A dangerous high-pressure reactor situation occurs only when both the alarm system and the shutdown system fail. These two components are in parallel. For the alarm system the components are in series:

$$R = \prod_{i=1}^{2} R_i = (0.87)(0.96) = 0.835,$$

$$P = 1 - R = 1 - 0.835 = 0.165,$$

$$\mu = -\ln R = -\ln(0.835) = 0.180 \text{ faults/yr},$$

$$\text{MTBF} = \frac{1}{\mu} = 5.56 \text{ yr}.$$

For the shutdown system the components are also in series:

$$R = \prod_{i=1}^{2} R_i = (0.87)(0.66) = 0.574,$$

$$P = 1 - R = 1 - 0.574 = 0.426,$$

$$\mu = -\ln R = -\ln(0.574) = 0.555 \text{ faults/yr},$$

$$\text{MTBF} = \frac{1}{\mu} = 1.80 \text{ yr}.$$

The two systems are combined using Equation 12-6:

$$P = \prod_{i=1}^{2} P_i = (0.165)(0.426) = 0.070,$$

$$R = 1 - P = 0.930,$$

$$\mu = -\ln R = -\ln(0.930) = 0.073 \text{ faults/yr},$$

$$\text{MTBF} = \frac{1}{\mu} = 13.7 \text{ yr}.$$

For the alarm system alone a failure is expected once every 5.5 yr. Similarly, for a reactor with a high-pressure shutdown system alone, a failure is expected once every 1.80 yr. However, with both systems in parallel the MTBF is significantly improved and a combined failure is expected every 13.7 yr.

The overall failure probability is given by

$$P = P(A)P(S),$$

where $P(A)$ is the failure probability of the alarm system and $P(S)$ is the failure probability of the emergency shutdown system. An alternative procedure is to invoke Equation 12-9 directly. For the alarm system

$$P(A) = P_1 + P_2 - P_1P_2.$$

For the shutdown system

$$P(S) = P_3 + P_4 - P_3P_4.$$

The overall failure probability is then

$$P = P(A)P(S) = (P_1 + P_2 - P_1P_2)(P_3 + P_4 - P_3P_4).$$

Substituting the numbers provided in the example, we obtain

$$\begin{aligned} P &= [0.13 + 0.04 - (0.13)(0.04)][0.34 + 0.13 - (0.34)(0.13)] \\ &= (0.165)(0.426) = 0.070. \end{aligned}$$

This is the same answer as before.

If the products P_1P_2 and P_3P_4 are assumed to be small, then

$$P(A) = P_1 + P_2,$$
$$P(S) = P_3 + P_4,$$

and

$$\begin{aligned} P &= P(A)P(S) = (P_1 + P_2)(P_3 + P_4) \\ &= 0.080. \end{aligned}$$

The difference between this answer and the answer obtained previously is 14.3%. The component probabilities are not small enough in this example to assume that the cross-products are negligible.

Revealed and Unrevealed Failures

Example 12-2 assumes that all failures in either the alarm or the shutdown system are immediately obvious to the operator and are fixed in a negligible amount of time. Emergency alarms and shutdown systems are used only when a dangerous situation occurs. It is possible for the equipment to fail without the operator being aware of the situation. This is called an unrevealed failure. Without regular and reliable equipment testing, alarm and emergency systems can fail without notice. Failures that are immediately obvious are called revealed failures.

A flat tire on a car is immediately obvious to the driver. However, the spare tire in the trunk might also be flat without the driver being aware of the problem until the spare is needed.

Figure 12-6 shows the nomenclature for revealed failures. The time that the component is operational is called the period of operation and is denoted by τ_o. After a failure occurs, a period of time, called the period of inactivity or downtime (τ_r), is required to repair the component. The MTBF is the sum of the period of operation and the downtime, as shown.

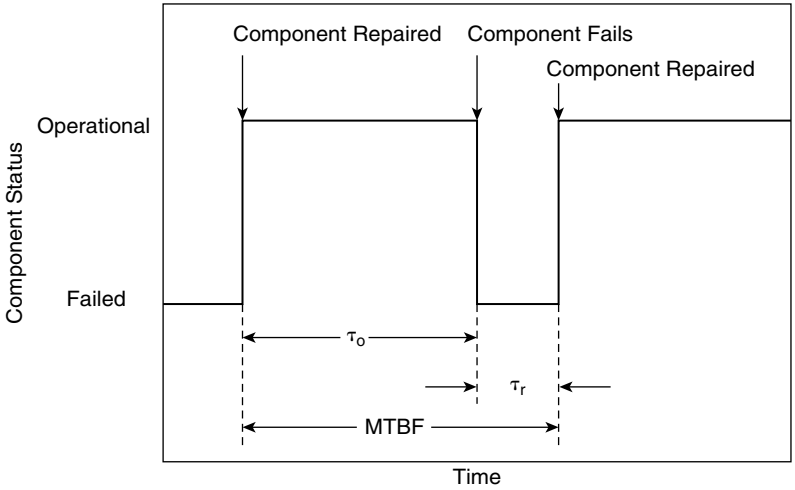

Figure 12-6 Component cycles for revealed failures. A failure requires a period of time for repair.

For revealed failures the period of inactivity or downtime for a particular component is computed by averaging the inactive period for a number of failures:

$$\tau_r \cong \frac{1}{n}\sum_{i=1}^{n} \tau_{r_i}, \tag{12-12}$$

where

n is the number of times the failure or inactivity occurred and
τ_{r_i} is the period for repair for a particular failure.

Similarly, the time before failure or period of operation is given by

$$\tau_o \cong \frac{1}{n}\sum_{i=1}^{n} \tau_{o_i}, \tag{12-13}$$

where τ_{o_i} is the period of operation between a particular set of failures.

The MTBF is the sum of the period of operation and the repair period:

$$\text{MTBF} = \frac{1}{\mu} = \tau_r + \tau_o. \tag{12-14}$$

It is convenient to define an availability and unavailability. The availability A is simply the probability that the component or process is found functioning. The unavailability U is the probability that the component or process is found not functioning. It is obvious that

$$A + U = 1. \tag{12-15}$$

The quantity τ_o represents the period that the process is in operation, and $\tau_r + \tau_o$ represents the total time. By definition, it follows that the availability is given by

$$A = \frac{\tau_o}{\tau_r + \tau_o}, \tag{12-16}$$

and, similarly, the unavailability is

$$U = \frac{\tau_r}{\tau_r + \tau_o}. \tag{12-17}$$

By combining Equations 12-16 and 12-17 with the result of Equation 12-14, we can write the equations for the availability and unavailability for revealed failures:

$$\boxed{\begin{aligned} U &= \mu\tau_r, \\ A &= \mu\tau_o. \end{aligned}} \tag{12-18}$$

For unrevealed failures the failure becomes obvious only after regular inspection. This situation is shown in Figure 12-7. If τ_u is the average period of unavailability during the inspection interval and if τ_i is the inspection interval, then

$$U = \frac{\tau_u}{\tau_i}. \tag{12-19}$$

The average period of unavailability is computed from the failure probability:

$$\tau_u = \int_0^{\tau_i} P(t)\, dt. \tag{12-20}$$

Combining with Equation 12-19, we obtain

$$U = \frac{1}{\tau_i} \int_0^{\tau_i} P(t)\, dt. \tag{12-21}$$

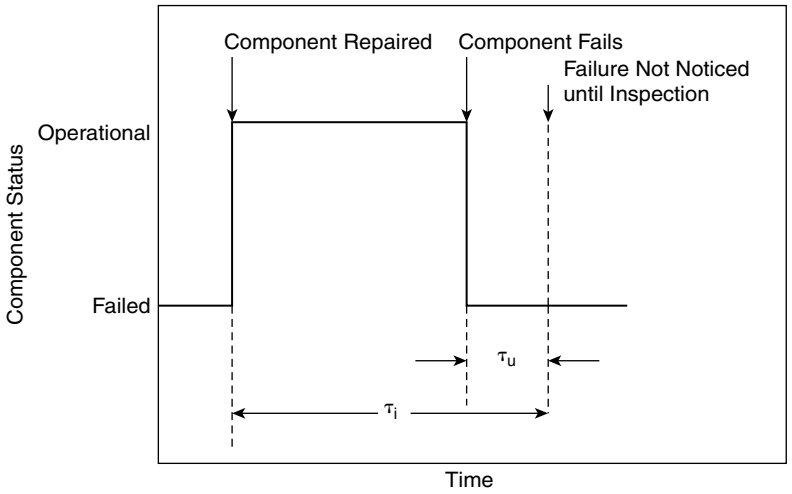

Figure 12-7 Component cycles for unrevealed failures.

The failure probability $P(t)$ is given by Equation 12-2. This is substituted into Equation 12-21 and integrated. The result is

$$U = 1 - \frac{1}{\mu\tau_i}(1 - e^{-\mu\tau_i}). \tag{12-22}$$

An expression for the availability is

$$A = \frac{1}{\mu\tau_i}(1 - e^{-\mu\tau_i}). \tag{12-23}$$

If the term $\mu\tau_i \ll 1$, then the failure probability is approximated by

$$P(t) \approx \mu t, \tag{12-24}$$

and Equation 12-21 is integrated to give, for unrevealed failures,

$$\boxed{U = \frac{1}{2}\mu\tau_i.} \tag{12-25}$$

This is a useful and convenient result. It demonstrates that, on average, for unrevealed failures the process or component is unavailable during a period equal to half the inspection interval. A decrease in the inspection interval is shown to increase the availability of an unrevealed failure.

Equations 12-19 through 12-25 assume a negligible repair time. This is usually a valid assumption because on-line process equipment is generally repaired within hours, whereas the inspection intervals are usually monthly.

Example 12-3

Compute the availability and the unavailability for both the alarm and the shutdown systems of Example 12-2. Assume that a maintenance inspection occurs once every month and that the repair time is negligible.

Solution

Both systems demonstrate unrevealed failures. For the alarm system the failure rate is $\mu = 0.18$ faults/yr. The inspection period is 1/12 = 0.083 yr. The unavailability is computed using Equation 12-25:

$$U = \frac{1}{2}\mu\tau_i = (1/2)(0.18)(0.083) = 0.0075,$$

$$A = 1 - U = 0.992.$$

The alarm system is available 99.2% of the time. For the shutdown system $\mu = 0.55$ faults/yr. Thus

$$U = \frac{1}{2}\mu\tau_i = (1/2)(0.55)(0.083) = 0.023,$$

$$A = 1 - 0.023 = 0.977.$$

The shutdown system is available 97.7% of the time.

Probability of Coincidence

All process components demonstrate unavailability as a result of a failure. For alarms and emergency systems it is unlikely that these systems will be unavailable when a dangerous process episode occurs. The danger results only when a process upset occurs and the emergency system is unavailable. This requires a coincidence of events.

Assume that a dangerous process episode occurs p_d times in a time interval T_i. The frequency of this episode is given by

$$\lambda = \frac{p_d}{T_i}. \tag{12-26}$$

For an emergency system with unavailability U, a dangerous situation will occur only when the process episode occurs and the emergency system is unavailable. This is every $p_d U$ episodes.

The average frequency of dangerous episodes λ_d is the number of dangerous coincidences divided by the time period:

$$\lambda_d = \frac{p_d U}{T_i} = \lambda U. \tag{12-27}$$

For small failure rates $U = \frac{1}{2}\mu\tau_i$ and $p_d = \lambda T_i$. Substituting into Equation 12-27 yields

$$\lambda_d = \frac{1}{2}\lambda\mu\tau_i. \tag{12-28}$$

The mean time between coincidences (MTBC) is the reciprocal of the average frequency of dangerous coincidences:

$$\text{MTBC} = \frac{1}{\lambda_d} = \frac{2}{\lambda\mu\tau_i}. \tag{12-29}$$

Example 12-4

For the reactor of Example 12-3 a high-pressure incident is expected once every 14 months. Compute the MTBC for a high-pressure excursion and a failure in the emergency shutdown device. Assume that a maintenance inspection occurs every month.

Solution

The frequency of process episodes is given by Equation 12-26:

$$\lambda = 1 \text{ episode}/[(14 \text{ months})(1 \text{ yr}/12 \text{ months})] = 0.857/\text{yr}.$$

The unavailability is computed from Equation 12-25:

$$U = \frac{1}{2}\mu\tau_i = (1/2)(0.55)(0.083) = 0.023.$$

The average frequency of dangerous coincidences is given by Equation 12-27:

$$\lambda_d = \lambda U = (0.857)(0.023) = 0.020.$$

The MTBC is (from Equation 12-29)

$$\text{MTBC} = \frac{1}{\lambda_d} = \frac{1}{0.020} = 50 \text{ yr}.$$

It is expected that a simultaneous high-pressure incident and failure of the emergency shutdown device will occur once every 50 yr.

If the inspection interval τ_i is halved, then $U = 0.023$, $\lambda_d = 0.010$, and the resulting MTBC is 100 yr. This is a significant improvement and shows why a proper and timely maintenance program is important.