LLNL-CONF-402910

LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Application of RAM to Facility/Laboratory Design

K. Mohammadi

April 14, 2008

EFCOG 2008 Safety Analysis Workshop
Richland, WA, United States
May 3, 2008 through May 8, 2008

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Application of RAM to Facility/Laboratory Design

Kazem Mohammadi
Safety Analysis Engineer
Safety Basis Division
Nuclear Operations Directorate
Lawrence Livermore National Laboratory
P.O. Box 808 (L-372)
Livermore, CA 94551
Phone (925) 423-5795/Fax (925) 423-1787
Mohammadi2@llnl.gov

Abstract

Reliability, Availability, and Maintainability (RAM) studies are extensively used for mission critical systems (e.g., weapons systems) to predict the RAM parameters at the preliminary design phase. A RAM methodology is presented for predicting facility/laboratory inherent availability (i.e., availability that only considers the steady-state effects of design) at the preliminary design phase in support of Department of Energy (DOE) Order 430.1A (Life Cycle Asset Management) and DOE Order 420.1B (Facility Safety). The methodology presented identifies the appropriate system-level reliability and maintainability metrics and discusses how these metrics are used in a fault tree analysis for predicting the facility/laboratory inherent availability. The inherent availability predicted is compared against design criteria to determine if changes to the facility/laboratory preliminary design are necessary to meet the required availability objective in the final design.

Introduction

Understanding the structure of a facility's life-cycle cost during design phase is paramount to successful mission of the facility. Life-cycle cost of a facility is defined as all costs related to land acquisition, design, construction, operation, maintenance, and decommissioning. Operation and maintenance costs, which typically comprise a large portion of the overall life-cycle cost, are greatly influenced by the facility's original design. Application of Reliability, Availability, and Maintainability (RAM) analysis at the preliminary design phase can help determine the degree to which reliability and maintainability are incorporated into facility design. Comparison of analysis results to design criteria can help determine if changes to the preliminary design are necessary to meet the required availability objective in the final design and to optimize the overall facility life-cycle cost.

This paper presents a RAM methodology using fault tree technique for predicting facility/laboratory inherent availability at the preliminary design phase in support of DOE Order 430.1A (Life Cycle Asset Management)[1] and DOE Order 420.1B (Facility Safety).[2]

RAM Parameters Defined

Reliability is the probability that a component or system will perform a required function for a given period of time when used under stated operating conditions.[3] The reliability metric typically used for components and systems when evaluating a facility's inherent availability at design phase is Mean Time Between Failures (MTBF) or failure rate (λ) which is the inverse of MTBF (λ = 1/MTBF). Since most failures during useful life of a component or system (steady-state condition) are random, it is typically assumed that the MTBF and λ values during this period remain constant. This is depicted in the classic bathtub curve provided in Figure 1 below.

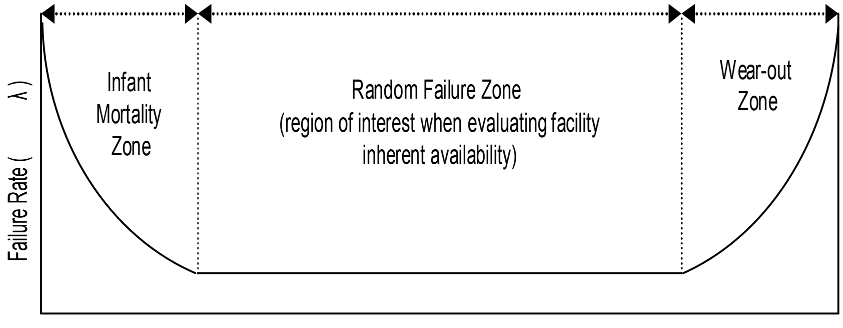

Figure 1 – Bathtub Curve.

M*aintainability* (M) is the probability that a failed component or system will be restored or repaired to a specified condition within a period of time when maintenance is performed in accordance with prescribed procedures.[3] The maintainability metric typically used for components and systems when evaluating a facility's inherent availability at design phase is Mean Time To Repair (MTTR) or repair rate (μ) which is the inverse of MTTR (μ = 1/MTTR). The repair time is considered to be an inherent design feature of a system or component and includes time factors related to accessibility, diagnosis, repair or replacement, and verification of proper operation (time factors related to administrative delays are excluded). During the useful life (steady-state condition) of a component or system, the MTTR and μ values are expected to remain constant if the design of the facility is not going to change.

Availability is the probability that a component or system is performing its required function at a given point in time or over a stated period of time when operated and maintained in a prescribed manner.[3] Availability is a function of both reliability and maintainability. When evaluating a preliminary design, *Inherent Availability* is the parameter of interest. This availability only considers steady-state reliability and corrective maintenance (or repair) effects of a component or system and thus is solely a function of the inherent design characteristics and is defined as:

$$A = MTBF/(MTBF+MTTR)$$

This equation shows that the same availability can be achieved with different levels of reliability (MTBF) and maintainability (MTTR). With higher reliability, lower levels of maintainability are needed to achieve the same availability and vice versa.

Relationship to Safety Analysis

The relationship of RAM to safety analysis is best illustrated using the event tree shown in Figure 2. This event tree represents a simple accident with an initiating event and two systems (Systems A and B) that provide preventive and/or mitigating functions in response to the event. The failure probabilities of System A and B are denoted by P_A and P_B, respectively. Since an initiating event can result from hardware failure or human error, it can be discerned that incorporating sound reliability and maintainability principles in design can lower the initiating event frequency (IE_f) and thus lower the sequence frequencies. Similarly, incorporating sound reliability and maintainability principles in design of preventive and mitigative systems will lower their failure probabilities (P_A and P_B) and thus additionally reduce the sequence frequencies. Also, any design changes resulting from a RAM analysis could potentially provide consequence reductions. Reductions in sequence frequencies and consequences would then lower the overall risk.

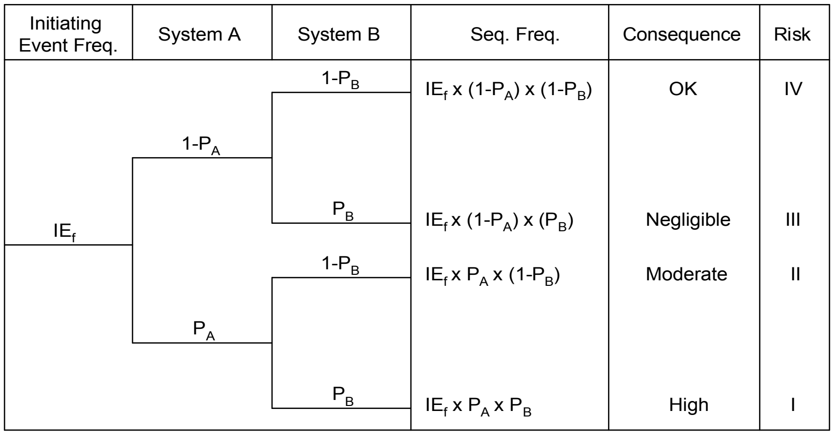

Figure 2 – Event Tree Representation of an Accident.

Analysis Approach

The overall approach for evaluating the inherent availability of a facility's preliminary design is depicted in Figure 3. A brief discussion of the main elements is provided below.

Facility Mission

The facility mission and the duration of the mission must be properly defined at the beginning of the analysis. Facilities could have one or more missions with different availability requirements. For example, a facility could have an Operating Mode reflecting the purpose for which the facility is designed for as well as a secondary mission to provide prevention and mitigation capabilities in response to abnormal events and accidents (Event Mode). The inherent availability requirement for all facility missions must be defined. This is typically a requirement that is imposed by the facility owner/user (e.g., DOE) on the architect engineer designing the facility. Inherent availability requirement are usually specified in terms of number of hours per year or a percentage (e.g., 95%) on annual basis.

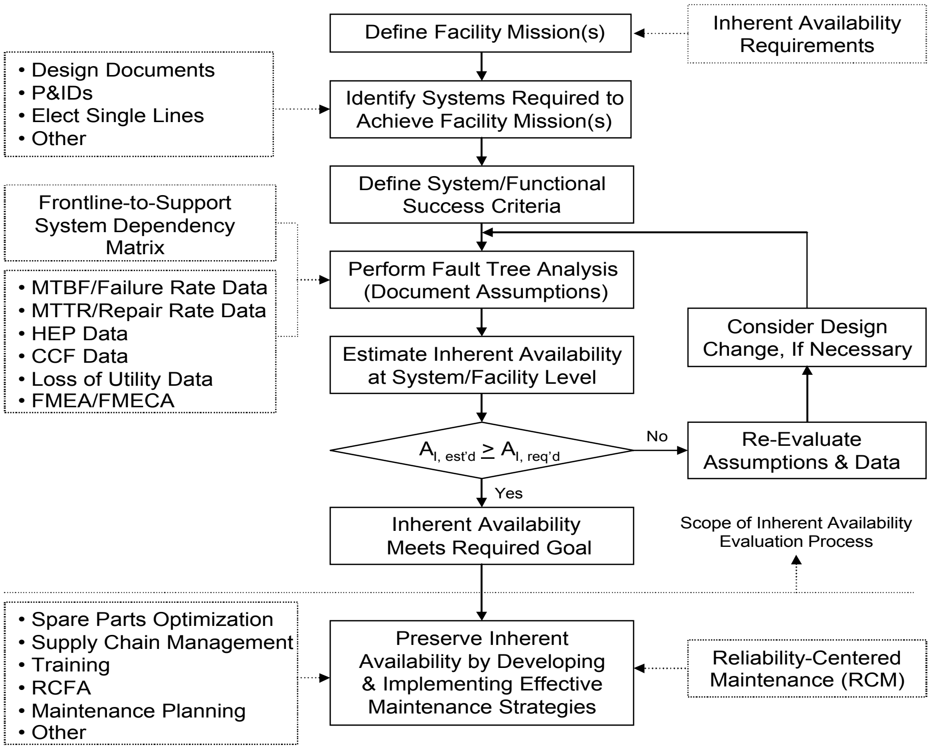
Define Facility Mission(s)
Inherent Availability Requirements
• Design Documents
• P&IDs
• Elect Single Lines
• Other
Identify Systems Required to Achieve Facility Mission(s)
Define System/Functional Success Criteria
Frontline-to-Support System Dependency Matrix
• MTBF/Failure Rate Data
• MTTR/Repair Rate Data
• HEP Data
• CCF Data
• Loss of Utility Data
• FMEA/FMECA
Perform Fault Tree Analysis (Document Assumptions)
Consider Design Change, If Necessary
Estimate Inherent Availability at System/Facility Level
$A_{I,\ est'd} \geq A_{I,\ req'd}$
No
Re-Evaluate Assumptions & Data
Yes
Inherent Availability Meets Required Goal
Scope of Inherent Availability Evaluation Process
• Spare Parts Optimization
• Supply Chain Management
• Training
• RCFA
• Maintenance Planning
• Other
Preserve Inherent Availability by Developing & Implementing Effective Maintenance Strategies
Reliability-Centered Maintenance (RCM)

Figure 3 – Facility Inherent Availability Evaluation Process.

Systems Required for Mission Success

A facility is a collection of systems which work in concert to perform a certain mission. The initial phase of the evaluation requires identification of all facility systems that are required to achieve mission success for each mission. These systems are those whose failure would put the facility in repair mode and thus render it unavailable. To this end, a review of design documents is essential to ensure proper understanding of the facility, systems, and interactions between systems.

Systems are either front-line or support. A front-line system is a system (e.g., ventilation system, fire detection and suppression system) that directly supports the facility mission(s). A support system is a system that supports one or more front-line systems (e.g., instrument air system). For both front-line and support systems, the functional success criteria and the minimum number of equipment required for functional success (e.g., 1 out of 2 fans, instrument air availability) must be defined. A dependency matrix similar to what is shown in Figure 4 could be developed to establish the relationship between the front-line and support systems. This will act as a guide to ensure that system interactions are properly modeled.

		Frontline Systems					
		System A	System B	System C	System D	System E	System F
Support Systems	System G				X		X
	System H			X		X	
	System I	X			X		
	System J		X				
	System K	X		X		X	X
	System L		X		X		

Figure 4 – Frontline-to-Support Dependency Matrix

For all front-line and support systems the mechanical, electrical, and instrumentation and control (I&C) boundaries must also be defined. This is important since certain components or systems may be omitted from the analysis due to contractual reasons, passive nature of some of the components/systems, or lack of availability of resources. Structural and piping systems are typically omitted due to their passive nature and the higher reliability associated with these systems. Additionally, conditions that can result in failure of structures are usually beyond the normal operating environment of the facility. Exclusion of these systems is not expected to change the outcome of the analysis.

Availability Prediction Using Fault Tree Analysis (FTA)

A number of techniques such as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), and Markov Analysis (MA) are available that can be used for RAM modeling. FTA is a top-down, deductive, technique that graphically depicts the combination of failures that can lead to an undesirable event through use of logical connections (e.g., OR Gate, AND Gate, Transfers).[9] The RBD technique shows the logical connections between components of the system using block representation of component reliability. FTA perspective is on faults and failures (unreliability/unavailability), whereas RBD works in the success space (reliability/availability). MA looks at a system as being in one of several states (e.g., all components operating, one component failed, two components failed, all components failed) with the objective to find the probability of the system being in each state. The reader is referred to References 3 and 9 for additional detail on FTA, RBD, and MA techniques.

Traditionally, the FTA and RBD tools have been only capable of modeling combinatorial systems (i.e., those in which failures are not sequence dependent). Additionally, these tools have had difficulty capturing the component repair events necessary for availability prediction. MA on the other hand allows for proper treatment of sequence dependent failures and repair events and can be used in both combinatorial and non-combinatorial systems. The complexity associated with MA, however, is much higher than RBD and FTA and, therefore, it requires a much greater effort to perform, especially when dealing with large, multi-component, systems. Most FTA and RBD software tools available today are hybrid tools that integrate the FTA or RBD technique with MA so that sequence dependent events and repair events can be properly modeled.

This paper focuses on the use of FTA augmented with MA, as necessary, for inherent availability prediction. In FTA, facility unavailability is modeled through fault tree logical connections representing system unavailabilities, and systems unavailabilities are modeled using component unavailabilities represented by basic events under system logic.

A fault tree is developed for each facility mission when evaluating inherent unavailability. Mission unavailability is represented by the highest level gate in the fault tree called the top gate (see Figure 5). The logic under the top gate includes front-line system unavailabilities. These systems are those required to operate for mission success.

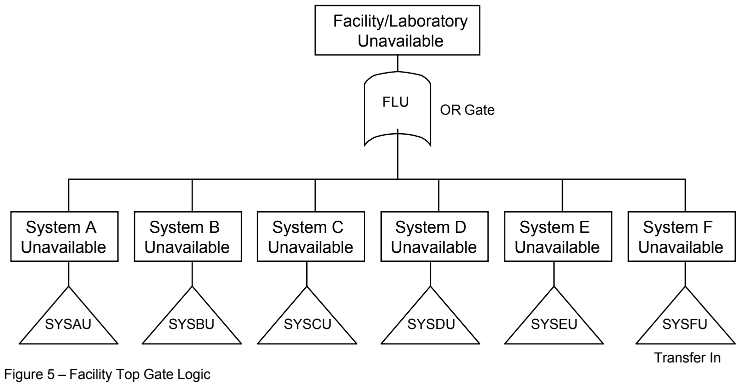

Figure 5 – Facility Top Gate Logic

A fault tree for each required system is developed and properly connected to the top gate (see Figure 6). The system success criteria discussed earlier will facilitate construction of the fault tree for each system. The knowledge of what is required for system success will help determine what can cause system failure.

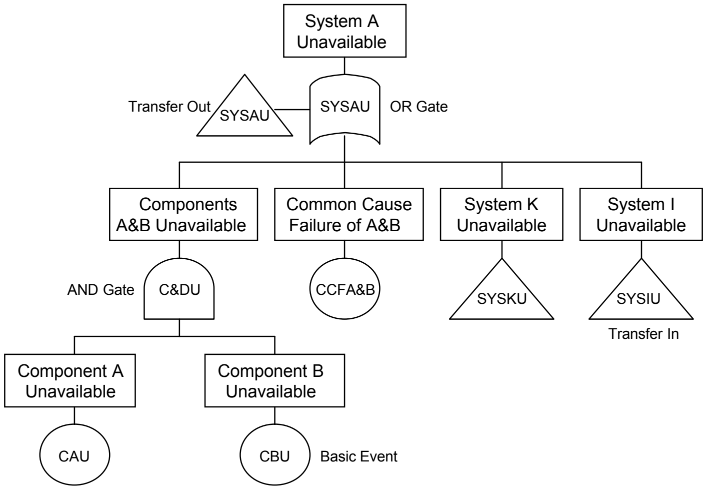

Figure 6 – System Fault Tree Model

The events at the lowest level in system fault trees represent equipment unavailabilities, human error probabilities, or external event-induced unavailabilities (e.g., loss of offsite power-induced unavailability, loss of natural gas-induced unavailability). It is essential that all assumptions made during fault tree modeling be documented.

Often times Failure Modes and Effects Analysis (FMEA) or Failure Modes and Effects Criticality Analysis (FMECA) are performed during the design phase with the objective of improving the design reliability. These analyses, if available, should be used to facilitate fault tree modeling.

The inherent unavailability for each facility mission is determined by quantifying the top gate for that facility mission. This is accomplished by quantification of all basic events via the system logic to determine system unavailability and then rolling up the system level results through the top level logic to determine the facility inherent unavailability. The inherent availability of the facility is the complement of the calculated inherent unavailability (or A = 1-U).

Treatment of Dependent Failures

FTA requires proper modeling of dependencies. Dependent failures (also referred to as common mode failures) are comprised of the following two types of failures:

- Internal (or Intrinsic), and
- External (or Extrinsic) (or Common Cause Failures).

Internal dependent failures include those related to support systems (e.g., instrument air) that can render front-line system(s) unavailable as well as single point failures that can impact redundant components or systems. Support system failures may affect one or more front-line systems and are directly modeled under the logic for the supported front-line system(s).

External dependent failures or common cause failures (CCF) are component failures that occur at the same time, or in a short time interval, due to a common external coupling factor (e.g., environment, maintenance, storage) disabling redundant components. Common cause failures can be important contributors to availability and thus their inclusion is important in modeling, when appropriate. Although a number of techniques exist for modeling of common cause failures[4], the two most widely used are the β-Factor Method and the Multiple Greek Letter (MGL) Method. Use of the simpler β-Factor Method is adequate in most cases. These techniques are not discussed in this paper.

Common cause failures can be explicitly modeled in the fault tree using basic events. Certain software tools allow for implicit modeling of common cause failures once the β values and common cause component groups are identified.

Fault Tree Basic Event Mathematical Modeling

It is essential that the mathematical modeling of each fault tree basic event be done properly based on the type of event modeled. Some typical models used for fault tree basic event quantification are discussed below. It should be noted that these models are not meant to be exhaustive and thus additional models may need to be used, as necessary, depending on the events that are modeled in the fault trees.

Most basic events in fault trees represent unavailability of repairable components (e.g., pumps, fans). These basic events are quantified using the following formulation derived using Markov Analysis for a single repairable component assuming constant failure and repair rates (λ and μ), both mean values:[3]

$$U_{mean} = (\lambda/(\lambda + \mu)) \times (1 - e^{-(\lambda + \mu)t})$$

For large values of time (t) (steady-state conditions), the exponential term drops out and the equation reduces to:

$$U_{mean} = \lambda/(\lambda + \mu) = MTTR/(MTBF + MTTR)$$

Basic events that represent steady-state unavailabilities of repairable components that are in standby with a protective function (e.g., interlocks) are quantified using the following formulation derived using Markov Analysis, where λ is mean failure rate (constant), MTTR is mean time to repair, and T represents the periodic inspection interval:[3]

$$U_{mean} = [\lambda T – (1 - e^{-\lambda T}) + \lambda MTTR\ (1 - e^{-\lambda T})]/[\lambda T + \lambda MTTR\ (1 - e^{-\lambda T})]$$

Standby components may not have their failures revealed until they are required to operate, or until inspection (test) takes place; only at these times repairs can be performed. The above formulation assumes perfect repair that restores the component to as good as new condition.

For standby components an estimation of the inspection interval at design phase is necessary for quantification of the associated basic events. For safety systems that are governed by IEC-61508 Standard[8], the inspection interval used in the above equation must be consistent with that determined as part of the safety integrity level (SIL) assessment performed under IEC-61508.

Basic events that represent unavailabilities of repairable components with mission times much shorter than the facility mission time and without the possibility of repair due to the short mission time are quantified using the following formulation, where λ is the mean failure rate (constant) and T represents the component mission time:[3]

$$U_{mean} = 1 – e^{-\lambda T}$$

This model is derived from the first equation above by setting μ to zero and is used for quantifying component unavailabilities that only contribute to system unavailability during certain phases of the facility mission.

Quantification of basic events that represent unavailabilities due to external initiators such as loss of offsite power or loss of natural gas supply to the facility require both the frequencies of the events as well as the mean duration of the events and are quantified using the following formulation:[10]

$$U_{mean} = \text{Frequency x Duration}$$

Basic events representing component unavailabilities due to common cause failures are quantified using the following formulation if the β-Factor Method is used, where λ is mean failure rate for the failure mode of interest and β is the fraction of the failure rate that is due to common causes:[4]

$$U_{mean} = \beta\lambda$$

Human actions (e.g., failure to isolate main line and use bypass line) are modeled in fault trees, as necessary. Quantification of fault tree basic events that represent unavailabilities due to human failure to perform certain actions require mean human error probabilities (HEPs) as input.

Data

During facility design phase, generally no facility-specific data is available. As such, data from similar facilities, if available, or generic data can be used in model quantification, as appropriate. It should be noted that in certain cases the use of specific data sources may be specified and required by the facility owner/user (e.g., DOE).

A number of generic data sources that are sponsored by the U.S. Nuclear Regulatory Commission (NRC) and the DOE are identified and discussed in NUREG/CR-6823[10]. The Savannah River Site (SRS) generic component database[15] is also available as a source of component failure data. These data sources provide component failure rates that can be used in model quantification. The component failure rate data should be selected judiciously to ensure applicability to events modeled and to minimize the uncertainty. It is critical to define what the component boundary is in order to collect the right component failure rate data. Additionally, the component failure rate data selected should reflect the component failure mode being modeled.

Frequencies and durations of external initiating events (e.g., loss of offsite power or loss of natural gas) are dependent on the area in which the facility resides. Since facility-specific values do not exist during design phase, applicable data from similar facilities in the same locale, if available, can be used in model quantification. Otherwise generic data from data sources such as Reference 11 may be used, as appropriate.

MTTR values for certain components are published in the literature.[7,14] However, published MTTR values are scarce and, therefore, in most cases it may be necessary to derive the MTTR values based on past experience with similar components and/or engineering judgment. In such cases, the derivation of MTTR values should consider the following time factors:

- time to access (e.g., removing guards or panels)
- time to diagnose failure,
- time to disassemble,
- time to remove failed parts and replace with new parts,
- time to reassemble, and
- time to verify proper operation.

Derivation of the MTTR values assumes availability of the spare parts required for the corrective maintenance task; additionally, it assumes that the maintenance crew has the required skill to be able to perform the corrective maintenance task.

HEP values for the human actions modeled either can be directly obtained from sources such as NUREG/CR -1278[5] or SRS human error database[16], as appropriate, or can be calculated if necessary using the available Human Reliability Analysis (HRA) techniques.[6,17]

Common cause failure β values can be obtained from data sources such as References 12 and 13.

Evaluation of Fault Tree Results

The calculated inherent availability is compared against design criteria to determine if the availability goal is met. If the estimated inherent availability exceeds the design goal with an adequate margin of uncertainty, the design objective is met. However, if the estimated inherent availability is below the design goal, the assumptions made in the analysis and the uncertainties that exist in the data should be examined to determine if any changes in those areas (e.g., removing conservatisms) could potentially improve the overall result. If examination of the assumptions and the uncertainties does not impact the overall result, design changes may need to be considered. The fault tree results can be evaluated to identify dominant contributors to unavailability. Any design change considerations should initially focus on these dominant contributors as well as items that would have minimal impact on the overall design. Design change considerations may include the following, among others:

- selecting high quality (high reliability) components for dominant contributors,
- adding redundancy,
- adding diversity,
- reducing number of parts/components, and
- improving maintainability (i.e., lowering MTTR).

In order to improve maintainability, the repair time and thus MTTR must be reduced. This can be accomplished by methods such as incorporating self-diagnosis and fault detection capability into design, parts standardization and interchangeability, and improved accessibility to failed components/parts.

Preserve Inherent Availability

It is important to ensure that the inherent availability is preserved over the useful life of the facility after construction and commissioning. The RAM parameters tend to degrade overtime; some of the reasons for this degradation include:

- change in operating concept,
- change in operating environment,
- inadequate training,
- improper maintenance,
- aging/wear-out,
- change in supplier, and
- use of lower quality parts.

Developing and implementing programs such as Reliability-Centered Maintenance can help determine the critical versus non-critical components, and to identify the required maintenance tasks and frequencies to preserve component reliability, commensurate with component criticality. Maintenance strategies such as repair versus replacement policy, application of condition-based maintenance, spare parts inventory optimization, formal maintenance planning, root cause failure analysis, training of operations and maintenance personnel can also help maintain system/component reliability and maintainability and thus preserve the overall facility availability following construction and commissioning.

Conclusions

Application of RAM to facility preliminary design can help determine the degree to which reliability and maintainability as well as safety are incorporated into facility design and to determine whether the availability objective in design is met. Although a number of techniques are available to perform a RAM analysis, FTA augmented with MA, as necessary, is judged to be a viable technique. Developing and implementing sound maintenance strategies are essential to ensure availability is preserved over the useful life of the facility.

Acknowledgements

The author is grateful for the review of this paper by Mr. Kenneth Foote and Thomas Altenbach of the Lawrence Livermore National Laboratory (LLNL). Their comments and feedback improved the content of this paper. Prepared by LLNL under Contract DE-AC52-07NA27344.

References

1. DOE Order 430.1A, Life Cycle Asset Management, October 14, 1998.

2. DOE Order 420.1B, Facility Safety, December 22, 2005.

3. An Introduction to Reliability and Maintainability Engineering, Charles E. Ebeling, 2005.
4. Procedures for Treating Common Cause Failures in Safety and Reliability Studies, EPRI NP 5613, Volume 2, Analytic Background and Techniques, December 1988.

5. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP), NUREG/CR-1278, Final Report, Sandia National Laboratories, August 1983.

6. Accident Sequence Evaluation Program (ASEP) Human Reliability Analysis Procedure, NUREG/CR-4772, Sandia National Laboratories, October 1986.

7. IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, IEEE Std 500-1984.

8. Functional Safety of Electrical/Electronic, Programmable Electronic Safety Related Systems, IEC-61508, International Electrotechnical Committee, Parts 1 through 7, 1998.

9. Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, January 1981.

10. Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823, Sandia National Laboratories, September 2003.

11. Analysis of Loss of Offsite Power Events: 1986-2004, NUREG/CR-6890, Idaho National Laboratory, Volume 1, December 2005.

12. Advanced Light Water Reactor (ALWR) Utility Requirements Document, Electric Power Research Institute (EPRI), 1989.

13. Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980-1996, NUREG/CR-5496, U.S. Nuclear Regulatory Commission, November 1998.

14. Maintainability Prediction, MIL-HDBK-472, U.S. Department of Defense (DOD), May 1966.

15. Blanton, C.H., et al., Savannah River Site Generic Database Development, Westinghouse Savannah River Company, WSRC-TR-93-262, June 1993.

16. Benhardt, S. A., et al., Savannah River Site Human Error Database Development for Nonreactor Nuclear Facilities, Westinghouse Savannah River Company, WSRC-TR-93-581, February 1994.

17. Spurgin, A.J,. et al., A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination, EPRI NP-6560-L, December 1989.