$R\_system(T) := R\_A(T) \cdot R\_B(T) \cdot R\_C(T) \cdot R\_D(T)$
$R\_system(100) = 0.427415$

System Mean Up Time (MUT):

$$MUT := \frac{\int_0^{100} R\_A(T) \cdot R\_B(T) \cdot R\_C(T) \cdot R\_D(T)\, dT}{1 - R\_system(100)}$$

MUT = 117.65

EXAMPLE 2 - NO REPAIR PARALLEL/ SERIAL SYSTEM



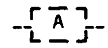
Define Constants and Variables:

T :=0,50 ..1000 Operation time (variable, in steps of 50 up to 1000 hours)

MTTF1 := 1000	MTTF for Block A
MTTF2 := 200	MTTF for Block B
MTTF3 := 500	MTTF for Block C
MTTF4 := 5000	MTTF for Block D

Reliability for first stage:

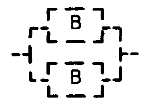
$$R\_A(T) := e^{-\left[\frac{T}{MTTF1}\right]}$$ Block A



$R\_STAGE1(T) := R\_A(T)$ Stage 1

Reliability for second stage :

$$R\_B(T) := e^{-\left[\frac{T}{MTTF2}\right]}$$ Block B

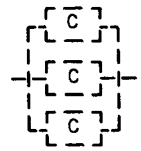


$$R\_STAGE2(T) := R\_B(T)^2 + 2 \cdot R\_B(T) \cdot (1 - R\_B(T))$$

Stage 2 (1 of 2 required)

Reliability for third stage:

$$R\_C(T) := e^{-\left[\frac{T}{MTTF3}\right]}$$ Block C

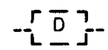


$$R\_STAGE3(T) := R\_C(T)^3 + 3 \cdot R\_C(T)^2 \cdot (1 - R\_C(T))$$

Stage 3 (2 of 3 required

Reliability for the fourth stage:

$$R\_D(T) := e^{-\left[\frac{T}{MTTF4}\right]}$$ Block D



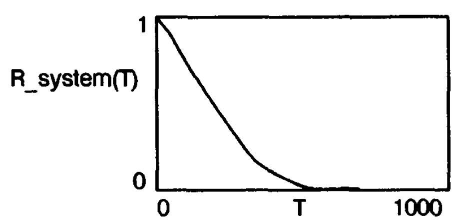
$R\_STAGE4(T) := R\_D(T)$ Stage 4

System Reliability Analysis:

$R\_system(T) := R\_STAGE1(T) \cdot R\_STAGE2(T) \cdot R\_STAGE3(T) \cdot R\_STAGE4(T)$

$R\_system(100) = 0.684646$ System reliability at 100 hours mission

System reliability as a function of operation time can be plotted as shown here:

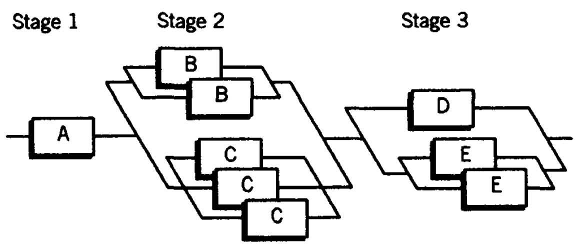


System Mean Up Time (MUT):

$$MUT := \frac{\int_0^{1000} R\_system(T)\, dT}{1 - R\_system(1000)}$$

MUT = 179.286

EXAMPLE 3 - REPAIRABLE, LOWER LEVELS IN PARALLEL, COVERAGE = 1



Define Constants and Variables:

MTTF_A := 1000	MTTR_A := 1
MTTF_B := 500	MTTR_B := 1
MTTF_C := 200	MTTR_C := 2
MTTF_D := 1000	MTTR_D := 5
MTTF_E := 300	MTTR_E := 10

Reliability for the first stage:

MTTF_S1 := MTTF_A — Stage 1 MTTF
MTTR_S1 := MTTR_A — Stage 1 MTTR

Reliability for the second stage:

Using the Einhorn model, the MTTFs of the combined "B" branches are:

$$\text{MTTF\_B1} := \frac{\text{MTTF\_B}^2}{2\cdot\text{MTTR\_B}}$$ MTTF for 1 of 2 parallel B units

MTTF_B1 = 125000
N := 2 — Number of B units in parallel
R := 1 — Number of B units required

$$\text{MTTR\_B1} := \frac{\text{MTTR\_B}}{N - R + 1}$$ MTTR of parallel units using Einhorn equation

MTTR_B1 = 0.5

$$\text{MTTF\_C1} := \frac{\text{MTTF\_C}^3}{3\cdot\text{MTTR\_C}^2}$$ MTTF for 1 of 3 parallel C units

MTTF_C1 = 666667
N := 3 — Number of C units in parallel
R := 1 — Number of C units required

$$\text{MTTR\_C1} := \frac{\text{MTTR\_C}}{N - R + 1}$$ MTTR of parallel units using the Einhorn definition

MTTR_C1 = 0.667

Stage 2 MTTF and MTTR for the parallel non-identical units are:

$$\text{MTTR\_S2} := \frac{1}{\frac{1}{\text{MTTR\_B1}} + \frac{1}{\text{MTTR\_C1}}}$$ Stage 2 MTTR

MTTR_S2 = 0.286

$$\text{U\_B1} := \frac{\text{MTTR\_B1}}{\text{MTTF\_B1} + \text{MTTR\_B1}}$$ Unavailability of B1 unit

$\text{U\_B1} = 4\cdot 10^{-6}$

$$\text{U\_C1} := \frac{\text{MTTR\_C1}}{\text{MTTF\_C1} + \text{MTTR\_C1}}$$ Unavailability of C1 unit

$\text{U\_C1} = 1\cdot 10^{-6}$

$\text{U\_S2} := \text{U\_B1}\cdot\text{U\_C1}$ — Stage 2 Unavailability

$$\text{MTTF\_S2} := \text{MTTR\_S2}\cdot\frac{1 - \text{U\_S2}}{\text{U\_S2}}$$ Stage 2 MTTF

$\text{MTTF\_S2} = 7\cdot 143\cdot 10^{10}$

Reliability for the third stage:

$$\text{MTTF\_E1} := \frac{\text{MTTF\_E}^2}{2\cdot\text{MTTR\_E}}$$

MTTF_E1 = 4500

N := 2 — Number of E units in parallel
R := 1 — Number of E units required

$$\text{MTTR\_E1} := \frac{\text{MTTR\_E}}{N - R + 1}$$

MTTR_E1 = 5

Stage 3 MTTF and MTTR for the parallel non-identica units are:

$$\text{MTTR\_S3} := \frac{1}{\frac{1}{\text{MTTR\_D}} + \frac{1}{\text{MTTR\_E1}}}$$ Stage 3 MTTR

MTTR_S3 = 2.5

$$\text{U\_D} := \frac{\text{MTTR\_D}}{\text{MTTF\_D} + \text{MTTR\_D}}$$ Unavailability of D unit

U_D = 0.005

$$\text{U\_E1} := \frac{\text{MTTR\_E1}}{\text{MTTR\_E1} + \text{MTTF\_E1}}$$ Unavailability of combined E units

U_E1 = 0.001

$\text{U\_S3} := \text{U\_D}\cdot\text{U\_E1}$ — Stage 3 Unavailability

$$\text{MTTF\_S3} := \text{MTTR\_S3}\cdot\frac{1 - \text{U\_S3}}{\text{U\_S3}}$$ Stage 3 MTTF

$\text{MTTF\_S3} = 4.528\cdot 10^5$

System Analysis

System Mean Up Time (MUT)

$$MUT := \frac{1}{\frac{1}{MTTF\_S1} + \frac{1}{MTTF\_S2} + \frac{1}{MTTF\_S3}}$$

$MUT = 998$

System Mean Down Time (MDT)

$$MDT := \frac{\frac{1}{MTTF\_S1} \cdot MTTR\_S1 + \frac{1}{MTTF\_S2} \cdot MTTR\_S2 + \frac{1}{MTTF\_S3} \cdot MTTR\_S3}{\frac{1}{MUT}}$$

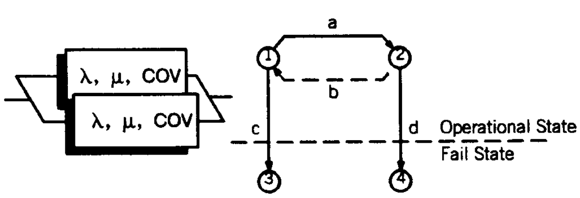
$MDT = 1.0033$

System Availability (AVAIL) :

$$AVAIL := \frac{MUT}{MUT + MDT}$$

$AVAIL = 0.999$

EXAMPLE 4 - STEADY STATE MARKOV, COVERAGE < 1



In this example, the effect of redundancy and stand–by operation is examined.

Assumptions:

$\lambda := .001$	Failure rate per million hours of operation
$MTTR := 1$	MTTR, hours (= $1/\mu$)
$COV := .9$	Coverage, the degree of fault tolerance

One of two units, degraded mode

The coefficients of the matrix are:

$a := 2 \cdot \lambda \cdot COV$ $\quad c := 2 \cdot \lambda \cdot (1 - COV)$

$b := \frac{1}{MTTR}$ $\quad d := \lambda$

The matrix equations are:

$$M := \begin{bmatrix} -(a+c) & b \\ a & -(b+d) \end{bmatrix} \quad V := \begin{bmatrix} -1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} T1 \\ T2 \end{bmatrix} := M^{-1} \cdot V$$

T1 and T2 are the times spent in states 1 and 2, respectively.

$MTTF := T1 + T2$ — MTTF can be found by summing the times spent in the two Up states

$MTTF = 4964$

One of two units, hot stand–by (one unit is active):

$a := \lambda \cdot COV + \lambda$

$c := \lambda \cdot (1 - COV)$

$$M := \begin{bmatrix} -(a+c) & b \\ a & -(b+d) \end{bmatrix} \quad V := \begin{bmatrix} -1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} T1 \\ T2 \end{bmatrix} := M^{-1} \cdot V$$

T1 and T2 are the times spent in states 1 and 2, respectively.

$MTTF := T1 + T2$ — MTTF can be found by summing the times spent in the two Up states

$MTTF = 9832$

Cold standby (one unit is active, the other is non–operating):

$a := \lambda \cdot COV$

$c := \lambda \cdot (1 - COV)$

$$M := \begin{bmatrix} -(a+c) & b \\ a & -(b+d) \end{bmatrix} \quad V := \begin{bmatrix} -1 \\ 0 \end{bmatrix}$$

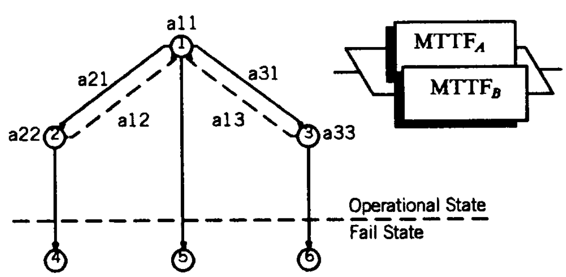
$$\begin{bmatrix} T1 \\ T2 \end{bmatrix} := M^{-1} \cdot V$$

T1 and T2 are the times spent in states 1 and 2, respectively.

$MTTF := T1 + T2$

$MTTF = 9920$

EXAMPLE 5 - NON-IDENTICAL, REPAIRABLE, COVERAGE < 1 MTTF MODEL, MARKOV ANALYSIS



Define Constants and Variables:

$MTTF\_A := 1000$	MTTF for unit A
$MTTF\_B := 500$	MTTF for unit B
$MTTR\_A := 1$	MTTR for unit A
$MTTR\_B := 1$	MTTR for unit B
$COV\_A := .95$	Coverage for unit A
$COV\_B := .99$	Coverage for unit B

The coefficients of the matrix are:

$$a11 := \frac{1}{MTTF\_A} + \frac{1}{MTTF\_B}$$

$$a12 := \frac{1}{MTTR\_A} \qquad a13 := \frac{1}{MTTR\_B}$$

$$a21 := \frac{1}{MTTF\_A} \cdot COV\_A$$

$$a22 := \frac{1}{MTTF\_B} + \frac{1}{MTTR\_A} \qquad a23 := 0$$

$$a31 := \frac{1}{MTTF\_B} \cdot COV\_B$$

$$a32 := 0 \qquad a33 := \frac{1}{MTTF\_A} + \frac{1}{MTTR\_B}$$

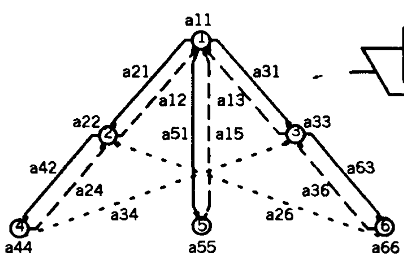
The matrix equations are:

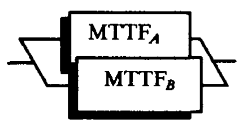
$$M := \begin{bmatrix} -a11 & a12 & a13 \\ a21 & -a22 & a23 \\ a31 & a32 & -a33 \end{bmatrix} \qquad V := \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} T1 \\ T2 \\ T3 \end{bmatrix} := M^{-1} \cdot V \qquad \begin{bmatrix} T1 \\ T2 \\ T3 \end{bmatrix} = \begin{bmatrix} 13536.52 \\ 12.834 \\ 26.776 \end{bmatrix}$$

MTTF := T1 + T2 + T3   Sum of the Up states
MTTF = 13576

EXAMPLE 6 - NON-IDENTICAL, REPAIRABLE, COVERAGE < 1 AVAILABILITY MODEL, MARKOV ANALYSIS





Define Constants and Variables:

MTTF_A := 1000	MTTF for unit A
MTTF_B := 500	MTTF for unit B
MTTR_COV_A := 1	MTTR for covered unit A failures
MTTR_UCOV_A := .5	MTTR for uncovered unit A failures
MTTR_COV_B := 1	MTTR for covered unit B failures
MTTR_UCOV_B := .5	MTTR for uncovered unit B failures
COV_A := .95	Coverage for unit A
COV_B := .99	Coverage for unit B

The Markov Availability solution for non-identical 1 or 2 units with coverage < 1 is computed as follows:

The Coefficients of the Matrix:

$$a11 := \frac{1}{MTTF\_A} + \frac{1}{MTTF\_B}$$

$$a12 := \frac{1}{MTTR\_COV\_A}$$

$$a13 := \frac{1}{MTTR\_COV\_B} \qquad a14 := 0$$

$$a21 := \frac{1}{MTTF\_A} \cdot COV\_A$$

$$a22 := \frac{1}{MTTF\_B} + \frac{1}{MTTR\_COV\_A}$$

$$a23 := 0$$

$$a31 := \frac{1}{MTTF\_B} \cdot COV\_B \qquad a32 := 0$$

$$a33 := \frac{1}{MTTF\_A} + \frac{1}{MTTR\_COV\_B}$$

$$a15 := \frac{\frac{1-COV\_A}{MTTF\_A} \cdot MTTR\_UCOV\_A + \frac{1-COV\_B}{MTTF\_B} \cdot MTTR\_UCOV\_B}{\frac{1-COV\_A}{MTTF\_A} + \frac{1-COV\_B}{MTTF\_B}}$$

$$a16 := 0$$

$$a24 := \frac{1}{MTTR\_COV\_A} \qquad a25 := 0$$

$$a26 := \frac{1}{MTTR\_COV\_B}$$

$$a34 := \frac{1}{MTTR\_COV\_A} \qquad a35 := 0$$

$$a36 := \frac{1}{MTTR\_COV\_A} \qquad a41 := 0$$

$$a42 := \frac{1}{MTTF\_B} \qquad a43 := 0$$

$$a44 := \frac{1}{MTTR\_COV\_A} + \frac{1}{MTTR\_COV\_B}$$

$$a45 := 0$$

$$a46 := 0$$

$$a51 := \frac{1-COV\_A}{MTTF\_A} + \frac{1-COV\_B}{MTTF\_B}$$

$$a52 := 0 \qquad a53 := 0 \qquad a54 := 0$$

$$a55 := a15 \qquad a56 := 0 \qquad a61 := 0$$

$$a62 := 0 \qquad a63 := \frac{1}{MTTF\_A}$$

$$a64 := 0 \qquad a65 := 0 \qquad a66 := a44$$

The matrix equations are:

$$M := \begin{bmatrix} -a11 & a12 & a13 & a14 & a15 & a16 \\ a21 & -a22 & a23 & a24 & a25 & a26 \\ a31 & a32 & -a33 & a34 & a35 & a36 \\ a41 & a42 & a43 & -a44 & a45 & a46 \\ a51 & a52 & a53 & a54 & -a55 & a56 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$V := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} A1 \\ A2 \\ A3 \\ A4 \\ A5 \\ A6 \end{bmatrix} := M^{-1} \cdot V$$

$$\begin{bmatrix} A1 \\ A2 \\ A3 \\ A4 \\ A5 \\ A6 \end{bmatrix} := \begin{bmatrix} 0.99693747 \\ 0.00094713 \\ 0.0019739 \\ 0.00000095 \\ 0.00013957 \\ 0.00000099 \end{bmatrix}$$

Availability := A1 + A2 + A3 Sum of the Up states
Availability = 0.99986

CONCLUSIONS

The MathCAD program has proven to be very useful in reliability analysis of simple to more complex fault tolerant systems. Sensitivity and trade–off analyses can be performed easily and within the program, and the results can be shown in graphical format for effective evaluation.

Libraries of function/macros can be developed that may be used to model every system configuration.

Text, formulas and graphics inside the MathCAD program, describing the entire analysis, can be used to generate formal documentation such as a reliability analysis report. The results are readable and easily understandable. There are no hidden functions/formulas or procedures in the body of the analysis. What you see is what you get.

Error messages are especially useful in the sequential analysis process, since every error is flagged on the spot when it first occurs and is shown throughout the analysis wherever it appears and affects other computations. This assures step–by–step error checking and optimum accuracy of the analysis.

The MathCAD tool helps the reliability engineer concentrate on modeling systems without getting involved in detailed mathematical computation of the system models.

REFERENCES

1. Godin, Edward E., "What you always wanted to know about reliability but were afraid to ask", Internal Unisys Document, December 1988.
2. Mathsoft, Inc. "MathCAD User's Guide", 1987.

BIOGRAPHY

Jahangir Ghajar Dowlatshahi
Unisys Corporation,
Computer Systems Division (CSD),
Unisys Park, 3333 Pilot Knob Road,
Eagan, MN 55121

Jahangir Dowlatshahi is a Principal Electrical Engineer at the System Effectiveness Group, Computer Systems Division, Unisys, Minnesota. His duties, among others, include reliability modeling of complex fault tolerant systems. He received his B.Sc. in Electrical Engineering from Peshawar University, Pakistan, and M.Sc. in Nuclear Engineering from Imperial College of Science and Technology, London University, England. Currently he is pursuing a Master of Science degree in Software Design and Development at the College of St. Thomas, in St. Paul, Minnesota. Since 1979 he has been working in the area of Reliability and Maintainability Engineering.