

4

Reliability and Safety

Reliability Definitions

As the field of reliability engineering has evolved, several measures have been defined to express useful parameters that specifically relate to successful operation of a device. Based on that work, additional measures have been more recently defined that specifically relate to safety engineering. These measures have been defined to give the different kinds of information that engineers need to solve a number of different problems.

Time to Failure

The term “random variable” is well understood in the field of statistics. It is the independent variable—the variable being studied. Samples of the random variable are taken. Statistics are computed about that variable in order to learn how to predict its future behavior.

In reliability engineering, the primary random variable is T : Time to Failure or Failure Time. Reliability engineers gather data about when (and, using other measures, how) things fail. This information is used to gain insight into the future performance of system designs. For example, 10 modules are life tested and each module’s time to failure is recorded (Table 4-1). In this study, T is the random variable of interest.

The sample average (or mean) of the failure times can be calculated. For this set of test data, the sample mean time to failure, MTTF, is calculated to be 3,248 hours. This measurement provides some information about the future performance of similar modules.

Table 4-1. Ten Module Life Test Results

Module	Time to Fail
1	2327 Hrs.
2	4016 Hrs.
3	4521 Hrs.
4	3176 Hrs.
5	0070 Hrs.
6	3842 Hrs.
7	3154 Hrs.
8	2017 Hrs.
9	5143 Hrs.
10	4215 Hrs.

Reliability

Reliability is a measure of success. It is defined as the probability that a device will be successful; that is, that it will satisfactorily perform its intended function when required to do so if operated within its specified design limits. The definition includes four important aspects of reliability:

1. The device's "intended function" must be known.
2. "When the device is required to function" must be established.
3. "Satisfactory performance" must be determined.
4. The "specified design limits" must be known.

All four aspects must be addressed when measuring the reliability of a device.

Mathematically, reliability (R) has a precise definition: "The probability that a device will be successful during the operating time interval, t ." In terms of the random variable T ,

$$R(t) = P(T > t) \quad (4-1)$$

Reliability equals the probability that T , failure time, is greater than t , operating time interval (Ref. 1).

Consider a newly manufactured and successfully tested component. It operates properly when put into service at time $t = 0$. As the operating time interval increases, it becomes less likely that the component will continue to operate properly. Since the component will eventually fail, the probability of success for an infinite operating time interval is zero. $R(t)$ is a cumulative distribution function. It begins at a probability of one and decreases to a probability of zero (Figure 4-1).

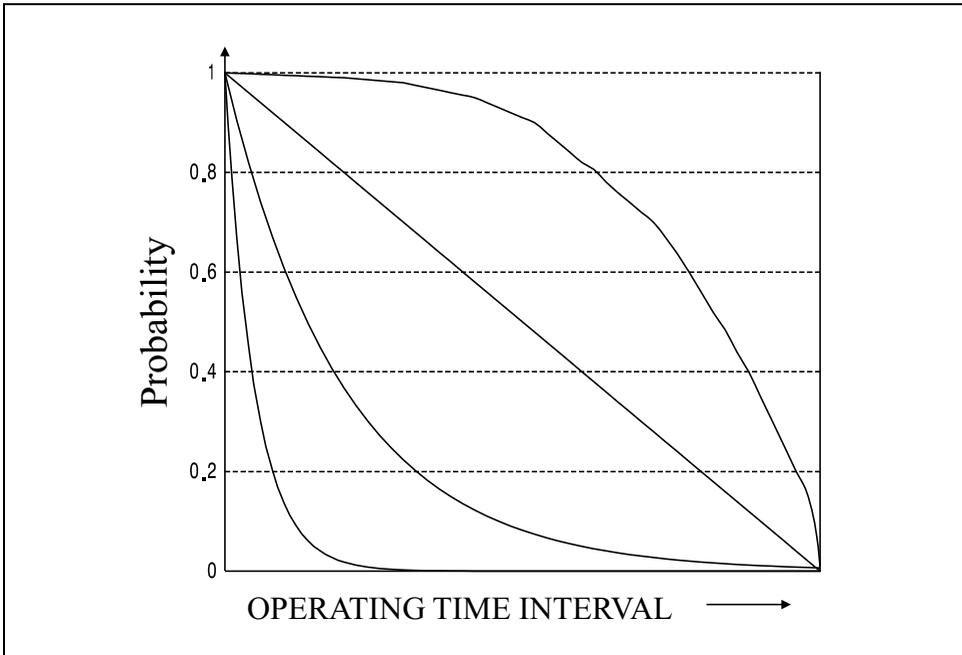


Figure 4-1. Reliability Functions

Reliability is a function of failure probability and operating time interval. A statement such as “System reliability is 0.95” is meaningless because the time interval is not known. The statement “The reliability equals 0.98 for a mission time of 100 hours” makes perfect sense. Reliability is a measure that is usually applied to situations such as aircraft flights and space missions where no repair is possible. In these circumstances a system must operate continuously without any failure to achieve mission success.

Unreliability

Unreliability, $F(t)$, a measure of failure, is defined as “the probability that a device will fail during the operating time interval, t .” In terms of the random variable T ,

$$F(t) = P(T \leq t) \quad (4-2)$$

Unreliability equals the probability that failure time will be less than or equal to the operating time interval. Since any device must be either successful or failed, $F(t)$ is the one’s complement of $R(t)$.

$$F(t) = 1 - R(t) \quad (4-3)$$

$F(t)$ is also a cumulative distribution function. It begins with a probability of zero and increases to a probability of one.

Availability

Reliability is a measure that requires success (that is, successful operation) for an entire time interval. No failures (and subsequent repairs) are allowed. This measurement was not enough for engineers who needed to know the chance of success when repairs may be made.

Another measure of success was required for repairable devices (Figure 4-2). That measure is availability. Availability is defined as “the probability that a device is successful (operational) at any moment in time.” There is no operational time interval involved. If a device is operational, it is available. It does not matter whether it has failed in the past and has been repaired or has been operating continuously without any failures. Therefore availability is a function of failure probabilities and repair probabilities whereas reliability is a function of failure probabilities and operating time interval.

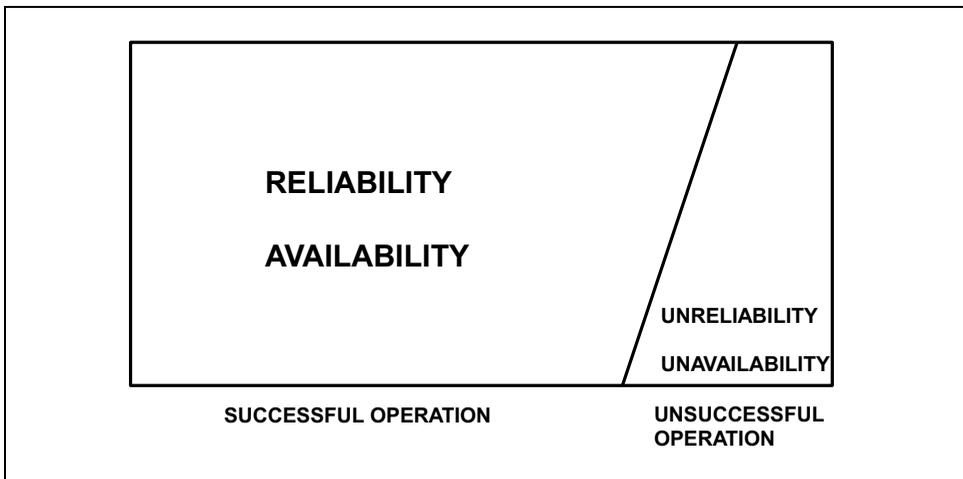


Figure 4-2. Successful – Unsuccessful Operation

Unavailability

Unavailability, a measure of failure, is also used for repairable devices. It is defined as “the probability that a device is not successful (is failed) at any moment in time.” Unavailability is the one’s complement of availability; therefore,

$$U(t) = 1 - A(t) \tag{4-4}$$

EXAMPLE 4-1

Problem: A controller has an availability of 0.99. What is the unavailability?

Solution: Using Equation 4-4, unavailability = $1 - 0.99 = 0.01$.

Probability of Failure

The probability of failure during any interval of operating time is given by a probability density function (See Chapter 2). Probability density functions for failure probability are defined as

$$f(t) = \frac{dF(t)}{dt} \quad (4-5)$$

The probability of failure function can be mathematically described in terms of the random variable T :

$$\lim_{\Delta t \rightarrow 0} P(t < T \leq t + \Delta t) \quad (4-6)$$

This can be interpreted as the probability that the failure time, T , will occur between a point in time t and the next interval of operation, $t + t$, and is called the “probability of failure function.”

The probability of failure function can provide failure probabilities for any time interval. The probability of failure between the operating hours of 2000 and 2200, for example, is:

$$P(2000, 2200) = \int_{2000}^{2200} f(t) dt \quad (4-7)$$

Mean Time to Failure (MTTF)

One of the most widely used reliability parameters is the MTTF. Unfortunately, it is also sometimes misused and misunderstood. It has been misinterpreted as “guaranteed minimum life.” Consider Table 4-1. The MTTF of 3,248 hours was calculated using a simple averaging technique. One of the modules failed after only 70 hours, however.

MTTF is merely the mean or “expected” failure time. It is defined from the statistical definition of expected or “mean” value (Equation 2-10). Using the random variable operating time interval, t , and recognizing that there

EXAMPLE 4-2

Problem: A valve positioner has an exponential probability of failure function (constant failure rate)

$$f(t) = 0.0002e^{-0.0002t}$$

What is the probability that it will fail after the warranty (6 months, 4,380 hr) and before plant shutdown (12 months, 8760 hr)?

Solution: Using Equation 4-7,

$$P(4380, 8760) = \int_{4380}^{8760} 0.0002e^{-0.0002t} dt$$

This evaluates to

$$P(4380, 8760) = -e^{-0.0002 \times 8760} - (-e^{-0.0002 \times 4380})$$

Calculating the result:

$$P(4380, 8760) = -0.1734 + 0.4165 = 0.243$$

This result states that the probability of failure during the interval from 4380 hours to 8760 hours is 24.3%.

is no negative time we can update the mean value equation and substitute the probability density function $f(t)$:

$$E(t) = \int_0^{+\infty} tf(t)dt \quad (4-8)$$

Substituting

$$f(t) = -\frac{d[R(t)]}{dt} \quad (4-9)$$

into the expected value formula yields

$$E(t) = -\int_0^{+\infty} td[R(t)]$$

Integrating by parts, this equals:

$$E(T) = [-tR(t)]_0^{\infty} - \left[- \int_0^{+\infty} R(t)dt \right]$$

The first term equals zero at both limits. This leaves the second term, which equals MTTF:

$$MTTF = E(T) = \int_0^{+\infty} R(t)dt \quad (4-10)$$

Thus, in reliability theory, the definition of MTTF is the definite integral evaluation of the reliability function. Note that the definition of MTTF is *NOT* related to the inverse of (failure rate), that is only a special case derived for a constant failure rate as noted below.

$$MTTF \neq \frac{1}{\lambda} \text{ by definition} \quad (4-11)$$

NOTE: The formula $MTTF = 1/\lambda$ is valid for single components with a constant failure rate or a series of components, all with constant failure rates. See “The Constant Failure Rate” later in this chapter.

Mean Time to Restore (MTTR)

MTTR is the “expected value” or mean of the random variable restore time (or time to restore a failed device to full operation), not failure time. The definition includes the time required to detect that a failure has occurred and to identify it as well as the time required to make the repair. The term MTTR applies only to repairable devices. Figure 4-3 shows that MTTF represents the average time required to move from successful operation to unsuccessful operation. MTTR is the average time required to move from unsuccessful operation to successful operation. The term Mean Dead Time (MDT) is an older term which means the same as MTTR.

Mean Time Between Failures (MTBF)

MTBF is a term that applies only to repairable systems. Like MTTF and MTTR, it is an average value, but it is the time between failures. This implies that a device has failed and then has been repaired. For a repairable device,

$$MTBF = MTTF + MTTR \quad (4-12)$$

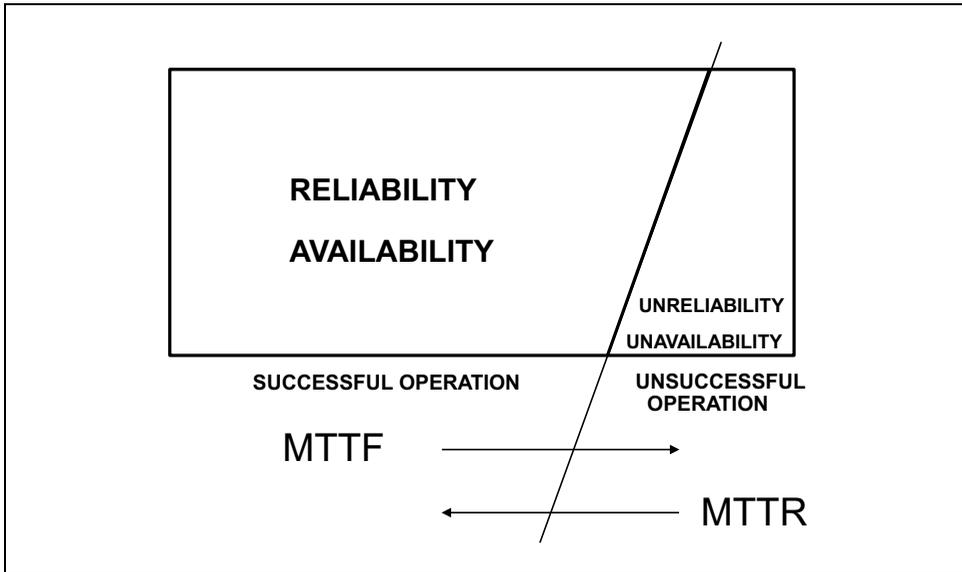


Figure 4-3. MTTF and MTTR in Operation

Figure 4-4 shows a graphical representation of MTTF, MTTR, and MTBF.

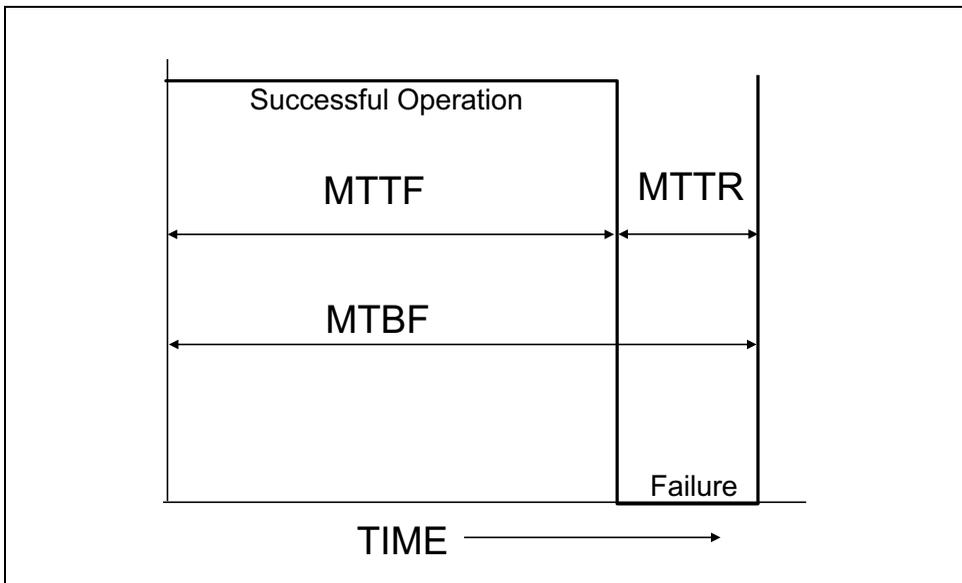


Figure 4-4. MTTF, MTTR, and MTBF

The term MTBF has been misused. Since MTTR is usually much smaller than MTTF, MTBF is often approximately equal to MTTF. MTBF, which by definition only applies to repairable systems, is often substituted for MTTF, which applies to both repairable and non-repairable systems.

EXAMPLE 4-3

Problem: A power supply module is potted in epoxy. The manufacturer quotes “MTBF equals 50,000 hours.” Is this term being used correctly?

Solution: This power supply is potted in epoxy. Although it can be argued that it is possible to repair the unit, it is generally not practical. The term MTBF applies to equipment that is designed to be repairable, and has been misused in this case.

EXAMPLE 4-4

Problem: An industrial I/O module contains 16 circuit assemblies mounted in sockets. The manufacturer claims that the module has an MTBF of 20,000 hours. Is the term MTBF being used correctly?

Solution: The module has been designed to be repairable. MTBF is appropriate although MTTF is preferable since average time to failure is the variable of interest. The manufacturer has no direct control over MTTR.

EXAMPLE 4-5

Problem: An industrial I/O module has an MTTF of 87,600 hours. When the module fails, it takes an average of 2 hours to repair. What is the MTBF?

Solution: Using formula 4-12, the $MTBF = 87,602$ hours. The MTBF is effectively equal to the MTTF.

EXAMPLE 4-6

Problem: An industrial I/O module has an MTTF of 87,400 hours. When the module fails, it takes an average of 400 hours to repair. What is the MTBF?

Solution: Using formula 4-12, the $MTBF = 87,800$ hours. It is interesting to note that compared to the module of example 4-5, this module will fail sooner (it has a lower MTTF). Using the MTBF number as a positive indicator would be misleading. MTTF is a more precise term than MTBF for the measurement of successful operation.

Failure Rate

Failure rate, often called “hazard rate” by reliability engineers, is a commonly used measure of reliability that gives the number of failures per unit time from a quantity of components exposed to failure.

$$\lambda(t) = \frac{\text{Failures per Unit Time}}{\text{Quantity Exposed}} \quad (4-13)$$

Failure rate has units of inverse time. It is a common practice to use units of “failures per billion (10^9) hours.” This unit is known as FIT for Failure InT. For example, a particular integrated circuit will experience seven failures per billion operating hours at 25°C and thus has a failure rate of seven FITs.

Note that the measure “failure rate” is most commonly attributed to a single component. Although the term can be correctly applied to a module, unit, or even system where all components are needed to operate (called a series system), it is a measure derived in the context of a single component.

EXAMPLE 4-7

Problem: 300 power resistors have been operating in a plant for seven years. Five failures have occurred. What is the average failure rate for this group of resistors?

Solution: Using formula 4-13, the average failure rate is $5/(295 \times 7 \times 8760) = 0.000000271798 = 276$ FITs. Note that a worst case assumption was used where all five failures occurred at the beginning of the seven years. If exact failure times were available, a more accurate number could be calculated.

The failure rate function is related to the other reliability functions. It can be shown that

$$\lambda(t) = \frac{f(t)}{R(t)} \quad (4-14)$$

Time-Dependent Failure Rates

If a collection of 50 transformers were put on life test, the time when any transformer fails could be recorded. An extremely stressful environment could be created to accelerate failures. A check to see how many transformers fail each week may show whether the percentage of failures decreases, increases, or stays constant.

Consider the failure log for a highly accelerated life test (HALT) as shown in Table 4-2. The number of failures is decreasing during the first few weeks. The number then remains relatively constant for many weeks. Toward the end of the test the number begins to increase.

“Failure rate” is calculated in column four and equals the number of failures divided by the number of module hours (surviving modules times hours) in each weekly period. The failure rate also decreases at first, then remains relatively constant, and finally increases. These changes in the failure rates of components are typically due to several factors including variations in strength and strength degradation with time. Note that, in such a test, the type and level of stress do not change.

Table 4-2. Life Test Data

WEEK	Number Surviving (beg. of week)	Failures	Failure Rate
1	50	9	0.0011
2	41	5	0.0007
3	36	3	0.0005
4	33	2	0.0004
5	31	2	0.0004
6	29	1	0.0002
7	28	2	0.0004
8	26	1	0.0002
9	25	1	0.0002
10	24	0	0.0000
11	24	2	0.0005
12	22	1	0.0002
13	21	1	0.0003
14	20	0	0.0000
15	20	1	0.0003
16	19	0	0.0000
17	19	1	0.0003
18	18	1	0.0003
19	17	0	0.0000
20	17	1	0.0003
21	16	1	0.0004
22	15	0	0.0000
23	15	1	0.0004
24	14	0	0.0000
25	14	1	0.0004
26	13	0	0.0000
27	13	1	0.0005
28	12	0	0.0000
29	12	1	0.0005
30	11	0	0.0000
31	11	1	0.0005
32	10	1	0.0006
33	9	1	0.0007
34	8	1	0.0007
35	7	1	0.0008
36	6	1	0.0010
37	5	2	0.0024
38	3	3	0.0059

Decreasing Failure Rate

A decreasing failure rate is characteristic of a “fault removal process.” Consider a collection of components in which a portion of the components have manufacturing defects. The entire collection of components is placed on an accelerated life test. Since manufacturing defects reduce the strength of a component, the components with defects will fail in a relatively short period of time. Failed components are removed from the test. After a period of time, no components that have manufacturing defects remain in the collection. The failure rate due to manufacturing defects will have dropped to zero (Figure 4-5).

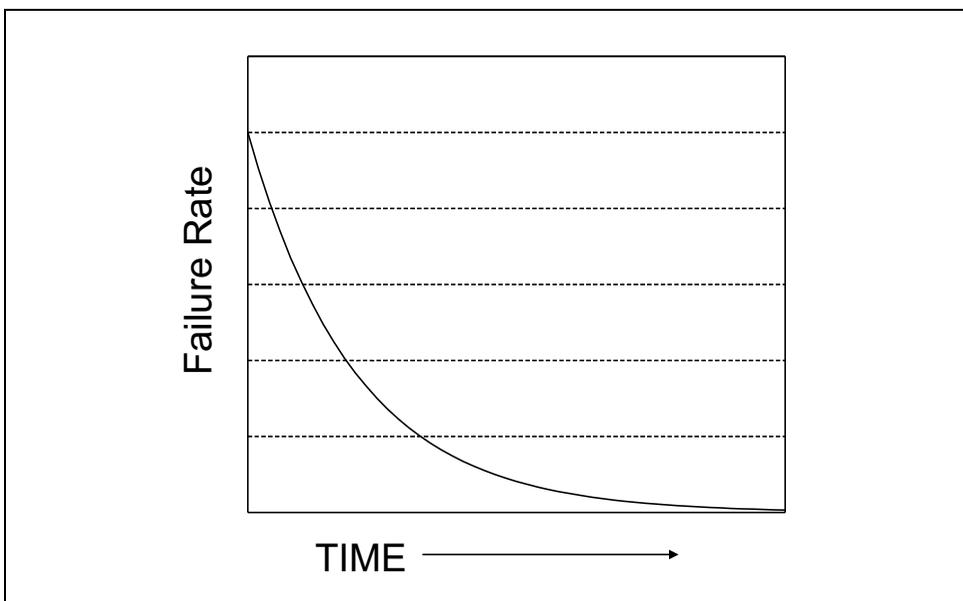


Figure 4-5. Decreasing Failure Rate

Constant Failure Rate

If failures in a large collection of components are due to uniform stresses from the environment and the strength is relatively constant, the failure rate for a large collection tends to be constant (refer back to Figure 3-10, which shows an approximately constant failure rate). This tends to happen because many stresses of many different types appear to behave like a uniform stress.

Increasing Failure Rate – Wear-out

The process of wear can be thought of as a gradual reduction in strength; eventually the strength drops below that required for normal use.

Some components have consumable resources. When the resource is gone, the component is worn out. A battery is an obvious example of a component with a consumable resource. A motor bearing is another example. In the case of the battery, chemical “wearout” occurs. In the case of the motor bearing, a mechanical wearout occurs. Consumption (or wear) occurs in these two components primarily as a function of use. Other components have wearout mechanisms that are independent of use. Electrolyte within an electrolytic capacitor will evaporate. This wearout process occurs even if the component is not being used (although at a slower rate).

Components wear at different rates. Imagine a life test of 100 fan motors in which the motor bearings wore at exactly the same rate; one day all the motors would fail at the same instant. Because components do not wear at the same rate, they do not fail at the same time. However, as a group of components approach wear-out, the failure rate increases.

Reductions in strength (wear) occur in other ways. Some failures are caused only by repeated stress events. Each stress event lowers component strength. Electrostatic discharge (ESD) is an example of this. Each time a component receives an ESD strike, it is damaged, and its strength is reduced. After some number of ESD hits, component strength drops below that required for normal operation and the component fails. Any strength reduction process will result in an increasing failure rate.

Bathtub Curve

As we have seen, a group of components will likely be exposed to many kinds of environmental stress: chemical, mechanical, electrical, and physical. The strength factors as initially manufactured will vary and strength will change at different rates as a function of time. When the failure rates due to these different failure sources are superimposed, the well-known “bathtub curve” results.

The failure rate of a group of components decreases in early life. The left part of the curve has been called the “roller coaster” curve (Ref. 2, 3). The failure rate will be relatively constant after the components containing manufacturing defects are removed. This failure rate can be very low if the components have few design faults and high strength. As physical resources on the components are consumed or if other strength reduction factors come into play, the failure rate increases (sometimes rapidly), completing the right side of the “bathtub” (Figure 4-6).

Many variations of the bathtub curve exist. In some cases, no wearout region exists. Some components rarely have manufacturing defects that are not detected during the manufacturing test process, and these components do not have a decreasing failure rate region.

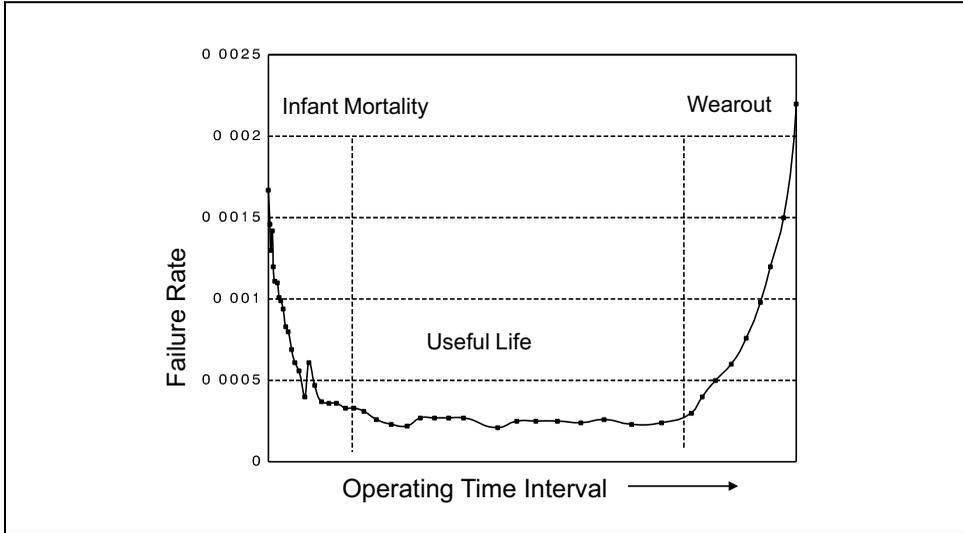


Figure 4-6. Bathtub Curve

The Constant Failure Rate

A useful probability density function in the field of reliability engineering is the exponential. For this distribution:

$$f(t) = \lambda e^{-\lambda t} \quad (4-15)$$

By integrating this function it can be determined that

$$F(t) = 1 - e^{-\lambda t} \quad (4-16)$$

and

$$R(t) = e^{-\lambda t} \quad (4-17)$$

The failure rate equals

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

This says that a collection of components that have an exponentially decreasing probability of failure will have a constant failure rate. The constant failure rate is very characteristic of many kinds of products. As seen in the stress-strength simulations, this is characteristic of a relatively constant strength and a random stress. Other products typically exhibit a decreasing failure rate. In these cases, though, the constant failure rate represents a worst-case assumption and can still be used.

The MTTF of a device with an exponential probability density function (PDF) can be derived from the definition of MTTF that was presented earlier:

$$MTTF = \int_0^{+\infty} R(t) dt$$

Substituting the exponential reliability function:

$$MTTF = \int_0^{+\infty} e^{-\lambda t} dt$$

and integrating,

$$MTTF = -\frac{1}{\lambda} [e^{-\lambda t}]_0^{\infty}$$

When the exponential is evaluated, the value at $t = \text{infinity}$ is zero and the value at $t = 0$ is one. Substituting these results, we have a solution:

$$MTTF = -\frac{1}{\lambda} [0 - 1] = \frac{1}{\lambda} \quad (4-18)$$

Equation 4-18 is valid for single components with an exponential PDF or a series system (a system where all components are required for successful operation) composed of components, all of which have an exponential PDF.

EXAMPLE 4-8

Problem: A motor has a constant failure rate of 150 FITs. What is the motor reliability for a mission time of 1000 hours?

Solution: Using Equation 4-17, values are substituted including the failure rate of 150/1,000,000,000 and the time interval of 1000.

$$\begin{aligned} R(1000) &= e^{-0.00000015 \times 1000} \\ &= e^{-0.00015} \\ &= 0.99985 \end{aligned}$$

EXAMPLE 4-9

Problem: Calculate the MTTF of the motor from Example 4-8.

Solution: Since the motor has an exponential PDF, Equation 4-18 can be used. Therefore:

$$\begin{aligned} MTTF &= \frac{1}{0.00000015} \\ &= 6,666,666.7 \text{ hr} \end{aligned}$$

EXAMPLE 4-10

Problem: Field failure records from a component indicate it has an average failure rate of 276 FITs. What is the component reliability for a mission time of 8760 hours (one year)?

Solution: Assuming a constant failure rate using Equation 4-17, values are substituted including the failure rate of 276/1,000,000,000 and the time interval of 8760.

$$\begin{aligned} R(t) &= e^{-0.000000276 \times 8760} \\ &= 0.9976 \end{aligned}$$

EXAMPLE 4-11

Problem: Calculate the MTTF of the component from Example 4-10.

Solution: Since the component has an exponential PDF, Equation 4-18 can be used. Therefore:

$$MTTF = \frac{1}{0.000000276} = 3,623,188 \text{ hr}$$

A Useful Approximation

Mathematics has shown how certain functions can be approximated by a series of other functions. One of these approximations can be useful in reliability engineering. For all values of x , it can be shown that

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots \quad (4-19)$$

For a sufficiently small x , the exponential can be approximated:

$$e^x = 1 + x$$

A rearrangement yields

$$1 - e^{-x} \approx x$$

Substituting gives the result:

$$1 - e^{-\lambda t} \approx \lambda t$$

A single component (or series of components) with an exponential PDF has a failure probability that equals

$$P(\text{failure}) = 1 - e^{-\lambda t} \approx \lambda t \quad (4-20)$$

when λt is small.

Thus, this probability can be approximated by substituting the times t value. This can save engineering time. However, be careful. The approximation degrades with higher values of failure rates and interval times. The approximate probability of failure numbers become higher. Remember, this is not a fundamental formula—only an approximation.

EXAMPLE 4-12

Problem: A component has an exponential probability of failure. The failure rate (λ) is 0.00001 failures per hour. We wish to calculate the probability of failure for a 1000 hour mission. If we use the approximation, what is the error?

Solution: Using Equation 4-20, the probability of failure can be approximated.

$$P(\text{failure}) = 0.00001 \times 1000 = 0.01$$

To check the error, the full formula must be used.

$$F(1000) = 1 - e^{-0.1} = 0.09950166.$$

In this case, the error is 0.00004983375, this is a 0.498% error. Note that the approximation gives a pessimistic result. This is on the conservative side when dealing with probabilities of failure, which is usually a safe approach.

Steady-State Availability – Constant Failure Rate Components

Remember that reliability and availability are different. Availability defines the chances of success with a repairable component, one that may or may not be in operating condition when called upon to function. Availability represents the percentage uptime of a device. Availability over a long period of time, steady-state availability, is usually the desired measurement. For long-term conditions it is assumed that the “restore rate” ($1/\text{MTTR}$) is constant. Restore rate is frequently represented by the lower case Greek letter μ (mu). The formula is:

$$\mu = \frac{1}{\text{MTTR}} \quad (4-21)$$

EXAMPLE 4-13

Problem: Diagnostics detect when a failure occurs within three seconds. The average failure detection and repair time is 4 hours. Assume a constant restore rate. What is the constant restore rate?

Solution: Using Equation 4-21,

$$\mu = \frac{1}{4} = 0.25$$

For single components with a constant failure rate and a constant restore rate, steady-state availability can be calculated (see Chapter 8 for more detail) using the formula:

$$A = \frac{\mu}{\lambda + \mu} \quad (4-22)$$

Substituting equations 4-18 and 4-21 into 4-22 yields:

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \quad (4-23)$$

This is a common formula for steady-state availability. Note that it has been derived for a single component with a constant failure rate and a constant restore rate. It will be shown later in the book that it also applies to series systems but—NOTE—it does not apply to many types of systems including parallel systems—systems with redundancy.

EXAMPLE 4-14

Problem: An industrial motor has an MTTF rating of 25 years. Assuming a constant failure rate, what is its failure rate?

Solution: Using Equation 4-18, $\lambda = 1/\text{MTTF} = \lambda/(25 \times 8760) = 0.000004566$ failures per hour.

EXAMPLE 4-15

Problem: An industrial motor has an MTTF rating of 25 years. Assuming a constant failure rate, what is the reliability for a one year period of operation?

Solution: Using Equation 4-17 with $\lambda = 0.000004566$ failures per hour (4566 FITs):

$$R(t) = e^{-0.000004566 \times 8760} = 0.9607.$$

The reliability can also be calculated using the approximation method. Unreliability = $\lambda t = 0.04$ and reliability = $1 - 0.04 = 0.96$. This is a quicker and more pessimistic answer.

EXAMPLE 4-16

Problem: An industrial motor has an MTTF rating of 25 years. Assuming a constant failure rate and a constant restore rate of 0.25 (4 hours MTTR), what is the steady-state availability?

Solution: Using Equation 4-23, $A = \text{MTTF} \div (\text{MTTF} + \text{MTTR}) = 0.99998$.

EXAMPLE 4-17

Problem: An industrial motor has an MTTF rating of 100 years. Assuming a constant failure rate and an MTTR of 4 hours, what is the reliability for a one year period of operation and the steady-state availability?

Solution: Using Equation 4-18, $\lambda = 1/\text{MTTF} = 1/(100 \times 8760) = 0.000001142$, (1142 FITs).

Using Equation 4-17 with $\lambda = 0.000001142$ failures per hour:

$$R(t) = e^{-0.000001142 \times 8760} = 0.99.$$

Equation 4-23, $A = \text{MTTF} \div (\text{MTTF} + \text{MTTR}) = (100 \times 8760) \div ((100 \times 8760) + 4) = 0.999995$.

Safety Terminology

When evaluating system safety an engineer must examine more than the probability of successful operation. Failure modes of the system must also be reviewed. The normal metrics of reliability, availability, and MTTF only suggest a measure of success. Additional metrics to measure safety include probability of failure on demand (PFD), average probability of failure on demand (PFDavg), risk reduction factor (RRF), and mean time to fail dangerously (MTTFD). Other related terms are probability of failing safely (PFS), mean time to fail safely (MTTFS), and diagnostic coverage. These terms are especially useful when combined with the other reliability engineering terms.

Failure Modes

A “failure mode” describes the way in which a device fails. Failure modes must be considered in systems designed for safety protection applications, called Safety Instrumented Systems (SIS). Two failure modes are important—safe and dangerous. ISA standard 84.00.01-2004 (IEC 61511 Mod.) defines “safe state” as “state of the process when safety is achieved.” In the majority of the most critical applications, designers choose a de-energized condition as the safe state. Thus a safe failure mode describes any failure that causes the device to go to the safe state. A device designed for these safety protection applications should de-energize its outputs to achieve a safe state. Such a device is called “normally energized.”

When a normally energized device is operating successfully (Figure 4-7), the input circuits read the sensors, perform calculation functions, and generate outputs. Input switches are normally energized to indicate a safe condition. Output circuits supply energy to a load (usually a valve). The sensor switch opens (de-energizes) in response to a potentially dangerous condition. If the logic solver (typically a safety PLC) is programmed to recognize the sensor input as a potentially dangerous condition it will de-energize its output(s). This action is designed to mitigate the danger.

A safe failure in such a device (Figure 4-8) happens when the output de-energizes even though there is no potentially dangerous condition. This is frequently called a “false trip.” There are many different reasons that this can happen. Input circuits can fail in such a way that the logic solver thinks a sensor indicates danger when it does not. The logic solver itself can miscalculate and command the output to de-energize. Output circuits can fail open circuit. Many of the components within an SIS can fail in a mode that will cause the system to fail safely.

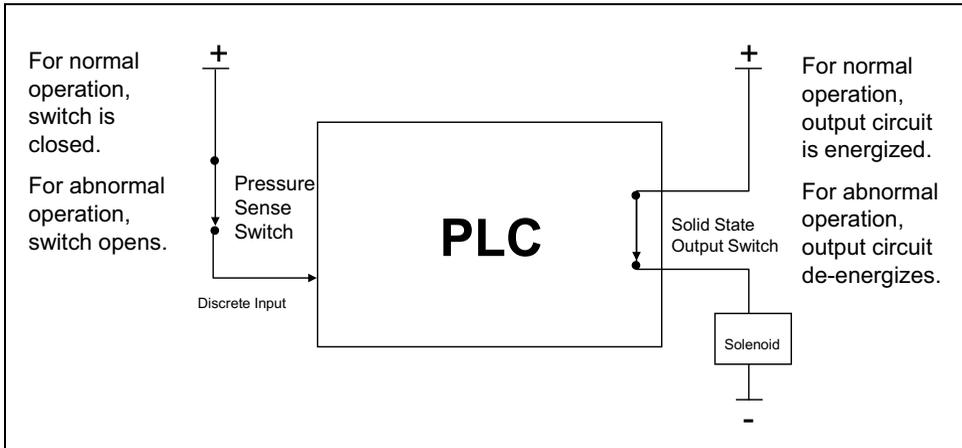


Figure 4-7. Successful Operation – Normally Energized System

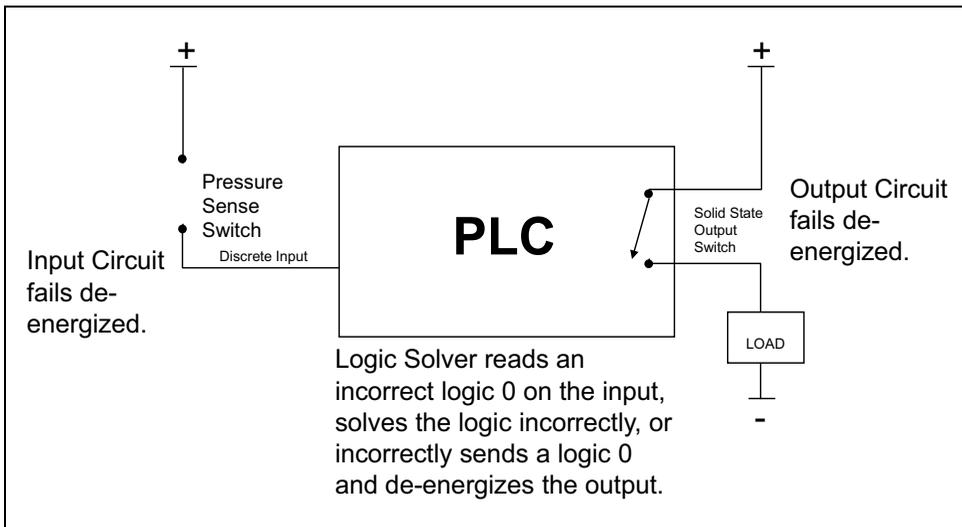


Figure 4-8. Safe Failure – Normally Energized System

Dangerous failures are defined as those failures which prevent a device from responding to a potentially dangerous condition known as a "demand." Figure 4-9 shows this situation.

There are many component failures that might cause dangerous system failure, especially if a system is not designed for high safety. An IEC 61508 Certified PLC is specifically designed to avoid this failure mode using a number of design techniques.

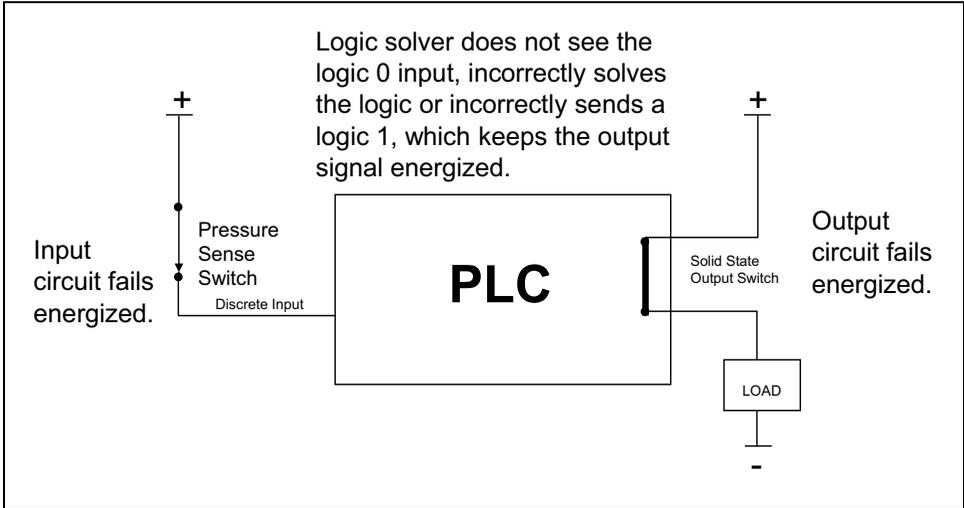


Figure 4-9. Dangerous Failure – Normally Energized System

PFS/PFD/PFDavg

There is a probability that a normally energized SIS will fail with its outputs de-energized. This is called probability of failure safely (PFS). There is also a probability that the system will fail with its outputs energized. This is called probability of failure on demand (PFD). The term refers to the fact that when a safety protection system is failed dangerously, it will NOT respond when a demand occurs. Figure 4-10 shows the relationship of safe and dangerous failure modes to overall system operation.

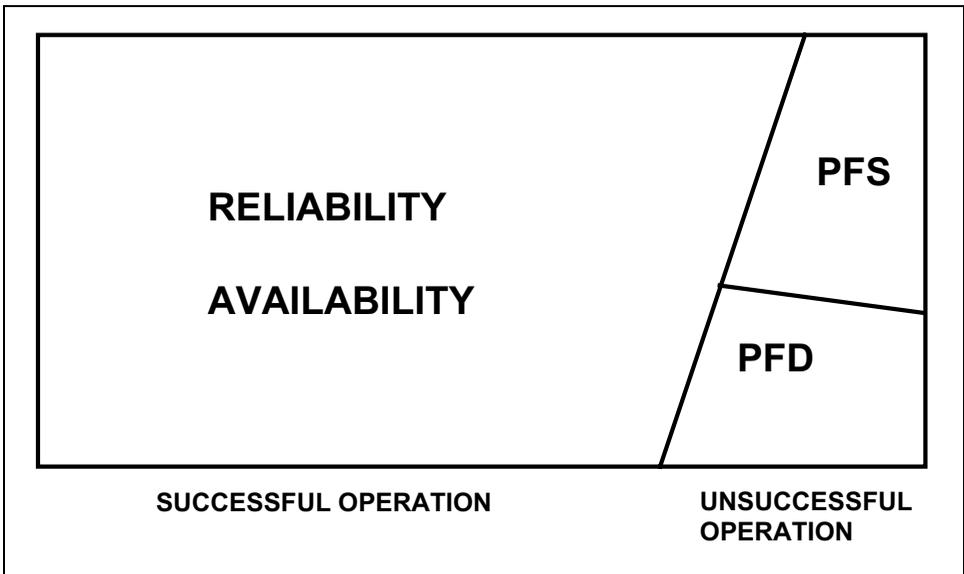


Figure 4-10. Failure Modes

Unavailability was defined as the probability that a device is not successful at any moment in time. Unavailability includes all failure modes, therefore for repairable systems:

$$U(t) = PFS(t) + PFD(t) \quad (4-24)$$

and availability:

$$A(t) = 1 - [PFS(t) + PFD(t)] \quad (4-25)$$

This applies for time dependent calculations or steady-state calculations.

EXAMPLE 4-18

Problem: A steady-state PFS value of 0.001 and a steady-state PFD value of 0.0001 have been calculated for an SIS. What is the availability?

Solution: Using equation 4-25, the availability = $1 - (0.001 + 0.0001) = 0.9989$.

PFD average (PFD_{avg}) is a term used to describe the average probability of failure on demand. PFD_{avg} is defined as:

$$PFD_{avg} = \frac{1}{T} \int_0^T PFD(t) dt \quad (4-26)$$

Since PFD increases with time, the average value over a period of time is typically calculated numerically (Figure 4-11).

MTTFS/MTTFD

As has been mentioned, MTTF describes the average amount of time until a device fails. The definition includes all failure modes. In industrial control systems, the measure of interest is the average operating time between failures of a particular mode, ignoring all other modes. In the case of an SIS, the mean time to fail safely (MTTFS) and the mean time to fail dangerously (MTTFD) are of interest.

The exact definition of mean time to failure in any mode must be explained. Consider the failure times of Table 4-3. Assume that one PLC is being measured. It starts operating at time $t = 0$ and fails dangerously after 2327 hours. It is then repaired and operates another 4016 hours before it fails safely. After repair it operates another 4521 hours before failing dan-

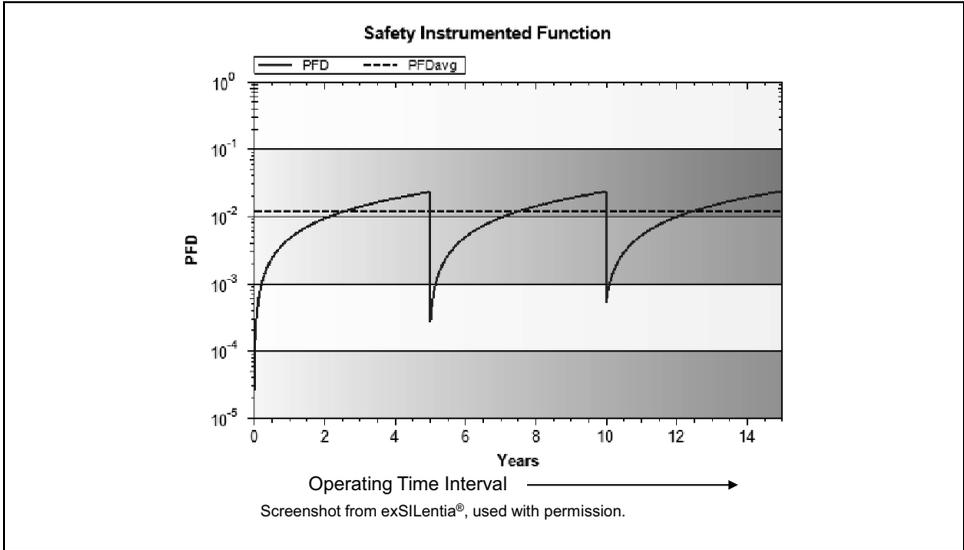


Figure 4-11. PFD and PFDavg

gerously again. So far the system has failed dangerously twice. The first time occurs after operating 2327 hours. The second time occurs after operating 8537 hours (4016 + 4521). The PLC is again repaired and placed in service, and the failure times shown in Table 4-3 are recorded.

Table 4-3. PLC System Failure Times

	Time to Fail	Mode
Failure 1	2327 Hrs.	Dangerous
Failure 2	4016 Hrs.	Safe
Failure 3	4521 Hrs.	Dangerous
Failure 4	3176 Hrs.	Safe
Failure 5	0070 Hrs.	Safe
Failure 6	3842 Hrs.	Safe
Failure 7	3154 Hrs.	Safe
Failure 8	2017 Hrs.	Dangerous
Failure 9	5143 Hrs.	Safe
Failure 10	4215 Hrs.	Dangerous

EXAMPLE 4-19

Problem: A PLC has measured failure data from Table 4-3. What is the MTTFD?

Solution: Four dangerous failures are recorded. The total operating times are:

- First dangerous failure = 2327 hours.
- Second dangerous failure = 8537 hours (4016 + 4521)
- Third dangerous failure = 12,259 hours (3176+70+3842+3154+2017)
- Fourth dangerous failure = 9358 hours (5143 + 4215)

The average of these four values is 8120 hours. Another way to calculate the MTTFD would be to note that the total operating hours is 32481 divided by four dangerous failures.

The MTTFs would be determined in a similar way, using the safe failures.

Diagnostic Coverage

The ability to detect a failure is an important feature in any control or safety system. This feature can be used to reduce repair times and to control operation of several fault tolerant architectures. The measure of this ability is known as the diagnostic coverage factor, C. The diagnostic coverage factor measures the probability that a failure will be detected given that it occurs. Diagnostic coverage is calculated by adding the failure rates of detected failures and dividing by the total failure rate, which is the sum of the individual failure rates. As an example consider a system of ten components. The failure rates and detection performance are shown in Table 4-4:

Table 4-4. Diagnostic Performance

Component 1	0.00991 failures per hour	Detected
Component 2	0.00001 failures per hour	NOT detected
Component 3	0.00001 failures per hour	NOT detected
Component 4	0.00001 failures per hour	NOT detected
Component 5	0.00001 failures per hour	NOT detected
Component 6	0.00001 failures per hour	NOT detected
Component 7	0.00001 failures per hour	NOT detected
Component 8	0.00001 failures per hour	NOT detected
Component 9	0.00001 failures per hour	NOT detected
Component 10	0.00001 failures per hour	NOT detected

Although only one component failure out of a possible ten is detected, the coverage factor is 0.991 (or 99.1%). For this example the detected failure rate is 0.00991. This number is divided by the total failure rate of 0.01. The coverage factor is not 0.1 as might be assumed by dividing the number of detected failures by the total number of known possible failures. Note that the result would have been quite different if Component 1 was NOT detected, while Component 2 was detected.

In control system reliability and safety analysis, it is generally necessary to define the coverage factor for safe failures and the coverage factor for dangerous failures. The superscript S is used for the safe coverage factor, C^S . The superscript D is used for the dangerous coverage factor, C^D . The evaluation of PFS and PFD will be affected by each different coverage factor.

In some fault tolerant architectures, two additional coverage factor designations may be required. Detection of component failures is done by two different techniques, classified as reference and comparison. Reference diagnostics can be done by a single unit. The coverage factor of reference diagnostics will vary widely depending on the implementation, with most results ranging from 0.0 to 0.999. Comparison diagnostics will require two or more units. The coverage factor depends on implementation but results are generally good, with most results ranging from 0.9 to 0.999.

Reference diagnostics utilize the predetermined characteristics of a successfully operating unit. Comparisons are made between actual measured parameters and the predetermined values for these parameters. Measurements of voltages, currents, signal timing, signal sequence, temperature, and other variables are used to accurately diagnose component failures. Advanced reference diagnostics include digital signatures and frequency domain analysis.

Comparison diagnostic techniques depend on comparing data between two or more operating units within a system. The coverage factor will vary since there are tradeoffs between the amount of data compared and diagnostic coverage effectiveness.

In some fault tolerant architectures the diagnostic coverage factor changes when the system is operating in a degraded condition. The appropriate coverage factor must be used in reliability and safety analysis depending on the operational state of the system. When fault tolerant systems that normally compare, degrade to a single operational unit, the comparison must stop and the reference coverage factor must be used. The following coverage factor notation is defined:

C - Coverage due to reference diagnostics, comparison diagnostics, or a combination of both

C_1 - Coverage due to single unit reference diagnostics

C_2 - Coverage due to comparison diagnostics

where C is equal to or greater than either number.

The terms C_1 and C_2 can be used for specific failure modes, such as safe and dangerous, as well as resulting in terms:

C_1^S - Coverage for safe failures due to single unit reference diagnostics

C_2^S - Coverage for safe failures due to comparison diagnostics

C_1^D - Coverage for dangerous failures due to single unit reference diagnostics

C_2^D - Coverage for dangerous failures due to comparison diagnostics

Exercises

- 4.1 Which term requires successful operation for an interval of time: reliability or availability?
- 4.2 Which term is more applicable to repairable systems: reliability or availability?
- 4.3 Unavailability for a system is given as 0.001. What is the availability?
- 4.4 When does the formula $MTTF = 1/\lambda$ apply?
- 4.5 Availability of the process control system is quoted as 99.9%. What is the unavailability?
- 4.6 A control module has an MTTF of 60 years. Assuming a constant failure rate, what is the failure rate?
- 4.7 A control module has an MTTF of 60 years. It has an average repair time of 8 hours. What is the steady-state availability?
- 4.8 A control module has an MTTF of 60 years. What is the reliability of this module for a time period of six months?
- 4.9 An SIS has a PFS of 0.002 and a PFD of 0.001. What is the availability?

Answers to Exercises

- 4.1 Reliability.
- 4.2 Availability.
- 4.3 Availability = 0.999.
- 4.4 The formula $MTTF = 1/\lambda$ applies to single components with a constant failure rate or series systems with a constant failure rate.
- 4.5 Unavailability = 0.001.
- 4.6 The failure rate equals $0.000001903 = 1903$ FITs.
- 4.7 Availability = 0.9999847.
- 4.8 Reliability = 0.9917.
- 4.9 Availability = 0.997.

References

1. Billinton, R., and Allan, R. N. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. NY: New York, Plenum Press, 1983.
2. Wong, K. L. "Off the Bathtub onto the Roller-Coaster Curve." *Proceedings of the Annual Reliability and Maintainability Symposium*, NY: New York, IEEE, 1988.
3. Wong, K. L. "The Physical Basis for the Roller-Coaster Hazard Rate Curve for Electronics." *Quality and Reliability Engineering International*, Vol. 7, No. 6. Sussex, England: John Wiley & Sons Ltd., 1991.