

Chapter 18

Markov Analysis

18.1 INTRODUCTION

Markov analysis (MA) is an analysis technique for modeling system state transitions and calculating the probability of reaching various system states from the model. MA is a tool for modeling complex system designs involving timing, sequencing, repair, redundancy, and fault tolerance. MA is accomplished by drawing system state transition diagrams and examining these diagrams for understanding how certain undesired states are reached and their relative probability. MA can be used to model system performance, dependability, availability, reliability, and safety. MA describes failed states and degraded states of operation where the system is either partially failed or in a degraded mode where some functions are performed while others are not.

Markov chains are random processes in which changes occur only at fixed times. However, many of the physical phenomena observed in everyday life are based on changes that occur continuously over time. Examples of these continuous processes are equipment breakdowns, arrival of telephone calls, and radioactive decay. Markov processes are random processes in which changes occur continuously over time, where the future depends only on the present state and is independent of history. This property provides the basic framework for investigations of system reliability, dependability, and safety. There are several different types of Markov processes. In a semi-Markov process, time between transitions is a random variable that depends on the transition.

18.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT) and should be used as a supplement to the SD-HAT analysis. Refer to Chapter 3 for a description of the analysis types. The purpose of MA is to provide a technique to graphically model and evaluate systems components in order to resolve system reliability, safety, and dependency issues. The graphical model can be translated into a mathematical model for probability calculations. The strength of MA is its ability to precisely model and numerically evaluate complex system designs, particularly those involving repair and dependencies.

Markov analysis can be used to model the operation, or failure, of complex system designs. MA models can be constructed on detailed component designs or at a more abstract subsystem design level. MA provides a very detailed mathematical model of system failure states, state transitions, and timing. The MA model quickly becomes large and unwieldy as system size increases and is, therefore, usually used only on small system applications or systems abstracted to a smaller more manageable model.

Markov analysis can be applied to a system early in development and thereby identify design issues early in the design process. Early application will help system developers to design in safety and reliability of a system during early development rather than having to take corrective action after a test failure or, worse yet, a mishap.

Markov analysis is a somewhat difficult technique to learn, understand, and master. A high-level understanding of mathematics is needed to apply the methodology. The technique must be mastered, the material understood, and there must be detailed requisite knowledge of the process being modeled. MA generally requires an analyst very experienced with the technique and the mathematics involved.

Although a very powerful analysis tool, MA does not appear to provide a strong benefit to the system safety analyst as do other analysis tools that are available. It is more often used in reliability for availability modeling and analysis. MA does not identify hazards; its main purpose is to model state transitions for better understanding of system operation and calculating failure state probabilities. MA models can quickly become excessively large and complex, thereby forcing simplified models of the system. MA is recommended primarily only when extremely precise probability calculations are required.

Fault tree analysis (FTA) is recommended for most analysis applications because the fault tree combinatorial model is easier to generate from the system design, and the resulting probability calculations are equal or very close to results from MA models. FTA can be used to model extremely large complex systems, which would be impossible by MA.

18.3 HISTORY

Markov chain theory derives its name from the Russian mathematician Andrei A. Markov (1856–1922), who pioneered a systematic investigation of

mathematically describing random processes. The semi-Markov process was introduced in 1954 by Paul Levy to provide a more general model for probabilistic systems.

18.4 DEFINITIONS

In order to facilitate a better understanding of MA, some definitions for specific terms are in order. The following are basic MA terms:

State Condition of a component or system at a particular point in time (i.e., operational state, failed state, degraded state, etc.).

Connecting edge Line or arrow that depicts a component changing from one system state to a different state, such as transitioning from an operational state to a failed state.

State transition diagram State transition diagram is a directed graph representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which are used for probability calculations. The state transition diagram is the backbone of the technique.

Combinatorial model Graphical representation of a system that logically combines system components together according to the rules of the particular model. Various types of combinatorial models available include reliability block diagrams (RBDs), fault trees (FTs), and success trees. In MA the state transition diagram is the combinatorial model.

Deterministic process Deterministic process or model predicts a single outcome from a given set of circumstances. A deterministic process results in a sure or certain outcome and is repeatable with the same data. A deterministic model is sure or certain and is the antonym of random.

Stochastic process A stochastic process or model predicts a set of possible outcomes weighted by their likelihoods or probabilities. A stochastic process is a random or chance outcome.

Markov chain Sequence of random variables in which the future variable is determined by the present variable but is independent of the way in which the present state arose from its predecessors (the future is independent of the past given the present). The Markov chain assumes discrete states and a discrete time parameter, such as a global clock.

Markov process Assumes states are continuous. The Markov process evaluates the probability of jumping from one known state into the next logical state until the system has reached the final state. For example, the first state is everything in the system working, the next state is the first item failed, and this continues until the final system failed state is reached. The behavior of this process is that every state is memoryless, meaning that the future state of the system

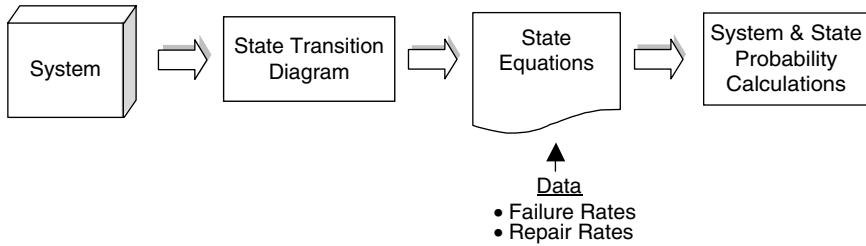


Figure 18.1 MA process.

depends only on its present state. In a stationary system the probabilities that govern the transitions from state to state remain constant, regardless of the point in time when the transition occurs.

Semi-Markov process Similar to that of a pure Markov model, except the transition times and probabilities depend upon the time at which the system reached the present state. The semi-Markov model is useful in analyzing complex dynamical systems and is frequently used in reliability calculations.

18.5 THEORY

Markov analysis utilizes a state transition diagram or directed graph that portrays in a single diagram the operational and failure states of the system. The state diagram is flexible in that it can serve equally well for a single component or an entire system. The diagram provides for representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which when resolved provide the probability calculations for each state. Figure 18.1 illustrates the overall MA process.

18.6 METHODOLOGY

Table 18.1 lists and describes the basic steps of the MA process.

18.6.1 State Transition Diagram Construction

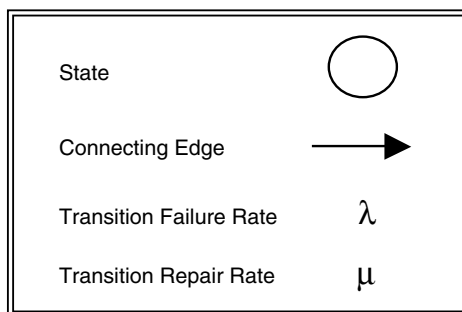
Although the basic rules guiding the construction of a state diagram are simple, a good understanding of the system being analyzed is necessary. Construction of a state diagram begins with an examination of the system and a determination of the possible states in which it may exist. Figure 18.2 shows the symbols utilized in MA modeling.

TABLE 18.1 MA Process

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, and interfaces.
2	Identify the system states.	Establish the goals of the MA and determine the system and component states of interest.
3	Construct state diagram.	Construct the state diagram for all of the identified system states. Show the transitions between states and transition rates.
4	Develop mathematical equations.	Develop the mathematical equations from the state diagram.
5	Solve mathematical equations.	Solve the mathematical equations through manual or computer techniques.
6	Evaluate the outcome.	Evaluate the outcome of the MA analysis.
7	Recommend corrective action.	Make recommended design changes as found necessary from the MA analysis.
8	Hazard tracking.	Enter identified hazards, or hazard data, into the hazard tracking system (HTS).
9	Document MA.	Document the entire MA process, including state diagrams, equations, transition rates, and mathematical solution.

Specifically, the state diagram is constructed as follows:

1. Begin at the left of the diagram with a state (circle) identified as S1. All equipment is initially good (operational) in this state.
2. Study the consequences of failing each element (any component, circuit, or channel defined as a single failure) in each of its failure modes. Group as a common consequence any that result in removing the same or equivalent circuitry from operation.
3. Assign new states (circles) and identify as S2, S3, S4, and so on for the unique consequences of step 2.

**Figure 18.2** MA symbols.

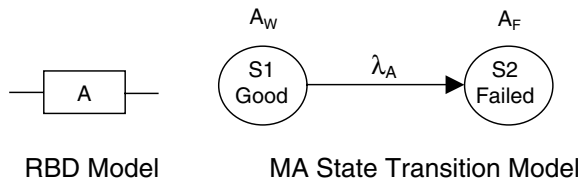


Figure 18.3 MA model—one-component system with no repair.

4. Connect arrows from S1, to each of the new states, and note on each arrow the failure rate or rates of the element or elements whose failure determined transition to the new state.
5. Repeat steps 2, 3, and 4 for each of the new states failing only the elements still operational in that state. Continuously observe for cases where the failures may cause transition to one of the states formerly defined.
6. Continue the process until the initial equipment is totally nonoperational.

To limit the state diagram to a reasonable size, without a major sacrifice in accuracy, longer paths between the initial operational state and the system failure state may be truncated. For example, if one path to a system failure consists of three transitions and another is five transitions, then the longer path may be truncated. The effect of this approximation must be examined in the final model to ensure minimal impact.

Figure 18.3 shows an example MA state transition model for a one-component system with no repair. The reliability block diagram (RBD) shows the system design complexity. In this MA model only two states are possible, the operational state and the failed state. The starting state is S1 in which the system is operational (good). In state S2 the system is failed. The transition from state S1 to state S2 is based on the component failure rate λ_A . Note that A_W indicates component A working and A_F indicates component A failed. The connecting edge with the notation λ_A indicates the transitional failure of component A.

Figure 18.4 shows an example MA model for a one-component system with repair. Note how component A can return from the failed stated to the operational state at the repair transition rate μ_A .

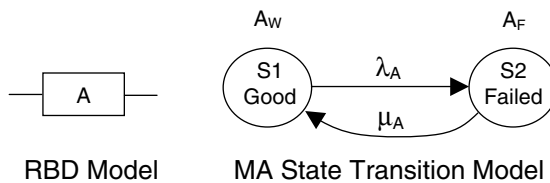


Figure 18.4 MA model—one-component system with repair.

$\dot{\underline{P}} = [A]\underline{P}$	Where \underline{P} and \underline{P} are $n \times 1$ column vectors and $[A]$ is an $n \times n$ matrix.
$\underline{P} = \exp[A]t \bullet \underline{P}(0)$	Where $\exp[A]t$ is an $n \times n$ matrix and $\underline{P}(0)$ is the initial probability vector describing the initial state of the system.

Figure 18.5 Markov state equations.

18.6.2 State Equation Construction

A stochastic processes is a random process controlled by the laws of probability that involve the “dynamic” part of probability theory, which includes a collection of random variables, their interdependence, their change in time, and limiting behavior. The most important variables in analyzing a dynamic process are those of rate and state. MA models are representations of a stochastic process.

A Markov process is completely characterized by its transition probability matrix, which is developed from the transition diagram. In safety and reliability work, events involve failure and repair of components. The transitional probabilities between states are a function of the failure rates of the various system components. A set of first-order differential equations is developed by describing the probability of being in each state in terms of the transitional probabilities from and to each state. The number of first-order differential equations will equal the number of system states. The mathematical formula is shown in Figure 18.5 and the solution then becomes one of solving the differential equations.

Figure 18.6 shows a Markov transition diagram for a two-component system comprised of components A and B. A_W indicates component A working and A_F indicates component A failed. States S1, S2, and S3 are noted a “good,” indicating

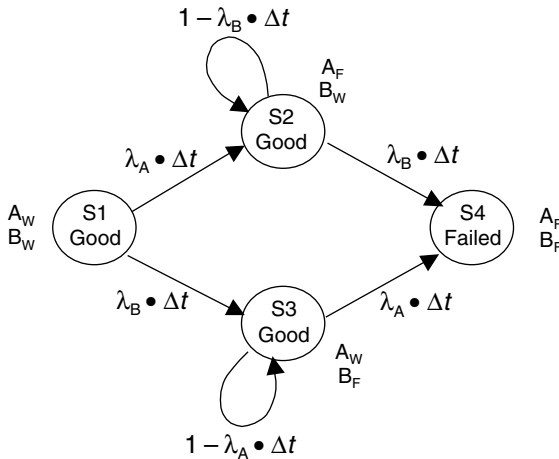


Figure 18.6 Markov transition diagram—two-component system.

the system is operational. State S4 is noted as “failed,” meaning the system is now in the failed state.

The Markov differential equations are developed by describing the probability of being in each system state at time $t + \Delta t$ as a function of the state of the system at time t . The probability of being in state S1 at some time $t + \Delta t$ is equal to the probability of being in state S1 at time t and not transitioning out during Δt . This equation can be written as:

$$P_1(t + \Delta t) = P_1(t) \cdot [1 - (\lambda_A + \lambda_B) \cdot \Delta t]$$

The probability of being in state S2 at time $t + \Delta t$ is equal to the probability of being in state S1 at time t and transitioning to state S2 in Δt plus the probability of being in state S2 at time t and not transitioning out during Δt . This equation can be written as:

$$P_2(t + \Delta t) = P_1(t) \cdot \lambda_A \cdot \Delta t + P_2(t)(1 - \lambda_B \cdot \Delta t)$$

All of the state equations are generated in a similar manner, resulting in the following equations:

$$\begin{aligned} P_1(t + \Delta t) &= P_1(t) \cdot [1 - (\lambda_A + \lambda_B) \cdot \Delta t] \\ P_2(t + \Delta t) &= P_1(t) \cdot \lambda_A \cdot \Delta t + P_2(t)(1 - \lambda_B \cdot \Delta t) \\ P_3(t + \Delta t) &= P_1(t) \cdot \lambda_B \cdot \Delta t + P_3(t)(1 - \lambda_A \cdot \Delta t) \\ P_4(t + \Delta t) &= P_2(t) \cdot \lambda_B \cdot \Delta t + P_3(t) \cdot \lambda_A \cdot \Delta t + P_4(t) \end{aligned}$$

Rearranging the equations results in:

$$\begin{aligned} [P_1(t + \Delta t) - P_1(t)]/\Delta t &= -(\lambda_A + \lambda_B) \cdot P_1(t) \\ [P_2(t + \Delta t) - P_2(t)]/\Delta t &= \lambda_A \cdot P_1(t) - \lambda_B \cdot P_2(t) \\ [P_3(t + \Delta t) - P_3(t)]/\Delta t &= \lambda_B \cdot P_1(t) - \lambda_A \cdot P_3(t) \\ [P_4(t + \Delta t) - P_4(t)]/\Delta t &= \lambda_B \cdot P_2(t) + \lambda_A \cdot P_3(t) \end{aligned}$$

Taking the limit as $\Delta t \rightarrow 0$ results in:

$$\begin{aligned} dP_1(t)/\Delta t &= -(\lambda_A + \lambda_B) \cdot P_1(t) \\ dP_2(t)/\Delta t &= \lambda_A \cdot P_1(t) - \lambda_B \cdot P_2(t) \\ dP_3(t)/\Delta t &= \lambda_B \cdot P_1(t) - \lambda_A \cdot P_3(t) \\ dP_4(t)/\Delta t &= \lambda_B \cdot P_2(t) + \lambda_A \cdot P_3(t) \end{aligned}$$

In matrix form this becomes:

$$\begin{pmatrix} dP_1(t)/\Delta t \\ dP_2(t)/\Delta t \\ dP_3(t)/\Delta t \\ dP_4(t)/\Delta t \end{pmatrix} = \begin{pmatrix} -(\lambda_A + \lambda_B) & 0 & 0 & 0 \\ \lambda_A & -\lambda_B & 0 & 0 \\ \lambda_B & 0 & -\lambda_A & 0 \\ 0 & \lambda_B & \lambda_A & 0 \end{pmatrix} \cdot \begin{pmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{pmatrix}$$

Solution of these equations provides the probability of being in each state.

18.7 EXAMPLES

18.7.1 Markov Chain

A Markov model can look at a long sequence of rainy and sunny days and analyze the likelihood that one kind of weather is followed by another kind. Let us say it was found that 25 percent of the time, a rainy day was followed by a sunny day, and 75 percent of the time a rainy day was followed by more rain. Additionally, sunny days were followed 50 percent of the time by rain and 50 percent by sun. Given this data, a new sequence of statistically similar weather can be generated from the following steps:

1. Start with today's weather.
2. Given today's weather, choose a random number to pick tomorrow's weather.
3. Make tomorrow's weather "today's weather" and go back to step 2.

A sequence of days would result, which might look like:

Sunny–Sunny–Rainy–Rainy–Rainy–Rainy–Sunny–Rainy–
Rainy–Sunny–Sunny . . .

The "output chain" would statistically reflect the transition probabilities derived from observed weather. This stream of events is called a Markov chain.

18.7.2 Markov Model of Two-Component Series System with No Repair

Figure 18.7 shows an example MA model for a two-component series system with no repair. The RBD indicates that successful system operation requires successful operation of both components A and B. If either component fails, the system fails.

In this MA model two states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. Transition to state S2 occurs when either A fails or B fails. In state S2, either A and B are failed and the system is failed.

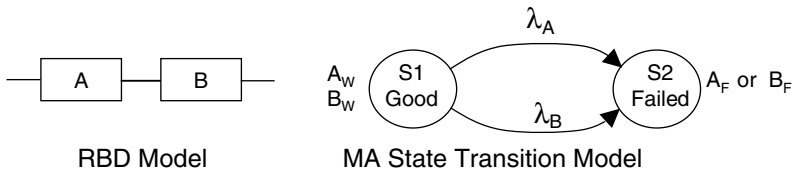


Figure 18.7 MA model—two-component series system with no repair.

18.7.3 Markov Model of Two-Component Parallel System with No Repair

Figure 18.8 shows an example MA model for a two-component parallel system with no repair. The RBD indicates that successful system operation only requires successful operation of either component A or B. Both components must fail to result in system failure.

In this MA model four states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. Based on A failure rate λ_A , it transitions to the failed state S2. In state S2, A is failed, while B is still good. In state S3, B is failed, while A is still good. In state S4, both A and B are failed. In states S1, S2, and S3 the system is good, while in state S4 the system is failed.

18.7.4 Markov Model of Two-Component Parallel System with Component Repair

Figure 18.9 shows the MA model for a two-component parallel system with component repair but no system repair. As in the previous figure, this MA model has four possible states. In this system design and MA model, if the system transitions to state S2, but A is repaired before B fails, then the system is returned to state S1.

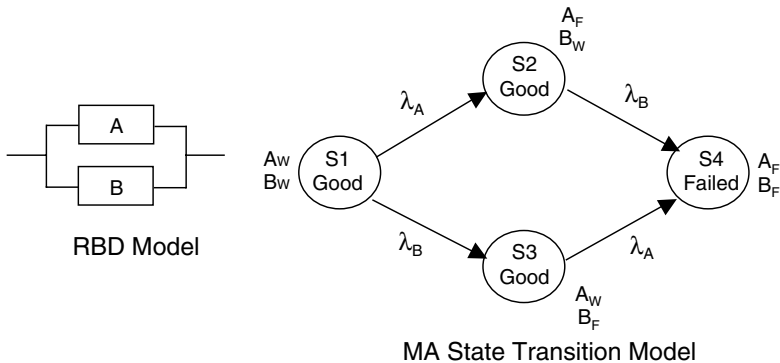


Figure 18.8 MA model—two-component parallel system with no repair.

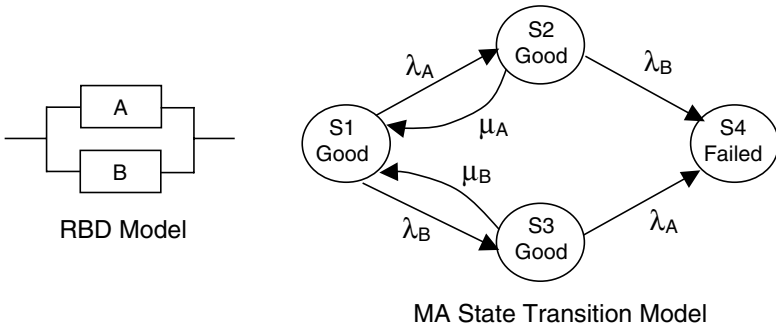


Figure 18.9 MA model—two-component parallel system with component repair.

Conversely, if the system is in state S3, the system returns to state S1 if component B is repaired before component A fails. The connecting edge with the notation μ_A indicates repair of component A, and μ_B indicates repair of component B.

18.7.5 Markov Model of Two-Component Parallel System with Component/System Repair

Figure 18.10 shows the MA model for a two-component parallel system with component repair and/or system repair. In this system design, even after system failure occurs, one or both components can be repaired, thereby making the system operational again.

As in the previous figure, this MA model has four possible states. In this system design, and corresponding MA model, if the system transitions to state S2, but A is repaired before B fails, then the system is returned to state S1. Conversely, if the system is in state S3, the system returns to state S1 if component B is repaired before component A fails. If state S4 is reached, the system can be repaired through repair of A and/or B.

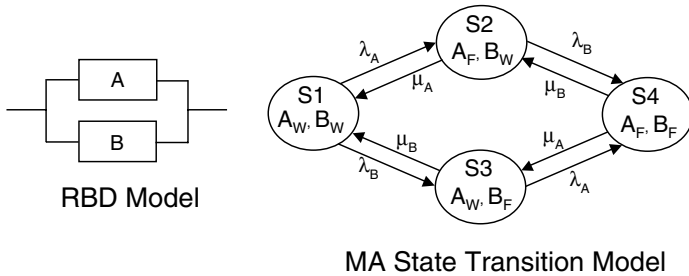


Figure 18.10 MA model—two-component parallel system with system/component repair.

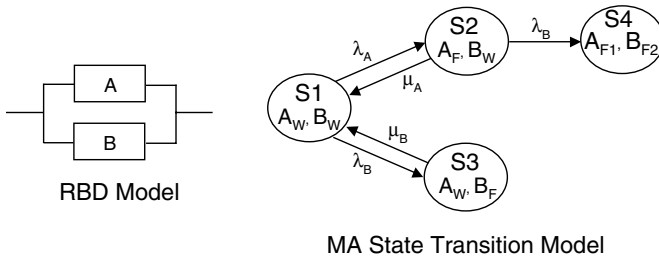


Figure 18.11 MA model—two-component parallel system with sequencing.

18.7.6 Markov Model of Two-Component Parallel System with Sequencing

Figure 18.11 shows the MA model for a two-component parallel system where system failure only occurs when the components fail in a specific sequence. In this system design, A monitors B such that if B fails, the fault is detected by A and is immediately repaired. If A fails before B, then it cannot detect failure of B and initiate the repair of B and system failure occurs. Note that this model assumes that B is always repaired before A can fail, thereby maintaining an operational system.

In this MA model four states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. In state S3 component B has failed while A is still working. In this state repair is the only option, thereby taking the system back to state S1. In state S2 component A is failed while B is working. If A is repaired before B fails, the system can be restored to state S1, otherwise the system will continue to operate until component B fails, thereby taking the system to state S4, which is system failure.

18.8 MARKOV ANALYSIS AND FTA COMPARISONS

Markov analysis and FTA are often competing techniques. Each technique has its advantages and disadvantages. This section demonstrates both MA and FTA models and probability calculations for the same system design complexities. Comparing the two methods side by side helps to illustrate some of the strengths and weaknesses of each methodology.

Figure 18.12 compares MA and FTA for a two-component series system. The conclusion from this comparison is that both methods provide the same results (i.e., the equations are identical). For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.

Figure 18.13 compares MA and FTA for a two-component parallel system. The conclusion from this comparison is that both methods provide the same results (i.e., the equations are identical). For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.

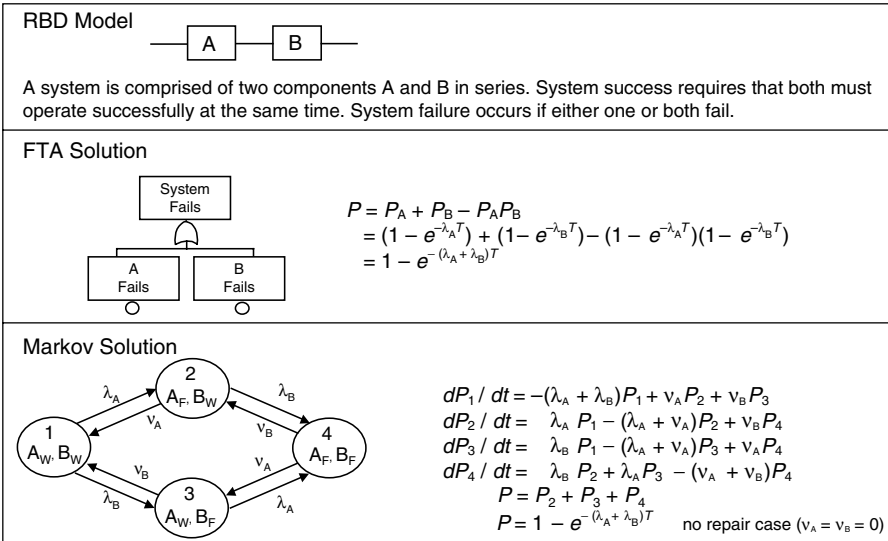


Figure 18.12 MA and FTA comparison for a two-component series system.

Figure 18.14 compares MA and FTA for a two-component sequence parallel system. The conclusion from this comparison is that the resulting equations for each model are different. The FT equation is an approximation. The numerical comparison table shows calculations for different time intervals using the same failure rates. The results contained in this table show that the two models produce very close

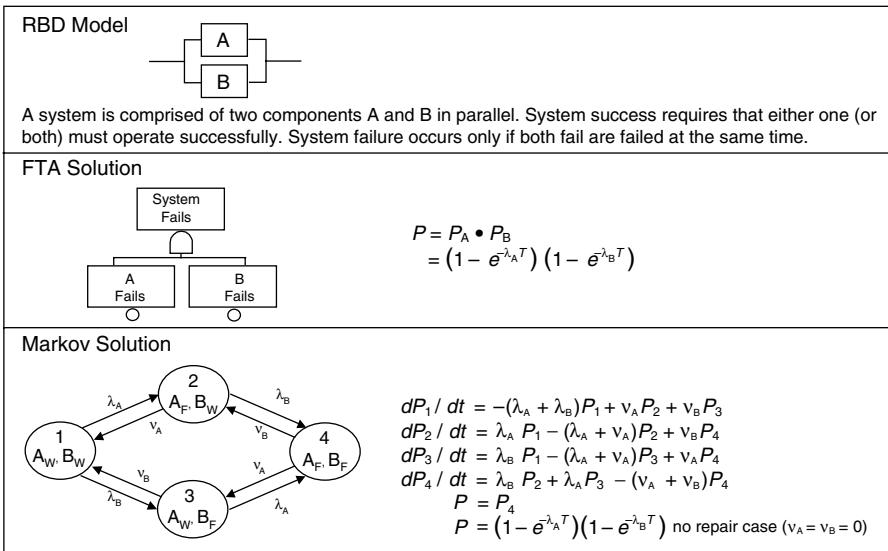


Figure 18.13 MA and FTA comparison for a two-component parallel system.

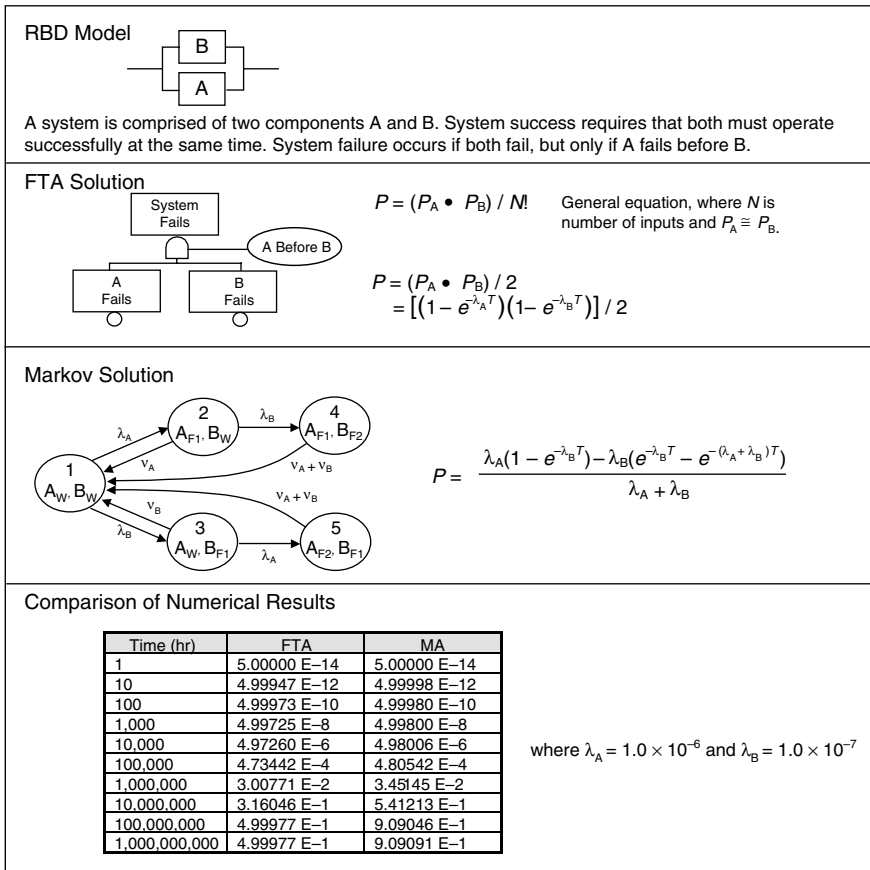
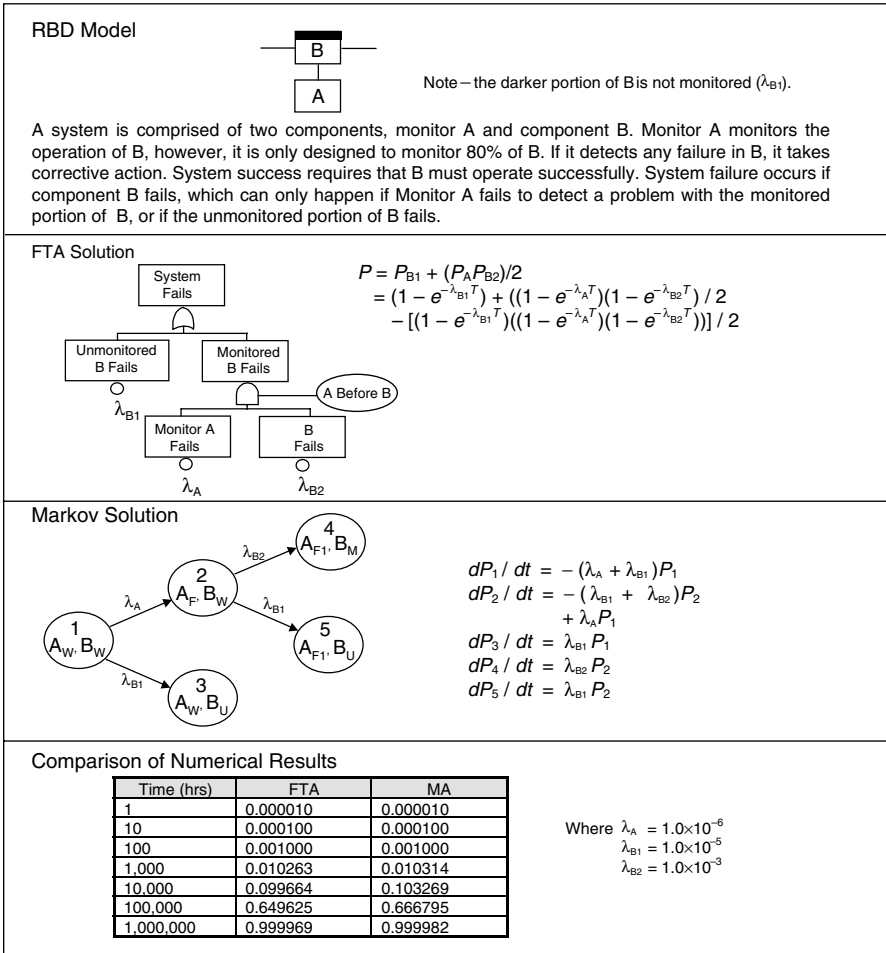


Figure 18.14 MA and FTA comparison for a two-component sequence parallel system.

results up to about 1 million hours of operation. This indicates that the FTA approximation produces very good results. For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.

Figure 18.15 compares MA and FTA for a partial monitor with coverage system. This is a coverage-type problem, whereby the monitor does not provide complete coverage of the circuit being monitored.

The conclusion from this comparison is that the resulting equations for each model are different. The FT equation is an approximation. The numerical comparison table shows calculations for different time intervals using the same failure rates. The results contained in this table show that the two models produce very close results up to about 10,000 hours of operation. This indicates that the FTA approximation produces very good results. For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.



4. There are commercial software packages available to assist in MA modeling and probability calculations.

Although a strong and powerful technique, MA analysis has the following disadvantages:

1. MA does not identify system hazards; it only evaluates identified hazards in more detail.
2. MA is not a root cause analysis tool. It is a tool for evaluating the most effective methods for combining components together.
3. MA requires an experienced analyst to generate the graphical models and probability calculations.
4. The MA model quickly becomes large and complex; thus it is more limited to small systems or a high-level system abstraction.

18.10 COMMON MISTAKES TO AVOID

When first learning how to perform an MA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an MA:

1. Not obtaining the necessary training.
2. Using the complex MA technique when a simpler technique, such as FTA, might be more appropriate.
3. Failing to recognize that the transitions (probabilities) of changing from one state to another are assumed to remain constant. Thus, a Markov model is used only when a constant failure rate and repair rate assumption is justified.
4. Failing to recognize that the transition probabilities are determined only by the present state and not the system's history. This means future states of the system are assumed to be independent of all but the current state of the system. The Markov model allows only the representation of independent states.

18.11 SUMMARY

This chapter discussed the MA technique. The following are basic principles that help summarize the discussion in this chapter:

1. MA is a tool for modeling complex system designs involving timing, sequencing, repair, redundancy, and fault tolerance.
2. MA provides both graphical and mathematical (probabilistic) system models.

3. MA models can easily become too large in size for comprehension and mathematical calculations, unless the system model is simplified. Computer tools are available to aid in analyzing more complex systems.
4. MA is recommended only when very precise mathematical calculations are necessary.
5. MA should be a supplement to the SD-HAT analysis.

BIBLIOGRAPHY

- Ericson, C. A. and J. D. Andrews, Fault Tree and Markov Analysis Applied to Various Design Complexities, Proceedings of the 18th International System Safety Conference, 2000, pp. 324–335.
- Faraci, V., Jr., Calculating Probabilities of Hazardous Events (Markov vs. FTA), Proceedings of the 18th International System Safety Conference, 2000, pp. 305–323.
- International Electrotechnical Commission, IEC 61165, Application of Markov Techniques, 1995.
- Pukite, J. and P. Pukite, *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety and Supportability Analyses of Complex Computer Systems*, IEEE Press, 1998.