SECTION 5 Failure Finding Maintenance

1 Introduction

Failure-finding maintenance tasks are employed to discover equipment faults that are not detected during normal crew operations (e.g., hidden failures). Because these failures are hidden, if proper maintenance is not performed, a second failure must occur and a failure consequence realized before the equipment fault is detected. For example, a standby electrical generator failing to start on loss of power may only be discovered when the primary generator fails and power is lost.

Because these types of faults result in hidden failures, condition-monitoring or planned-maintenance tasks are typically not an effective failure management strategy. Failure-finding maintenance tasks usually involve a functional test of the equipment to ensure the equipment is available to perform its function(s) when demanded.

2 Statistical View of Hidden Failures

The purpose of a failure-finding task is to reduce the risk of multiple failures to an acceptable level by managing the frequency of occurrence of a multiple failure. Assuming that the multiple failure can only occur from the combination of a specific initiating event concurrent with the unavailability of the safety or backup system, the frequency of occurrence of a multiple failure is defined by the following equation:

$$F_{MF} = F_{IE} \cdot \bar{a}_{SYS} \quad \text{.....(1)}$$

where

F_{MF} = frequency of occurrence of the multiple failure

F_{IE} = frequency of occurrence of the initiating event making the hidden failure evident

$\bar{a}_{SYS}$ = $(1 - a_{SYS})$, or the unavailability of the safety system or backup system

a_{SYS} = availability of the safety system or backup system

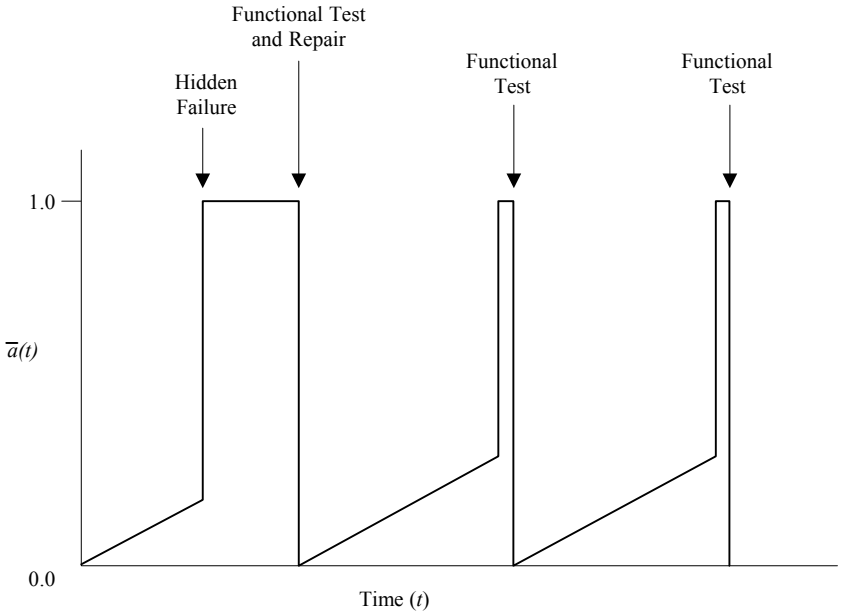
This equation can be rearranged to solve for the unavailability of the safety system or backup system:

$$\bar{a}_{SYS} = F_{MF}/F_{IE} \quad \text{.....(2)}$$

An acceptable frequency of occurrence of a failure is achieved by ensuring that the unavailability of the equipment is less than what is needed to ensure the frequency of occurrence of a multiple failure is low enough to yield an acceptable risk of failure. For example, if the acceptable frequency of occurrence of a multiple failure for a specific event is 0.01/yr and the frequency of failure of the initiating event (e.g., F_{IE}) is 0.1/yr, then the acceptable unavailability for the hidden failure is 0.1.

Failure-finding tasks are effective in managing hidden failures because these tasks either (1) confirm that the equipment is functioning or (2) allow us to discover that the equipment has failed and needs repair. Once the task is performed, the unavailability of the safety system or backup system is "reset" to zero (or nearly zero). Then, as time progresses, the unavailability increases until the item fails or is retested again. If an exponential failure distribution is assumed, the failure rate is constant, which means the probability of the failure increases linearly (or at least nearly so over most reasonable time periods) at a slope equal to the failure rate (e.g., the probability of failure is a product of the failure rate and elapsed time). Section 5, Figure 1 illustrates the effect of failure-finding tasks.

FIGURE 1
Effect of a Failure-finding Task



3 Failure-finding Task Applicability and Effectiveness

For a failure-finding task to be considered effective, the following considerations must be made:

i) Must be no applicable or cost-effective condition-monitoring or planned-maintenance task that can detect or prevent the failure.

ii) Must be technically feasible to perform. The task must be practical to perform at the required interval and must not disrupt an otherwise stable system.

iii) Must reduce the probability of failure (and therefore the risk) to an acceptable level. The tasks must be carried out at an interval so that probability of multiple failures allows an acceptable risk level to be achieved. Agreed-upon risk acceptance criteria should be determined and recorded.

iv) Must not increase the risk of a multiple failure (e.g., when testing a relief valve, an over-pressure should not be created without the relief valve in service).

v) Must ensure that protective systems are tested in their entirety rather than as individual components that make up the system.

vi) Must be cost-effective. The cost of undertaking a task over a period of time should be less than the total cost of the consequences of failure.

4 Determining Failure-finding Maintenance Task Interval

The interval for failure-finding tasks can be determined:

i) Mathematically, using reliability equations, or

ii) Using general guidelines developed to ensure acceptable risk.

Regardless of the technique used, the key is to ensure that the unavailability of a safety system or backup system is low enough to ensure that frequency of occurrence of a multiple failure is sufficiently low to achieve an acceptable risk. For a given consequence resulting from a multiple failure, an acceptable frequency of occurrence for the multiple failure needs to be established. For example, an acceptable frequency of occurrence for a $1 million operational loss might be 0.01/yr and acceptable frequency of occurrence for a $100,000 operational loss could be 0.1/yr. In both cases, the risk is equivalent ($10,000/yr).

These two techniques for setting failure-finding task intervals are briefly explained in the following paragraphs

4.1 Mathematical Determination of Failure-finding Task Interval

The highest-risk hidden failures usually require that the failure-finding task interval be mathematically determined. This is generally done by assuming the hidden failure is random and, therefore, is best modeled using the exponential distribution. This assumption is usually valid for the following reasons:

i) If the failure has a wear-in failure characteristic, then either a one-time change or a condition-monitoring task is usually employed to manage the failure.

ii) If the failure has a wear-out failure characteristic, then a condition-monitoring task or a planned-maintenance task should be applied to manage the failure.

To determine a failure-finding task interval, the equation for the frequency of a multiple failure and the equation for the unavailability of the hidden failure are combined as follows:

The equation for the frequency of occurrence of a multiple failure is:

$$F_{MF} = F_{IE} \cdot \bar{a}_{SYS} \quad \text{.....(3)}$$

To determine the maximum unavailability allowed to achieve an acceptable risk level, F_{MF} is set equal to the acceptable frequency (F_{ACC}) for the consequence being evaluated. Equation 3 is rearranged and unavailability ($\bar{a}_{SYS}$) is then solved for as shown in Equations 4a and 4b:

$$\bar{a}_{SYS} = F_{MF}/F_{IE} \quad \text{.....(4a)}$$

$$\bar{a}_{SYS} = F_{ACC}/F_{IE} \quad \text{.....(4b)}$$

The following additional assumptions are often true and will produce the simplification shown in Equation 5.

i) The distribution of the failures is exponential.

ii) The conditional failure rate times the test interval time ($\lambda \times$ test interval) is less than 0.1.

iii) The time to conduct a failure-finding task is short when compared to the length of time that the system is available.

iv) The time to conduct a repair of the system is short when compared to the length of time that the system is available.

v) The multiple failure can only occur from the combination of the specified initiating event concurrent with the unavailability of the backup or safety system.

$$T = \frac{2 \cdot F_{ACC} \cdot MTTF}{F_{IE}} \quad \text{.....(5)}$$

where

T = test interval

F_{ACC} = acceptable frequency of occurrence of the multiple failure

F_{IE} = frequency of occurrence of the initiating event making the hidden failure evident

$MTTF$ = mean time to failure for the system with the hidden failure

4.2 Using Guidelines to Determine the Failure-finding Task Interval

Guidelines are developed and documented for determining the failure-finding task interval. This usually involves the following:

i) Establishing rules for determining required unavailability of the hidden failure based on the risk of the hidden failure

ii) Estimating the MTTF of the hidden failure

iii) Determining the test interval using a table based on Equation 5

Section 5, Tables 1 and 2 provide examples of the acceptable probability rules and failure-finding test interval.

TABLE 1
Example of Failure-finding Task Interval Rules

Risk of Hidden Failure	*Unavailability Required*
Very High	< 0.0001
High	> 0.0001 to 0.001
Moderate	> 0.001 to 0.01
Low	> 0.01 to 0.05

TABLE 2
Example of Failure-finding Task Intervals Based on MTTF

Unavailability Required	*Failure-finding Task Interval (as % of MTTF)*
0.0001	0.02
0.001	0.2
0.01	2
0.05	10

When applying this guideline approach, the user must be aware of the assumptions used in developing the rules and task intervals, and ensure that the assumptions are valid.