An Approach to Ensure the Availability of Complex Systems

Kaushik Chatterjee[*], Kumar Bhimavarapu, Robert Kasiski, and William Doerr
FM Global, Norwood, MA, USA

Abstract: Availability of a system depends on: (1) the components' reliabilities; and (2) the Inspection, Testing and Maintenance (ITM) characteristics (i.e., inspection/testing frequency, repair/replacement duration, and maintenance restoration factor). Complex systems typically have several sub-systems and components with complicated interactions and dependencies. In order to ensure a desired availability of a safety-critical complex system such as a fire protection system throughout its lifetime, it is necessary to: (1) ensure the needed reliability of the critical components through carefully planned durability/life tests; and (2) perform ITM actions at appropriate intervals (or frequencies).

This paper presents a comprehensive approach to: (1) establish the reliability targets and the ITM frequencies for the critical components based on the desired availability of the system; and (2) estimate durability/life test duration and sample size requirements based on the established reliability targets for these critical components. The steps of the comprehensive approach have been demonstrated using a typical foam-water sprinkler protection system. The comprehensive approach, when applied to a safety-critical complex system, would help achieve the desired availabilities of the critical components, which in turn would ensure the desired availability of the system throughout its lifetime.

Keywords: Availability; reliability targets; Inspection, Testing, and Maintenance (ITM); safety-critical complex systems.

1. INTRODUCTION

Safety-critical complex systems such as fire protection systems need to be available when called upon to prevent catastrophic losses. Complex systems typically have several sub-systems and components with complicated interactions and dependencies. Availability of a system depends on: (1) the components' reliabilities; and (2) the Inspection, Testing and Maintenance (ITM) characteristics (i.e., inspection/testing frequency, repair/replacement duration, and maintenance restoration factor). In order to ensure a desired availability of a safety-critical complex system throughout its lifetime, it is necessary to: (1) ensure the needed reliability of the critical components through carefully planned durability/life tests; and (2) perform ITM actions at appropriate intervals (or frequencies).

Durability/life tests are typically used to evaluate component failures from degradation mechanisms such as wear, fatigue or corrosion. Development of durability/life test methods includes two major steps: i) definition of test environmental requirements (e.g., temperature, humidity, vibration, and cycling rate) considering the physics-of-failure (failure mode and the causal degradation mechanisms); and ii) estimation of test duration and sample size requirements based on the established reliability targets. Reliability target is the reliability at a specified lifetime that a component is expected to demonstrate.

This paper presents a comprehensive approach to: (1) establish the reliability targets and the ITM frequencies for the critical components based on the desired availability of the system; and (2) estimate durability/life test duration and sample size requirements based on the established reliability targets for these critical components.

[*] Email: Kaushik.chatterjee@fmglobal.com

2. COMPREHENSIVE APPROACH

The objective of the comprehensive approach is to ensure that the critical components achieve the desired availabilities, which would ensure the desired availability of the system throughout its lifetime. The key steps of the approach include definition of the system (see Section 2.1); Failure Mode and Effect Analysis (see Section 2.2); availability model development for the system and its components (see Section 2.3); system availability analysis to establish the reliability targets and the ITM frequencies for the critical components (see Section 2.4); and estimation of the durability/life test duration and sample size requirements for the critical components based on the established reliability targets (see Section 2.5).

2.1. System Definition

A clear definition of a complex system is necessary to ensure that all the sub-systems/components and other relevant details are considered appropriately in the evaluation of the system. More specifically, the system definition, which forms the basis for the next steps, includes delineation of: (1) the sub-systems and components, (2) the system boundaries, and (3) the postulates where appropriate.

2.2. Failure Mode and Effect Analysis

Failure Mode and Effect Analysis (FMEA) identifies the credible failure modes of the components, the causes of failures, and their effect on the system. This analysis is necessary to build the system availability model, as well as to identify the causes of component failures. The causes include degradation through mechanisms such as wear or corrosion, and/or human errors. For a component failure mode, identification of the causal degradation mechanisms helps in defining the environmental requirements for the durability/life tests.

2.3. Availability Model Development for the System and its Components

The system availability model is developed in order to determine the logic (i.e., possible combinations of credible component failure modes) that can lead to the system failure. A system availability model can be developed using a fault tree or a reliability block diagram.

The system availability is estimated using the system availability model and the component availabilities. The instantaneous availability, $A(t)$, of a component at any random lifetime t is the sum of the probability of two mutually exclusive events, i.e., either the component is functioning properly at time t, the probability of which is its reliability $R(t)$; or the component is functioning properly since the last repair at time x $(0 < x < t)$, the probability of which is $\int_0^t R(t-x)m(x)dx$ [1]. These contributions are shown in Equation (1), where $m(x)$ is the renewal density function that incorporates maintainability information. The renewal density function is dependent on the probability density functions of the time to failure and the repair time distributions.

$$A(t) = R(t) + \int_0^t R(t-x)m(x)dx \qquad (1)$$

2.3.1. Reliability Distribution Parameters

The Weibull distribution is typically used for modelling reliability. The reliability $R(t)$ at a component lifetime t can be estimated using Equation (2), where, β is the shape parameter, and η is the scale parameter or characteristic life.

$$R(t) = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \qquad (2)$$

The shape parameter determines the shape of the failure distribution curve. The value of the shape parameter for a component depends on the physics of failure, i.e., the failure mode and the causal degradation mechanisms. The characteristic life is the lifetime at which the component reliability equals 0.368 (or 63.2% of the components fail). For a given shape parameter, the component reliability varies as a function of the characteristic life. For example, corresponding to a shape parameter value of 3, the reliability values at 50 years would be 0.368, 0.89 and 0.98 respectively for characteristic life values of 50, 100 and 200 years.

2.3.2. ITM Parameters

The ITM parameters include the inspection/testing frequency, repair/replacement duration, and maintenance restoration factor. Restoration factor indicates the percentage (of new condition) to which a component will be restored after the performance of the maintenance action. While performing availability estimations, the restoration factor is assigned a value from 0 to 1. A restoration factor value of 1 indicates that the component will be "as good as new" after the maintenance action. Thus the age of the component will be reset to zero. A restoration factor value of 0 indicates that the component will not be improved at all by the maintenance action. Thus the age of the component will be the same as the age before the maintenance was performed[2].

The type of maintenance (i.e., corrective or preventive) also plays a key role in the system availability. Corrective maintenance is usually performed to restore a failed system to operational status by replacing or repairing the component that is responsible for the system failure[2]. Preventive maintenance is usually performed to replace components before they fail in order to maintain uninterrupted system operation[2]. Choice of corrective or preventive maintenance can affect the needed reliability targets. For example, if only corrective actions are considered, then relatively higher reliability values for components may be necessary to achieve the desired system availability, as compared to when preventive actions are also considered.

Another important factor is the repair/replacement time, which indicates whether the repair commences immediately after failure, or when a failure is detected during a periodic ITM. For example, in the case of revealed failures (e.g., a pipe rupture) the repair/replacement may commence immediately after failure, whereas in the case of unrevealed failures (e.g., a valve spring failure) the repair/replacement may commence after the failure is detected during a periodic ITM or a real demand.

2.4. System Availability Analysis to Establish Reliability Targets and ITM Frequencies

The reliability targets and the ITM frequencies for the critical components are established through an iterative process so as to achieve the desired system availability, as shown in Figure 1. The current system availability is estimated using: (1) the system availability model (e.g., fault tree); and (2) the current reliabilities of components (estimated based on the respective Weibull distribution parameters, i.e., shape parameter and characteristic life) and ITM parameters (i.e., inspection/testing frequency, repair/replacement duration, and maintenance restoration factor).

If the estimated current system availability is found to be unacceptable (less than the desired value), then the reliabilities and/or the ITM frequencies of the critical components (with focus on specific

[2] The descriptions have been adopted from the ReliaSoft BlockSim software manual.

failure modes) are increased to reasonable levels[3], and system availability is re-estimated. This is done iteratively until the desired system availability is achieved. This procedure establishes the reliability targets and the ITM frequencies for the critical components.

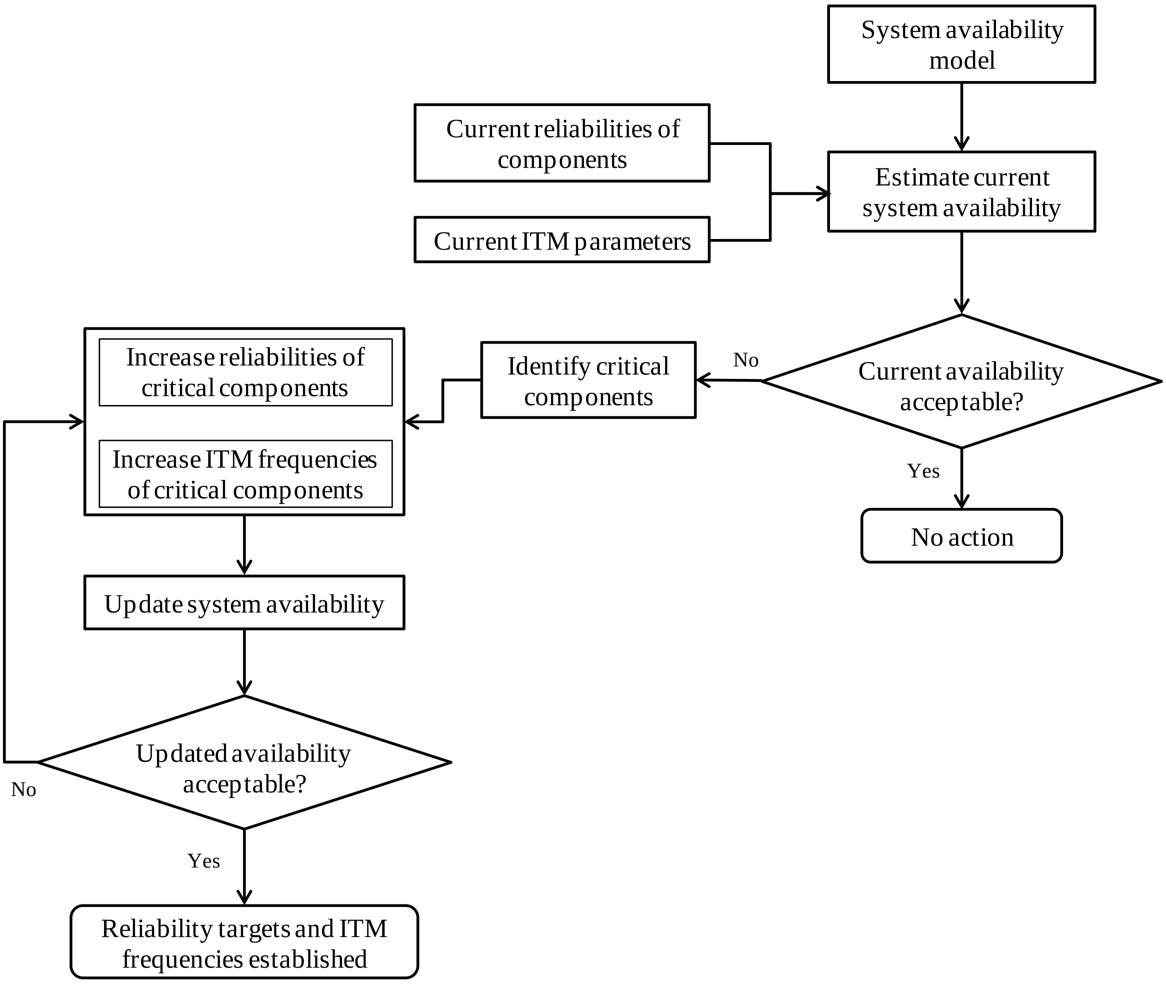
System availability model
Current reliabilities of components
Current ITM parameters
Estimate current system availability
Current availability acceptable?
No
Yes
No action
Identify critical components
Increase reliabilities of critical components
Increase ITM frequencies of critical components
Update system availability
Updated availability acceptable?
No
Yes
Reliability targets and ITM frequencies established

Figure 1: Iterative process for establishment of reliability targets and ITM frequencies

In order to increase the reliabilities of the critical components, the respective Weibull characteristic lives can be increased based on the relative contributions of each component to the system downtime. For example, the Weibull characteristic life of the most critical component (with highest contribution to the system downtime) can be increased by the highest factor, whereas the Weibull characteristic lives of the remaining critical components (with relatively smaller contributions to the system downtime) can be increased by relatively smaller factors.

Generally, the ITM frequencies are constant throughout the life of a system. Since the component reliabilities reduce with age, it can be useful to increase the ITM frequencies with age of the components to improve their availabilities. For example, for a component with specific reliability, prescribing a high ITM frequency only towards the end of life can be more useful and effective in achieving the desired minimum availability throughout the lifetime, when compared to prescribing a constantly high ITM frequency for the entire lifetime. Such an increase in the ITM frequency would also allow for less stringent reliability targets.

[3] A component's reliability or ITM frequency can only be increased to a certain level beyond which it may not be feasible owing to technology and cost constraints. Introducing component redundancy can also increase the system reliability, however, this method has not been considered in this study.

2.4.1. Identification of Critical Components

Critical component failure modes can be identified and ranked based on the Downtime Criticality Index (DTCI). DTCI is a relative index showing the contribution of each component to the system's downtime (i.e., the system downtime caused by a particular component divided by the total system downtime)[2]. A component with the highest DTCI value has the highest contribution to the system downtime, and is most critical for the system availability. Therefore, focusing on the critical components not only helps in achieving the desired system availability, but also ensures that the reliabilities and the ITM frequencies of less critical components are not unnecessarily increased from the current levels.

2.5. Estimation of Durability/Life Test Duration and Sample Size Requirements to Meet the Reliability Targets

The Weibayes zero-failure method can be used to demonstrate (through durability/life testing without observing any failure) a minimum reliability target at a specified confidence level. The test duration for a specific sample size needed to demonstrate the lower confidence limit for reliability R_d at the expected lifetime of t_d (cycles or years) can be estimated using the modified Weibayes equation, as shown in Equation (3) [2], where T is the test duration (cycles or years), C is the confidence level, N is the test sample size, and β is the Weibull shape parameter.

$$T = t_d \left[\frac{\ln(1-C)}{N \ln(R_d)} \right]^{\frac{1}{\beta}} \qquad (3)$$

A small sample size can result in very high test duration requirement (several times higher than the expected lifetime). Further, if the shape parameter values are uncertain, then a small sample size can result in wide variability in the test durations. Depending on the availability of resources (i.e., time and cost), large sample sizes can be used to: (1) reduce the test duration requirements; and (2) reduce variability in the test durations resulting from uncertainty in the shape parameter values.

3. EXAMPLE APPLICATION OF THE COMPREHENSIVE APPROACH

An active foam-water sprinkler protection system has been used to demonstrate the key steps of the comprehensive approach. The foam-water protection system consists of two major sub-systems: (1) the water supply (consisting of components such as controller, motor, pump, and valves); and (2) the foam supply (consisting of components such as bladder tank, foam concentrate, and hydraulic concentrate valve). These two sub-systems supply water and foam at the desired flow rate and pressure to a proportioner, which mixes the water and foam in the right proportion to prepare the foam-water solution for discharge through automatic sprinklers. The foam-water protection system failure is defined as 'no or low' foam-water discharge from sprinklers when required in the event of a fire. The fault tree technique has been used to develop the system availability model to determine the logic (possible combinations of credible component failure modes) leading to the system failure.

Based on the system fault tree, availability analysis was performed for an assumed lifetime of 30 years using the software package ReliaSoft BlockSim. The current system availability (curve shown by the dotted line in Figure 2), estimated using the current values of the reliability distribution and the ITM parameters, is below the desired availability value for most of the system lifetime. In order to achieve the desired system availability, an iterative availability analysis was performed by increasing the reliabilities and the ITM frequencies of the critical components (identified using the DTCI values). The achieved availability curves (for systems updated – 1 & 2) are shown in Figure 2.

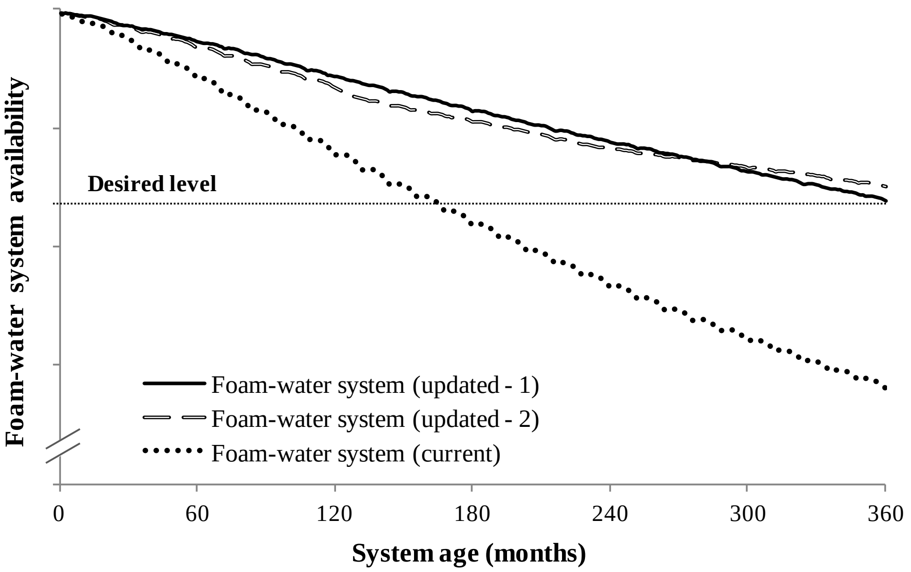

Figure 2: Foam-water system availabilities (current and updated)[4]

In Figure 2, the availability curves (updated – 1 & 2) were achieved by increasing the reliabilities of the critical components to the same level, but with different ITM frequencies. The solid line (updated – 1) represent the availability curve achieved by increasing the ITM frequencies by a factor of 1.33 throughout the lifetime. However, the dashed line (updated – 2) in Figure 2 represent the availability curve achieved by increasing the ITM frequencies with age. The current ITM frequencies were used for first 10 years of lifetime, increased by a factor of 1.33 from the current level for the next 10 years of lifetime, and increased by a factor of 2 from the current level for the last 10 years of lifetime.

When compared to the availability curve (updated – 1) shown by the solid line, the availability curve (updated – 2) shown by the dashed line has higher availability in the later part of the lifetime. Thus, for the system with the availability curve (updated – 2) shown by the dashed line, the reliability targets of components can be made relatively less stringent (i.e., lowered further) and still meet the desired availability level.

The durability/life test duration and sample size requirements were then estimated for the critical components based on the established reliability targets (used to achieve the updated curves in Figure 2) and at a specified confidence level. Figure 3 presents the durability/life test requirements for a component with an expected lifetime of 1000 cycles.

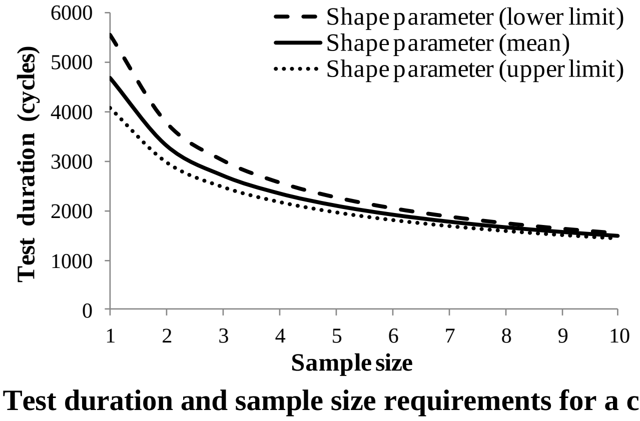

Figure 3: Test duration and sample size requirements for a component

[4] The absolute values of system availability are not provided in this figure, which is only intended to demonstrate the comprehensive approach.

The test duration requirements corresponding to a range of shape parameter values (lower limit, mean, upper limit) have been provided to demonstrate the benefit of using large sample sizes when shape parameter values are uncertain. As can be seen from Figure 3, for small sample sizes, there is higher variability in the test durations corresponding to the three shape parameter values. However, as the sample size is increased, the test durations (corresponding to the three shape parameter values) decrease exponentially and tend to converge.

4. CONCLUSION

This paper presented a comprehensive approach to: (1) establish the reliability targets and the ITM frequencies for the critical components based on the desired availability of the system; and (2) estimate durability/life test duration and sample size requirements based on the established reliability targets for these critical components. Focusing on the critical components not only helps in achieving the desired system availability, but also ensures that the reliabilities and the ITM frequencies of less critical components are not unnecessarily increased from the current levels.

Since the component reliabilities reduce with age, it can be useful to increase the ITM frequencies with age of the components to improve their availabilities. For example, for a component with specific reliability, prescribing a high ITM frequency only towards the end of life can be more useful and effective in achieving the desired minimum availability throughout the lifetime, when compared to prescribing a constantly high ITM frequency for the entire lifetime. Such an increase in the ITM frequency would also allow for less stringent reliability targets.

A small sample size can result in very high test duration requirements (several times higher than the expected lifetime). Further, if the shape parameter values are uncertain, then a small sample size can result in wide variability in the test durations. Depending on the availability of resources (i.e., time and cost), larger sample sizes can be used to: (1) reduce the test duration requirements; and (2) reduce variability in the test durations resulting from uncertainty in the shape parameter values.

The steps of the developed comprehensive approach have been demonstrated using a typical foam-water sprinkler protection system. The comprehensive approach, when applied to a safety-critical complex system, would help achieve the desired availabilities of the critical components, which in turn would ensure the desired availability of the system throughout its lifetime.

References

[1] E.A., Elsayed, "*Reliability Engineering*", John Wiley & Sons, 2012, Hoboken, New Jersey.

[2] J.C., Wang, "*Sample size determination of bogey tests without failures*", Quality and Reliability Engineering International, Vol. 7, pp: 35-38, 1991.