CHAPTER 11

Measurement Reliability and Safety Systems

Chapter Outline

Measurement and Instrumentation. http://dx.doi.org/10.1016/B978-0-12-800884-3.00011-3

11.1 Introduction

In the previous chapters of this book, we have discussed the design of measurement systems and we have said a lot about how the performance of measurement systems in respect of parameters like accuracy can be improved. However, this earlier discussion has mainly been about the attributes of measurement system when they are new. We have considered the effects of the passage of time only in respect of noting that the characteristics of measurement system degrade over time and have to be restored back to their starting point by the process of recalibration. What we have not so far considered is the possibility of faults developing in measurement systems. At best, these faults impair the performance of the system and, at worst they cause the system to stop working entirely. In safety-critical applications, measurement system faults can also have a serious adverse effect on the larger system that the measurement system is part of.

It is therefore appropriate for us to devote this chapter to a study of measurement system reliability issues and their effect on safety. We will start off by looking at how reliability is formally defined and we will say something about its theoretical principles. This will then lead us on to consider ways in which reliability can be quantified. We will look particularly at two laws that quantify the reliability of system components that are in series and in parallel with one another. This will enable us to examine how these laws can be applied to improve the reliability of measurement systems. We will also look at the general precautions that can be taken to reduce the failure rate of instruments, including choosing instruments that can withstand the operating conditions expected, protecting them adequately against damage during use, calibrating them at the prescribed intervals to ensure that measurement inaccuracy remains within acceptable bounds and duplicating critical measurement system components.

Since software is an important contributor to measurement system reliability, particularly with the current widespread use of intelligent devices, we will extend our treatise on reliability to consider the reliability of the software within a measurement system. We will see that the factors affecting reliability in software are fundamentally different to those affecting the reliability of hardware components. This is because software does not change with time. Therefore, we will realize that the reliability of software has to be quantified in terms of the probability of failure of the software because of some undetected error in the software that has existed since it was written. This kind of failure usually occurs when some particular combination of input data is applied to the software and, in consequence, may not occur until the software has been in use for some considerable period of time. Having established a satisfactory way of quantifying software reliability, we will go on to consider what can be done to improve reliability.

Our final consideration in this chapter will be system safety. We will see that measurement systems can have an impact on system safety in two main ways. Firstly, failure of the measurement system may cause a dangerous situation to arise in a process because incorrect data are fed into the process control system. Secondly, the process itself may develop a dangerous fault that the measurement system fails to detect, thus preventing the operation of emergency responses like the sounding of alarms or the opening of pressure-relief valves etc. In order to respond to the potential safety problems associated with the malfunction of measurement systems, we will look at the main ways available in designing safety systems.

11.2 Reliability

The reliability of measurement systems can be quantified as the mean time between faults occurring in the system. In this context, a fault means the occurrence of an unexpected condition in the system that causes the measurement output to either be incorrect or not to exist at all. The following sections summarize the principles of reliability theory that are relevant to measurement systems. A fuller account of reliability theory, and particularly its application in manufacturing systems, can be found elsewhere (Morris, 1997).

11.2.1 Principles of Reliability

The reliability of a measurement system is defined as the ability of the system to perform its required function within specified working conditions for a stated period of time. Unfortunately, factors such as manufacturing tolerances in an instrument and varying operating conditions conspire to make the faultless operating life of a system impossible to predict. Such factors are subject to random variation and chance, and therefore reliability cannot be defined in absolute terms. The nearest one can get to an absolute quantification of reliability are quasi-absolute terms like the mean-time-between-failures, which expresses the average time that the measurement system works without failure. Otherwise, reliability has to be expressed as a statistical parameter that defines the probability that no faults will develop over a specified interval of time.

In quantifying reliability for a measurement system, an immediate difficulty that arises is defining what counts as a fault. Total loss of a measurement output is an obvious fault, but a fault that causes a finite but incorrect measurement is more difficult to identify. The usual approach is to identify such faults by applying statistical process control techniques (Morris, 1997).

Reliability quantification in quasi-absolute terms

While reliability is essentially probabilistic in nature, it can be quantified in quasi-absolute terms by the mean-time-between-failures and the mean-time-to-failure parameters. It must

be emphasized that these two quantities are usually average values calculated over a number of identical instruments, and therefore the actual values for any particular instrument may vary substantially from the average value.

The *mean-time-between-failures* (*MTBF*) is a parameter that expresses the average time between faults occurring in an instrument, calculated over a given period of time. For example, suppose that the history of an instrument is logged over a 360-day period and the time intervals in days between faults occurring were as follows:

11 23 27 16 19 32 6 24 13 21 26 15 14 33 29 12 17 22

The mean interval is 20 days, which is therefore the mean-time-between-failures. An alternative way of calculating *MTBF* is simply to count the number of faults occurring over a given period. In the above example, there were 18 faults recorded over a period of 360 days and so the *MTBF* can be calculated as, $MTBF = 360/18 = 20$ days.

Unfortunately, in the case of instruments that have a high reliability, such in-service calculation of reliability in terms of the number of faults occurring over a given period of time becomes grossly inaccurate because faults occur too infrequently. In this case, *MTBF* predictions provided by the instrument manufacturer can be used, since manufacturers have the opportunity to monitor the performance of a number of identical instruments installed in different companies. If there are a total of F faults recorded for N identical instruments in time T, the *MTBF* can be calculated as $MTBF = TN/F$. One drawback of this approach is that it does not take the conditions of use, such as the operating environment, into account.

The mean-time-to-failure (*MTTF*) is an alternative way of quantifying reliability that is normally used for devices like thermocouples that are discarded when they fail. *MTTF* expresses the average time before failure occurs, calculated over a number of identical devices. Suppose that a batch of 20 thermocouples is put through an accelerated-use test in the same environment and the time before failure (in months) of each device is as follows:

7 9 13 6 10 11 8 9 14 8 8 12 9 15 11 9 10 12 8 11

The mean of these 20 numbers is 10. Therefore, the simulated mean-time-to-failure is 10 months.

The final reliability-associated term of importance in measurement systems is the *mean-time-to-repair* (*MTTR*). This expresses the average time needed for repair of an instrument. *MTTR* can also be interpreted as the *mean-time-to-replace*, since replacement of a faulty instrument by a spare one is usually preferable in manufacturing systems to losing production while an instrument is repaired. As an example, suppose that the time in hours

taken to repair an instrument over a history of 18 breakdowns are recorded, with the following times:

4 1 3 2 1 9 2 1 7 2 3 4 1 3 2 4 4 1

The mean of these values is 3 and the mean-time-to-repair is therefore 3 h.

The *MTBF* and *MTTR* parameters are often expressed in terms of a combined quantity known as the availability figure. This measures the proportion of the total time that an instrument is working, that is, the proportion of the total time that it is in an unfailed state. The availability is defined as the ratio:

$$\text{Availability} = \frac{MTBF}{MTBF + MTTR}$$

In measurement systems, the aim must always be to maximize the *MTBF* figure and minimize the *MTTR* figure, thereby maximizing the availability. As far as the *MTBF* and *MTTF* figures are concerned, good design and high quality control standards during manufacture are the appropriate means of maximizing these figures. Design procedures that mean that faults are easy to repair are also an important factor in reducing the *MTTR* figure.

Example 11.1

Data are collected by a manufacturer about a particular piece of machinery that is used 24 h/day, 7 days per week, recording both the intervals in days between breakdowns and the time taken to repair each fault that causes a breakdown. The following data are collected:

Times before breakdown in days: 11.4 16.7 9.8 12.3 17.9 14.1 20.2 15.0 8.6 18.5

Time to repair faults: 0.2 0.7 1.4 0.1 0.6 3.4 0.5 0.2 1.3 0.8

Calculate the availability of the machine.

■

Solution

$$\begin{aligned}\text{Mean time before failure } (MTBF) &= \sum(11.4 + 16.7 + 9.8 + 12.3 + 17.9 + 14.1 \\ &\quad + 20.2 + 15.0 + 8.6 + 18.5)/10 \\ &= 14.45\end{aligned}$$

$$\text{Mean-time-to-repair } (MTTR) = \sum(0.2 + 0.7 + 1.4 + 0.1 + 0.6 + 3.4 + 0.5 + 0.2 + 1.3 + 0.8)/10$$
$$= 0.92$$
$$\text{Availability} = \frac{MTBF}{MTBF + MTTR} = \frac{14.45}{14.45 + 0.92} = 0.94 = 94\%$$

■

Failure patterns

The pattern of failure in an instrument may increase, stay the same, or decrease over its life. In the case of *electronic components*, the failure rate typically changes with time in the manner shown in Figure 11.1(a). This form of characteristic is frequently known as a *bathtub curve*. Early in their life, electronic components can have quite a high rate of fault incidence up to time t_1 (see Figure 11.1(a)). After this initial working period, the fault rate decreases to a low level and remains at this low level until time t_2 when aging effects

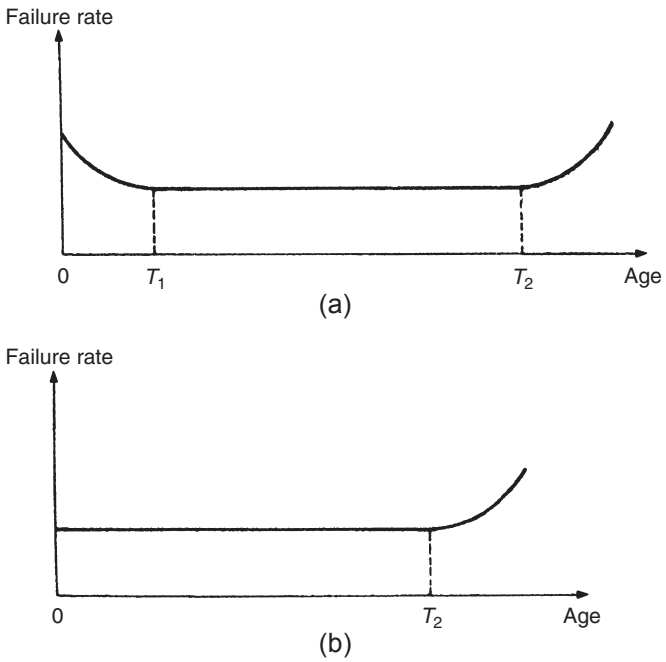

Figure 11.1
Typical variation of reliability with component age: (a) Electronic components ("bathtub" curve); (b) Mechanical components.

cause the fault rate to start increase again. Instrument manufacturers often "burn in" electronic components for a length of time corresponding to the time t_1. This means that the components have reached the high-reliability phase of their life before they are supplied to customers.

Mechanical components usually have different failure characteristics as shown in Figure 11.1(b). Material fatigue is a typical reason for the failure rate to increase over the life of a mechanical component. In the early part of their life, when all components are relatively new, many instruments exhibit a low incidence of faults. Then, at a later stage, when fatigue and other aging processes start to have a significant effect, the rate of faults increases and continues to increase thereafter.

Complex systems containing many different components often exhibit a constant pattern of failure over their lifetime. The various components within such systems have their own failure pattern where the failure rate is increasing or decreasing with time. The greater the number of such components within a system, the greater is the tendency for the failure patterns in the individual components to cancel out and for the rate of fault incidence to assume a constant value.

Reliability quantification in probabilistic terms

In probabilistic terms, the reliability $R(T)$ of an instrument X is defined as the probability that the instrument will not fail within a certain period of time T. The unreliability or likelihood of failure $F(T)$ is a corresponding term, which expresses the probability that the instrument will fail within the specified time interval. $R(T)$ and $F(T)$ are related by the expression:

$$F(T) = 1 - R(T) \tag{11.1}$$

To calculate $R(T)$, accelerated lifetime testing[1] is carried out for a number (N) of identical instruments. Providing all instruments have similar conditions of use, the times of failure, $t_1, t_2, \ldots, t_n$ will be distributed about the MTTF t_m. If the probability density of the time-to-failure is represented by $f(t)$, the probability that a particular instrument will fail in a time interval δt is given by $f(t)\delta t$, and the probability that the instrument will fail before a time T is given by:

$$F(T) = \int_0^T f(t)\mathrm{d}t$$

[1] Accelerated lifetime testing means subjecting an instrument to a much greater frequency of use than would normally be expected. If an instrument is normally used 10 times per day, then 100 days of normal use can be simulated by using it 1000 times in a single day.

The probability that the instrument will fail in a time interval ΔT following T, assuming that it has survived time T, is given by:

$$\frac{F(T+\Delta T)-F(T)}{R(T)}$$

where $R(T)$ is the probability that the instrument will survive to time T. Dividing this expression by ΔT gives the average failure rate in the interval from T to $T+\Delta T$ as:

$$\frac{F(T+\Delta T)-F(T)}{\Delta T R(T)}$$

In the limit as $\Delta T \to 0$, the instantaneous failure rate at time T is given by:

$$\theta_f = \frac{\mathrm{d}[F(T)]}{\mathrm{d}t}\frac{1}{R(T)} = \frac{F'(T)}{R(T)} \tag{11.2}$$

If it is assumed that the instrument is in the constant-failure-rate phase of its life, denoted by the interval between times t_1 and t_2 in Figure 11.1, then the instantaneous failure rate at T is also the mean failure rate, which can be expressed as the reciprocal of the *MTBF*, that is, mean failure rate $= \theta_f = 1/t_m$.

Differentiating Eqn (11.1) with respect to time gives, $F'(T) = -R'(T)$. Hence, substituting for $F'(T)$ in Eqn (11.2) gives, $\theta_f = -\frac{R'(T)}{R(T)}$. This can be solved (Johnson et al., 2009) to give the following expression:

$$R(T) = \exp(-\theta_f T) \tag{11.3}$$

Examination of Eqn (11.3) shows that, at time $t = 0$, the unreliability is zero. Also, as t tends to $\propto$, the unreliability tends to a value of 1. This agrees with intuitive expectations that the value of unreliability should lie between values of 0 and 1. Another point of interest in Eqn (11.3) is to consider the unreliability when $T = MTBF$, that is, when $T = t_m$. Then, $F(T) = 1 - \exp(-1) = 0.63$, that is, the probability of a product failing after it has been operating for a length of time equal to the *MTBF* is 63%.

Further analysis of Eqn (11.3) shows that, for $T/t_m \leq 0.1$:

$$F(T) \approx T/t_m \tag{11.4}$$

This is a useful formula for calculating (approximately) the reliability of a critical product, which is only used for a time that is a small proportion of its *MTBF*.

Example 11.2

If the mean-time-to-failure of an instrument is 50,000 h, calculate the probability that it will not fail during the first 10,000 h of operation.

■

Solution

From Eqn (11.3),

$$R(T) = \exp\left(-\theta_f T\right) = \exp(-10,000/50,000) = 0.8187.$$

■

Example 11.3

If the mean-time-to-failure of an instrument is 80,000 h, calculate the probability that it will not fail during the first 8000 h of operation.

■

Solution

In this case, $T/t_m = 80{,}000/8000 = 0.1$ and so Eqn (11.4) can be applied, giving $R(T) = 1 - F(T) \approx 1 - T/t_m \approx 0.9$. To illustrate the small level of inaccuracy involved in using the approximate expression Eqn (11.4), if we calculate the probability according to Eqn (11.3) we get $R(T) = \exp(-0.1) = 0.905$. Thus, there is a small but finite error in applying Eqn (11.4) instead of Eqn (11.3).

■

11.2.2 Laws of Reliability in Complex Systems

Measurement systems usually comprise a number of components that are connected together in series, and hence it is necessary to know how the reliabilities of individual components are aggregated into a reliability figure for the whole system. In some cases, identical measurement components are put in parallel to improve reliability, because the measurement system then only fails if all of the parallel components fail. These two cases are covered by particular laws of reliability.

Reliability of components in series

A measurement system consisting of several components in series fails when any one of the separate components develops a fault. The reliability of such a system can be quantified as the probability that none of the components will fail within a given interval of time. For a system of n series components, the reliability R_S is the product of the separate reliabilities of the individual components according to the joint probability rule (Morris, 1997):

$$R_S = R_1\, R_2 \cdots R_n \tag{11.5}$$

Example 11.4

A measurement system consists of a sensor, a variable conversion element, and a signal-processing circuit, for which the reliability figures are 0.9, 0.95, and 0.99, respectively. Calculate the reliability of the whole measurement system.

■

Solution

Applying Eqn (11.5), $R_S = 0.9 \times 0.95 \times 0.99 = 0.85$

■

Reliability of components in parallel

One way of improving the reliability of a measurement system is to connect two or more instruments in parallel. This means that the system only fails if every parallel instrument fails. For such systems, the system reliability R_S is given by,

$$R_S = 1 - F_S \tag{11.6}$$

where F_S is the unreliability of the system. The equation for calculating F_S is similar to Eqn (11.5). Thus, for n instruments in parallel, the unreliability is given by,

$$F_S = F_1\, F_2 \cdots F_n \tag{11.7}$$

If all the instruments in parallel are identical, then Eqn (11.7) can be written in the simpler form:

$$F_S = (F_X)^n \tag{11.8}$$

where F_X is the unreliability of each instrument.

Example 11.5

In a particular safety-critical measurement system, three identical instruments are connected in parallel. If the reliability of each instrument is 0.95, calculate the reliability of the measurement system.

■

Solution

From Eqn (11.1), the unreliability of each instrument F_X is given by: $F_X = 1 - R_X = 1 - 0.95 = 0.05$.

Applying Eqn (11.8), $F_S = (F_X)^3 = (0.05)^3 = 0.000125$.

Thus, from Eqn (11.6), $R_S = 1 - F_S = 1 - 0.000125 = 0.999875$.

■

11.2.3 Improving Measurement System Reliability

When designing a measurement system, the aim is always to reduce the probability of the system failing to as low a level as possible. An essential requirement in achieving this is to ensure that the system is replaced at or before the time t_2 in its life shown in Figure 11.1 when the statistical frequency of failures starts to increase. Therefore, the initial aim should be to set the lifetime T equal to t_2 and minimize the probability $F(T)$ of the system failing within this specified lifetime. Once all measures to reduce $F(T)$ have been applied, the acceptability of the reliability $R(T)$ has to be assessed against the requirements of the measurement system. Inevitably, cost enters into this, as efforts to increase $R(T)$ usually increase the cost of buying and maintaining the system. Lower reliability is acceptable in some measurement systems where the cost of failure is low, such as in manufacturing systems where the cost of lost production, or the loss due to making out-of-specification products, is not serious. However, in other applications, such as where failure of the measurement system incurs high costs or causes safety problems, high reliability is essential. Some special applications where human access is very difficult or impossible, such as measurements in unmanned spacecraft, satellites, and nuclear power plants, demand especially high reliability because repair of faulty measurement systems is impossible.

The various means of increasing $R(T)$ are considered below. However, once all efforts to increase $R(T)$ have been exhausted, the only solution available if the reliability specified for a working period T is still not high enough is to reduce the period T over which the reliability is calculated by replacing the measurement system earlier than time t_2.

Choice of instrument

The type of components and instruments used within measuring systems has a large effect on the system reliability. Of particular importance in choosing instruments is to have regard to the type of operating environment in which they will be used. In parallel with this, appropriate protection must be given (e.g., enclosing thermocouples in sheaths) if it is anticipated that the environment may cause premature failure of an instrument. Some instruments are more affected than others, and thus more likely to fail, in certain environments. The necessary knowledge to make informed choices about the suitability of instruments for particular environments, and the correct protection to give them, requires

many years of experience, although instrument manufacturers can give useful advice in most cases.

Instrument protection

Adequate protection of instruments and sensors from the effects of the operating environment is necessary. For example, thermocouples and resistance thermometers should be protected by a sheath in adverse operating conditions.

Regular calibration

The most common reason for faults occurring in a measurement system, whereby the error in the measurement goes outside acceptable limits, is drift in the performance of the instrument away from its specified characteristics. Such faults can usually be avoided by ensuring that the instrument is recalibrated at the recommended intervals of time. Types of intelligent instrument and sensor that perform self-calibration have clear advantages in this respect.

Redundancy

Redundancy means the use of two or more measuring instruments or measurement system components in parallel such that any one can provide the required measurement. Example 11.5 showed the use of three identical instruments in parallel to make a particular measurement instead of a single instrument. This increased the reliability from 95% to 99.99%. Redundancy can also be applied in larger measurement systems where particular components within it seriously degrade the overall reliability of the system. Consider the five-component measurement system shown in Figure 11.2(a) in which the reliabilities of the individual system components are $R_1 = R_3 = R_5 = 0.99$ and $R_2 = R_4 = 0.95$.

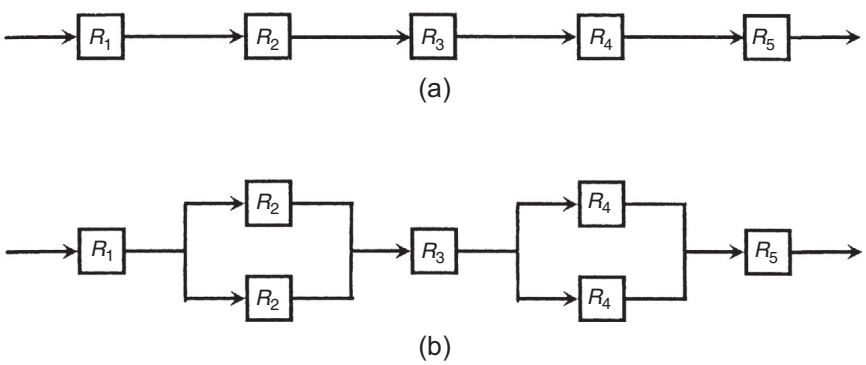

Figure 11.2
Improving measurement system reliability: (a) Original system; (b) Duplicating components that have poor reliability.

Using Eqn (11.5), the system reliability is given by,
$R_S = 0.99 \times 0.95 \times 0.99 \times 0.95 \times 0.99 = 0.876$. Now, consider what happens if redundant instruments are put in parallel with the second and fourth system component, as shown in Figure 11.2(b). The reliabilities of these sections of the measurement system are now modified to new values R_2' and R_4', which can be calculated using Eqns (11.1), (11.6), and (11.8) as follows: $F_2 = 1 - R_2 = 0.05$. Hence, $F_2' = (0.05)^2 = 0.0025$ and $R_2' = 1 - F_2' = 0.9975$. $R_4' = R_2'$ since $R_4 = R_2$.

Using Eqn (11.5) again, the system reliability is now
$R_S = 0.99 \times 0.9975 \times 0.99 \times 0.9975 \times 0.99 = 0.965$.

Thus, the redundant instruments have improved the system reliability by a large amount. However, this improvement in reliability is only achieved at the cost of buying and maintaining the redundant components that have been added to the measurement system. If this practice of using redundant instruments to improve reliability is followed, provision must be provided for replacing failed components by the standby units. The most efficient way of doing this is to use an automatic switching system, but manual methods of replacement can also work reasonably well in many circumstances.

The principle of increasing reliability by placing components in parallel is often extended to other aspects of measurement systems such as the connectors in electrical circuits, as bad connections are a frequent cause of malfunction. For example, two separate pairs of plugs and sockets are frequently used to make the same connection. The second pair is redundant, that is, the system can usually function at 100% efficiency without it, but it becomes useful if the first pair of connectors fails.

11.2.4 Software Reliability

As computer processors, and the software within them, are increasingly found in most measurement systems, the issue of the reliability of such components has become very important. Computer hardware behaves very much like electronic components in general, and the rules for calculating reliability given earlier can be applied. However, the factors affecting reliability in software are fundamentally different. Application of the general engineering definition of reliability to software is not appropriate because the characteristics of the error mechanisms in software and in engineering hardware are fundamentally different. Hardware systems that work correctly when first introduced can develop faults at any time in the future, and so the *MTBF* is a sensible measure of reliability. However, software does not change with time: if it starts off being error-free, then it will remain so. Therefore, what we need to know, in advance of its use, is whether or not faults are going to be found in the software after it has been put into use. Thus, for

software, an *MTBF* reliability figure is of little value. Instead, we must somehow express the probability that errors will not occur in it.

Quantifying software reliability

A fundamental problem in predicting that errors will not occur in software is that, however exhaustive the testing, it is impossible to say with certainty that all errors have been found and eliminated. Errors can be quantified by three parameters, D, U, and T, where D is the number of errors detected by testing the software, U is the number of undetected errors, and T is the total number of errors (both detected and undetected). Hence,

$$U = T - D \tag{11.9}$$

Good program testing can detect most errors and so make D approach T so that U tends toward zero. However, as the value of T can never be predicted with certainty, it is very difficult to predict that software is error-free, whatever degree of diligence is applied during testing procedures.

Whatever approach is taken to quantifying reliability, software testing is an essential prerequisite to the quantification methods available. While it is never possible to detect all the errors that might exist, the aim must always be to find and correct as many errors as possible by applying a rigorous testing procedure. Software testing is a particularly important aspect of the wider field of software engineering. However, as it is a subject of considerable complexity, the detailed procedures available are outside the scope of this book. A large number of books now cover good software engineering in general and software testing procedures in particular, and the reader requiring further information is referred to the referenced texts such as Fenton and Bieman (2014), Fenton and Pfleeger (1998), Naik and Tripathy (2008), Pfleeger and Atlee (2009), and Shooman (2002).

One approach to quantifying software reliability (Fenton and Bieman, 2014) is to monitor the rate of error discovery during testing and then extrapolate this into an estimate of the MTBFs for the software once it has been put into use. Testing can then be extended until the predicted *MTBF* is greater than the projected time-horizon of usage of the software. This approach is rather unsatisfactory because it accepts that errors in the software exist and only predicts that errors will not emerge very frequently.

Confidence in the measurement system is much greater if we can say, “There is a high probability that there are zero errors in the software” rather than “There are a finite number of errors in the software but they are unlikely to emerge within the expected lifetime of its usage.” One way of achieving this is to estimate the value of T (total number of errors) from initial testing and then carry out further software testing until the predicted value of T is zero, in a procedure known as *error-seeding*. In this method, the programmer responsible for producing the software deliberately puts a number of errors E

into the program, such that the total number of errors in the program increases from T to T', where $T' = T + E$. Testing is then carried out by a different programmer who will identify a number of errors given by D', where $D' = D + E'$ and E' is the number of deliberately inserted errors that are detected by this second programmer. Normally, the real errors detected (D) will be less than T and the seeded errors detected (E') will be less than E. However, on the assumption that the ratio of seeded errors detected to the total number of seeded errors will be the same as the ratio of the real errors detected to the total number of real errors, the following expression can be written:

$$\frac{D}{T} = \frac{E'}{E} \tag{11.10}$$

As E' is measured, E is known and D can be calculated from the number of errors D' detected by the second programmer according to $D = D' - E'$, the value of T can then be calculated as:

$$T = DE/E' \tag{11.11}$$

Example 11.6

The author of a digital signal-processing algorithm that forms a software component within a measurement system adds 12 deliberate faults to the program. The program is then tested by a second programmer, who finds 34 errors. Of these detected errors, the program author recognizes 10 of them as being seeded errors. Estimate the original number of errors present in the software (i.e., excluding the seeded errors).

■

Solution

The total number of errors detected (D') is 34 and the program author confirms that the number of seeded errors amounts these (E') is 10 and that the total number of seeded errors (E) was 12. Because $D' = D + E'$ (see earlier), $D = D' - E' = 24$. Hence, from Eqn (11.11), $T = DE/E' = 24 \times 12/10 = 28.8$.

■

One flaw in Eqn (11.11) is the assumption that the seeded errors are representative of all the real (unseeded) errors in the software, both in proportion and character. This assumption is never entirely valid in practice because, if errors are unknown, then their characteristics are also unknown. Thus, while this approach may be able to give an approximate indication of the value of T, it can never predict its actual value with certainty.

An alternative to error-seeding is the *double-testing* approach, where two independent programmers test the same program (Fenton and Bieman, 2014). Suppose that the number of errors detected by each programmer is D_1 and D_2, respectively. Normally, the errors

detected by the two programmers will be in part common and in part different. Let C be the number of common errors that both programmers find. The error-detection success of each programmer can be quantified as:

$$S_1 = D_1/T \quad ; \quad S_2 = D_2/T \tag{11.12}$$

It is reasonable to assume that the proportion of errors D_1 that programmer 1 finds out of the total number of errors T is the same proportion as the number of errors C that he/she finds out of the number D_2 found by programmer 2, that is:

$$\frac{D_1}{T} = \frac{C}{D_2} = S_1$$

and hence

$$D_2 = \frac{C}{S_1} \tag{11.13}$$

From Eqn (11.12), $T = D_2/S_2$, and substituting in the value of D_2 obtained from Eqn (11.13), the following expression for T is obtained:

$$T = C/S_1S_2 \tag{11.14}$$

From Eqn (11.13), $S_1 = C/D_2$ and from Eqn (11.12), $S_2 = D_2S_1/D_1 = C/D_1$. Thus, substituting for S_1 and S_2 in (11.14):

$$T = D_1D_2/C \tag{11.15}$$

Example 11.7

A piece of software is tested independently by two programmers, and the number of errors found is 24 and 26, respectively. Of the errors found by programmer 1, 21 are the same as errors found by programmer 2. Estimate the original number of errors in the software.

■

Solution

$D_1 = 24$, $D_2 = 26$ and $C = 21$. Hence, applying Eqn (11.15), $T = D_1D_2/C = 24 \times 26/21 = 29.7$.

■

Program testing should continue until the number of errors that have been found is equal to the predicted total number of errors T. In the case of Example 11.7, this means continuing testing until 30 errors have been found. However, the problem with doing this is that T is

only an estimated quantity and there may actually be only 28 or 29 errors in the program. Thus, to continue testing until 30 errors have been found would mean testing forever! Hence, once 28 or 29 errors have been found and continued testing for a significant time after this has detected no more errors, the testing procedure should be terminated, even though the program could still contain 1 or 2 errors. The approximate nature of the calculated value of T also means that its true value could be 31 or 32, and therefore the software may still contain errors if testing is stopped once 30 errors have been found. Thus, the fact that T is only an estimated value means the statement that a program is error-free once the number of errors detected is equal to T can only be expressed in probabilistic terms.

To quantify this probability, further testing of the program is necessary. The starting point for this further testing is the stage when the total number of errors T that are predicted have been found (or when the number found is slightly less than T but further testing does not seem to be finding any more errors). The next step is to seed the program with W new errors and then test it until all W seeded errors have been found. Provided that no new errors have been found during this further testing phase, the probability that the program is error-free can then be expressed as:

$$P = W/(W + 1) \tag{11.16}$$

However, if any new error is found during this further testing phase, the error must be corrected and then the seeding and testing procedure must be repeated. Assuming that no new errors are detected, a value of $W = 10$ gives $P = 0.91$ (probability 91% that program is error-free). To get to 99% error-free probability, W has to be 99.

Example 11.8

A program is tested and an estimate of 24 is obtained for the total number of errors. The program is then seeded with 30 deliberate errors and further testing is carried out until all 30 seeded errors have been found. If no new (previously undetected) errors are found during this further testing to find the seeded errors, calculate the probability that the program is error-free after this further testing.

■

Solution

If no new errors (i.e., unseeded ones) are found during the second stage of testing, the probability that the program is error-free can be expressed by the expression for P in Eqn (11.16) above.

For the given value of W of 30, $P = W/(W + 1) = 30/31 = 0.968$.

Thus, the probability that the program is error-free is 0.968 (96.8%).

■

Improving software reliability

The apriori requirement in achieving high reliability in software is to ensure that it is produced according to sound software engineering principles. Formal standards for achieving high quality in software are set out in BS/ISO/IEC 90003 (2014). Libraries and bookshops, especially academic ones, offer a number of texts on good software design procedures. These differ significantly in their style of approach, but all have the common aim of encouraging the production of error-free software that conforms to the design specification. It is not within the scope of this book to enter into arguments about which software design approach is best, as choice between the different software design techniques largely depends on personal preferences. However, it is essential that software contributing to a measurement system is produced according to good software engineering principles.

The second stage of reliability enhancement is the application of a rigorous testing procedure as described in the last section. This is a very time-consuming and hence expensive business, and so testing should only continue until the calculated level of reliability is the minimum needed for the requirements of the measurement system. However, if a very high level of reliability is demanded, such rigorous testing becomes extremely expensive and an alternative approach known as *N*-version programming is often used. *N-version programming* requires N different programmers to produce N different versions of the same software according to a common specification. Then, assuming that there are no errors in the specification itself, any difference in the output of one program compared with the others indicates an error in that program. Commonly, $N = 3$ is used, that is, three different versions of the program are produced, but $N = 5$ is used for measurement systems that are very critical. In this latter case, a "voting" system is used, which means that up to two out of the five versions can be faulty without incorrect outputs being generated.

Unfortunately, while this approach reduces the chance of software errors in measurement systems, it is not foolproof because the degree of independence between programs cannot be guaranteed. Different programmers, who may be trained in the same place and use the same design techniques, may generate different programs that have the same errors. Thus, this method has the best chance of success if the programmers are trained independently and use different design techniques.

Languages such as ADA also improve the safety of software because they contain special features that are designed to detect the kind of programming errors that are commonly made. Such languages have been specifically developed with safety-critical applications in mind.

11.3 Safety Systems

Measurement system reliability is usually inexorably linked with safety issues, since measuring instruments to detect the onset of dangerous situations that may potentially compromise safety are a necessary part of all safety systems implemented. Statutory safety legislation now exists in all countries around the world. While the exact content of legislation varies from country to country, a common theme is to set out responsibilities for all personnel whose actions may affect the safety of themselves or others. Penalties are prescribed for contravention of the legislation, which can include fines or custodial sentences or both. Legislation normally sets out duties for both employers and employees.

Duties of employers include the following:

- To ensure that process plant is operated and maintained in a safe way so that the health and safety of all employees is protected.
- To provide such training and supervision as is necessary to ensure the health and safety of all employees.
- To provide a monitoring and shutdown system (safety system) for any process plant or other equipment that may cause danger if certain conditions arise.
- To ensure the health and safety, as far as is reasonable practical, of all persons who are not employees but who may reasonably be expected to be at risk from operations carried out by a company.

Duties of employees include the following:

- To take reasonable care for their own safety.
- To take reasonable care for the safety of others.
- To avoid misusing or damaging any equipment or system that is designed to protect people's safety.

The primary concern of measurement and instrumentation technologists with regard to safety legislation is, firstly, to ensure that all measurement systems are installed and operated in a safe way and, secondly, to ensure that instruments and alarms installed as part of safety protection systems operate reliably and effectively.

Intrinsic safety

Intrinsic safety describes the ability of measuring instruments and other systems to operate in explosive or flammable environments without any risk of sparks or arcs causing an explosion or fire. The detailed design of systems to make them intrinsically safe is outside the scope of this book. However, the general principles are either to design electrical systems in a way that avoids any possibility of parts that may spark coming into contact

with the operating environment or else to avoid using electrical components altogether. The latter point means that pneumatic sensors and actuators continue to find favor in some applications despite the advantages of electrical devices in most other respects.

Installation practice

Good installation practice is necessary to prevent any possibility of people getting electrical shocks from measurement systems. Instruments that have a mains power supply must be subject to the normal rules about the condition of supply cables, clamping of wires, and earthing of all metal parts. However, most measurement systems operate at low voltages and so pose no direct threat unless parts of the system come into contact with mains conductors. This should be prevented by applying codes of practice that require that all cabling for measurement systems to be kept physically separate to that used for carrying mains voltages to equipment. Normally, this prohibits the use of the same trunking to house both signal wires and mains cables, although some special forms of trunking are available that have two separate channels separated by a metal barrier, thus allowing them to be used for both mains cables and signal wires. This subject is covered in depth in the many texts on electrical installation practice.

11.3.1 Introduction to Safety Systems

The purpose of safety systems is to monitor parameter values in manufacturing plant and other systems and to make an effective response when plant parameters vary away from normal operating values and cause a potentially dangerous situation to develop. The response can either be to generate an alarm for the plant operator to take action or else to take more direct action to shut down the plant automatically. The design and operation of safety systems is now subject to guidelines set by the international standard IEC61508.

IEC61508

IEC61508 (2010) sets out a code of practice that is designed to ensure that safety systems work effectively and reliably. Although primarily concerned with electrical, electronic, and programmable-electronic safety systems, the principles embodied by the standard can be applied as well to systems with other technologies, such as mechanical, pneumatic, and hydraulic devices.

The IEC61508 standard is subdivided into three sets of requirements:

- Proper management of design, implementation, and maintenance of safety systems.
- Competence and training of personnel involved in designing, implementing, or maintaining safety systems.
- Technical requirements for the safety system itself.

A full analysis of these various requirements can be found elsewhere (Dean, 1999).

A key feature of IEC61508 is the *safety integrity level* (SIL), which is expressed as the degree of confidence that a safety system will operate correctly and ensure that there is an adequate response to any malfunctions in manufacturing plant etc. that may cause a hazard and put human beings at risk. The SIL value is set according to what the tolerable risk is in terms of the rate of failure for a process. The procedure for defining the required SIL value is known as *risk analysis*. What is "tolerable" depends on what the consequences of a dangerous failure are in terms of injury to one or more people or death to one or more people. The acceptable level of tolerance for particular industries and processes is set according to guidelines defined by safety regulatory authorities, expert advice, and legal requirements. The table below gives the SIL value corresponding to various levels of tolerable risk for continuous operating plant.

SIL	Probability of Dangerous Failure per Hour	Probability of Dangerous Failure per Year
4	10^{-9} to 10^{-8}	10^{-5} to 10^{-4}
3	10^{-8} to 10^{-7}	10^{-4} to 10^{-3}
2	10^{-7} to 10^{-6}	10^{-3} to 10^{-2}
1	10^{-6} to 10^{-5}	10^{-2} to 10^{-1}

The safety system is required to have sufficient reliability to match the rate of dangerous failures in a plant to the SIL value set. This reliability level is known as the *safety integrity* of the system. *Plant reliability* is calculated by identical principles to those set out in Section 11.2 for measurement systems, and is based on a count of the number of faults that occur over a certain interval of time. However, it must be emphasized that the frequency of potentially dangerous failures is usually less than the rate of occurrence of faults in general. Thus, the reliability value for a plant cannot be used directly as a prediction of the rate of occurrence of dangerous failures. Hence, the total failures over a period of time must be analyzed and divided between faults that are potentially dangerous and those that are not.

Once risk analysis has been carried out to determine the appropriate SIL value, the required performance of the safety protection system can be calculated. For example, if the maximum allowable probability of dangerous failures per hour is specified as 10^{-8} and the actual probability of dangerous failures in a plant is calculated as 10^{-3} per hour, then the safety system must have a minimum reliability of $10^{-8}/10^{-3}$, that is, 10^{-5} failures for a 1-h period. A fuller account of calculating safety system requirements is given elsewhere (Simpson and Smith, 1999).

11.3.2 Design of a Safety System

A typical safety system consists of a sensor, a trip amplifier, and either an actuator or alarm generator, as shown in Figure 11.3. For example, in a safety system designed to

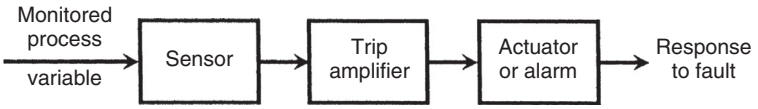

Figure 11.3
Elements of a safety system.

protect against abnormally high pressures in a process, the sensor would be some form of pressure transducer, and the trip amplifier would be a device that amplifies the measured pressure signal and generates an output that activates either an actuator or an alarm if the measured pressure signal exceeded a preset threshold value. A typical actuator in this case would be a relief valve.

Software is increasingly embedded within safety systems to provide intelligent interpretation of sensor outputs, such as identifying trends in measurements. Safety systems that incorporate software and a computer processor are commonly known as *microprocessor-based protection systems*. In any system-containing software, the reliability of the software is crucial to the overall reliability of the safety system, and the reliability-quantification techniques described in Section 11.3 assume great importance.

To achieve the very high levels of reliability normally specified for safety systems, it is usual to guard against system failure by either triplicating the safety system and implementing two-out-of-three voting or, alternatively, by providing a switchable, standby safety system. These techniques are considered below.

Two-out-of-three voting system

This system involves triplicating the safety system, as shown in Figure 11.4. Shutdown action is taken, or an alarm is generated, if two out of the three systems indicate the requirement for action. This allows the safety system to operate reliably if any one of the

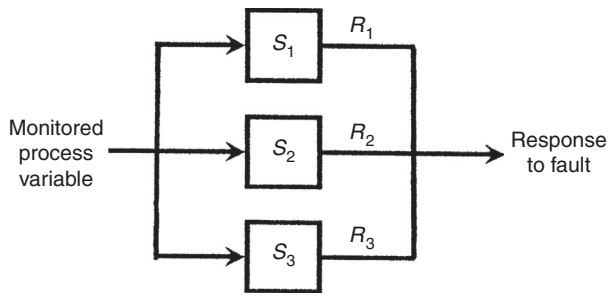

Figure 11.4
Two-out-of-three voting system.

triplicated systems fails and is often known as a two-out-of-three voting system. The reliability R_S is given by:

$$\begin{aligned} R_S &= \text{Probability of all three systems operating correctly} \\ &\quad + \text{ Probability of any two systems operating correctly} \\ &= R_1R_2R_3 + (R_1R_2F_3 + R_1F_2R_3 + F_1R_2R_3) \end{aligned} \tag{11.17}$$

where R_1, R_2, R_3 and F_1, F_2, and F_3 are the reliabilities and unreliabilities of the three systems, respectively. If all of the systems are identical (such that $R_1 = R_2 = R_3 = R$ etc.):

$$R_S = R^3 + 3R^2F = R^3 + 3R^2(1 - R) \tag{11.18}$$

Example 11.9

In a particular protection system, three safety systems are connected in parallel and a two-out-of-three voting strategy is applied. If the reliability of each of the three systems is 0.95, calculate the overall reliability of the whole protection system.

■

Solution

Applying Eqn (11.18), $R_S = 0.95^3 + [3 \times 0.95^2 \times (1 - 0.95)] = 0.993$

■

Standby system

A standby system avoids the cost of providing and running three separate safety systems in parallel. Use of a standby system means that only two safety systems have to be provided. The first system is in continuous use but the second system is normally not operating and is only switched into operation if the first system develops a fault. The flaws in this approach are the necessity for faults in the primary system to be reliably detected and the requirement that the switch must always work correctly. The probability of failure F_S of a standby system of the form shown in Figure 11.5, assuming no switch failures during normal operation, can be expressed as follows:

$$\begin{aligned} F_S &= \text{Probability of systems } S_1 \text{ and } S_2 \text{ both failing, given successful switching} \\ &\quad + \text{ Probability of } S_1 \text{ and the switching system both failing at the same time} \\ &= F_1F_2R_DR_W + F_1(1 - R_DR_W) \end{aligned}$$

System reliability is given by:

$$R_S = 1 - F_S = 1 - F_1(1 + F_2R_DR_W - R_DR_W) \tag{11.19}$$

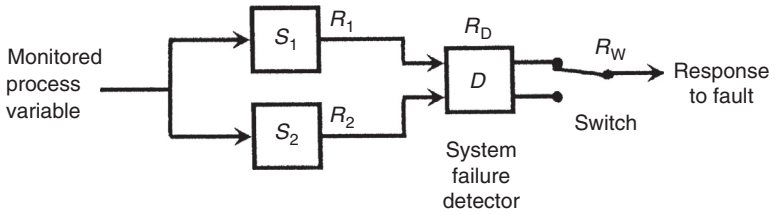

Figure 11.5
Standby system.

where R_D is the reliability of the fault detector and R_W is the reliability of the switching system.

The derivation of Eqn (11.19) assumes that there are no switch failures during normal operation of the system, that is, there are no switch failures during the time that the controlled process is operating satisfactorily and there is no need to switch over to the standby system. However, because the switch is subject to a continuous flow of current, its reliability cannot be assumed to be 100%. If the reliability of the switch in normal operation is represented by R_N, the expression in Eqn (11.19) must be multiplied by R_N and the reliability of the system becomes:

$$R_S = R_N[1 - F_1(1 + F_2 R_D R_W - R_D R_W)] \tag{11.20}$$

The problem of detecting faults in the primary safety system reliably can be solved by operating both safety systems in parallel. This enables faults in the safety system to be distinguished from faults in the monitored process. If only one of the two safety systems indicates a failure, this can be taken to indicate a failure of one of the safety systems rather than a failure of the monitored process. However, if both safety systems indicate a fault, this almost certainly means that the monitored process has developed a potentially dangerous fault. This scheme is known as *one-out-of-two voting*, but it is obviously inferior in reliability to the two-out-of-three scheme described earlier.

Example 11.10

In a particular protection system, a switchable standby safety system is used to increase reliability. If the reliability of the main system is 0.95, that of the standby system is 0.96^2, that of the fault detection and switching system is 0.95, and the reliability of the switch in normal operation is 0.98, calculate the reliability of the protection system.

[2] Because the standby system is not subject to normal use, its reliability tends to be higher than the primary system even if the two systems consist of nominally identical components.

■

Solution

Applying Eqn (11.20), the parameter values are $F_1 = 0.05$, $F_2 = 0.04$, $R_D R_W = 0.95$, and $R_N = 0.98$. Hence:

$$R_S = 0.98[1 - 0.05(1 + \{0.04 \times 0.95\} - 0.95)] = 0.976$$

■

Actuators and alarms

The final element in a safety system is either an automatic actuator or an alarm that requires a human response. The reliability of the actuator can be calculated in the same way as all other elements in the system and incorporated into the calculation of the overall system reliability as expressed in Eqns (11.17)–(11.20). However, the reliability of alarms cannot be quantified in the same manner. Therefore, safety system reliability calculations have to exclude the alarm element. In consequence, the system designer needs to take steps to maximize the probability that the human operator will take the necessary response to alarms that indicate a dangerous plant condition.

Some useful guidelines for measurement technologists involved in designing alarm systems are provided in a paper by Bransby (1999). A very important criterion in system design is that alarms about dangerous conditions in plant must be much more prominent than alarms about conditions that are not dangerous. Care should also be taken to ensure that the operator of a plant is not bombarded by too many alarms, as this leads the operator to get into the habit of ignoring alarms. Ignoring an alarm indicating that a fault is starting to occur may cause dangerous conditions in the plant to develop. Thus, alarms should be uncommon rather than routine, so that they attract the attention of the plant operator. This ensures, as far as possible, that the operator will take the proper action in response to an alarm about a potentially dangerous situation.

11.4 Summary

The topic that we have studied in this chapter has been the subject of measurement system reliability and the effect that this can have on other systems associated with the measurement system. We started off by studying the principles of reliability and looking at how the reliability of a measurement system can be quantified. We went on to look at the principal laws of reliability and consider how these could be applied to improve the reliability of a system. We also looked at other precautions that we could take when designing and operating measurement systems to avoid either failure or impaired performance. These precautions included choosing suitable instruments according to the expected operating conditions, protecting instruments appropriately when using them in

adverse environments, recalibrating them at the recommended frequency, and building an element into instruments used in critical parts of a measurement system.

We then went on to consider the subject of software reliability. We noted that this was now very important in view of the widespread use of intelligent instruments containing software. This study showed us that there are substantial differences between in the mechanisms contributing to the reliability of software and hardware. The reliability of instrument hardware is related to the factors like mechanical wear, degradation because of the effect of the operating environment, mechanical failure, etc. These are faults that develop over a period of time. However, the mechanisms of software failure are fundamentally different. Software does not change with time and, if it is error-free when first written, it will remain error-free forever. What happens when software is used is that errors that it has had all its life suddenly cause a problem when particular conditions occur, usually when particular combinations of input values are applied. Thus, the usual rules of reliability quantification applied to hardware components in measurement systems are not appropriate for associated software. Instead, we have seen that special procedures have to be applied to quantify software reliability in terms of the probability that it will not fail. Having established appropriate ways of quantifying software reliability, we went on to look at how reliability can be improved.

Our final topic of study in the chapter was that of system safety issues. Having first looked at the definition and quantification of safety levels and the associated IEC 61,508 code of practice for safety systems, we went on to look at how safety systems could be designed to address safety issues. We then ended the chapter by looking in some detail at particular designs of safety system in terms of "two-out-of-three" voting systems, using standby systems and appropriate use of safety actuators and alarms.

11.5 Problems

11.1 How is the reliability of a measurement system defined? What is the difference between quantifying reliability in quasi-absolute terms and in quantifying it probabilistic terms?

11.2 Explain the rules for calculating the overall reliability of system components that are connected
   (a) in series with each other and
   (b) in parallel with one another.

11.3 Discuss ways in which the reliability of measurement systems can be improved.

11.4 How do the mechanisms affecting the reliability of software differ from those affecting the reliability of mechanical and electrical system components?

11.5 How can software reliability be quantified?

11.6 Discuss some ways in which the reliability of software components within measurement systems can be improved.

11.7 What are the principal duties of employers and employees with regard to safety? How do these impact on the design and operation of measurement systems?

11.8 Explain the following terms that are met in the design of safety systems:
(a) two-out-of-three voting system,
(b) standby system.

11.9 The performance of a measuring instrument is monitored over a 1-year (365 days) period and the intervals between faults being recorded are as follows:

27 6 18 41 54 29 46 14 49 38 17 26

Calculate the mean-time-between-failures.

11.10 The days on which an instrument failed were recorded over a 12-month period as follows (such that day 1 = 1st Jan, day 32 = 1st Feb etc.):

Day number of faults: 18 72 111 173 184 227 286 309 356

Calculate the mean-time-between-failures.

11.11 A manufacturer monitors the performance of a new type of instrument that is installed at 20 different locations. If a total of 9 faults are recorded over a 100-day period, calculate the mean-time-between-failure that should be specified for any one instrument.

11.12 The time before failure of each a platinum resistance thermometer used in a particular location is recorded. The times before failure in days for 10 successive thermometers are recorded as:

405 376 433 425 388 402 445 412 397 366

Calculate the mean-time-to-failure.

11.13 The repair times in hours of an instrument over a history of 10 breakdowns are recorded as follows:

10.5 5.75 8.25 30.0 12.5 15.0 6.5 3.25 14.5 9.25.

Calculate the mean-time-to-repair.

11.14 If the mean-time-between-failure for an instrument is 247 days and the mean-time-to-repair is 3 days, calculate its availability.

11.15 Data are collected by a manufacturer about a particular piece of machinery that is used 24 h/day, 7 days per week, recording both the intervals in days between breakdowns and the time taken to repair each fault that causes a breakdown. The following data are collected:

Times before breakdown in days : 13.3 4.3 12.7 17.8 14.2 20.1 15.6 8.9 8.1 11.5

Time to repair faults : 0.8 1.5 0.2 0.7 4.0 0.6 0.9 1.4 0.8 0.1

Calculate the mean-time-before-failure, the mean-time-to-repair, and the availability of the machine.

11.16 Data are collected by a manufacturer about an industrial robot that is used 24 h/day, 7 days per week, recording both the intervals in days between breakdowns and the time taken to repair each fault that causes a breakdown. The following data are collected:

Times before breakdown in days : 21.4 18.5 36.7 19.8 22.3 27.9 24.1 30.2 25.0 8.6

Time to repair faults : 0.4 0.7 2.0 0.1 0.6 3.5 0.5 0.2 1.3 0.8

Calculate the mean-time-before-failure, the mean-time-to-repair, and the availability of the machine.

11.17 If the mean-time-to-failure of an instrument is 100,000 h, calculate the probability that it will not fail in the first 50,000 h.

11.18 If the mean-time-to-failure of a light bulb is 100,000 h, calculate the probability that it will not fail in the first 5000 h.

11.19 If the mean-time-to-failure of a hydraulic seal is 482 h, calculate the probability that it will not fail in the first 360 h.

11.20 Four measurement components connected in series have the following reliabilities: 0.98 0.93 0.95 0.99. Calculate the reliability of the whole measurement system.

11.21 Five components connected in series in a manufacturing system have the following reliabilities: 0.99 0.97 0.98 0.99 0.98. Calculate the reliability of the whole manufacturing system.

11.22 Four components connected in series in a production system have the following reliabilities: 0.98 0.94 0.99 0.97.

(a) Calculate the reliability of the whole production system.

(b) If a better quality component could be purchased to replace component 2 in the system (the one with a reliability of 94%), what would its reliability have to be in order to increase the overall system reliability to 90%?

11.23 In a particular measurement system, two instruments with individual reliability of 0.95 are connected together in parallel. Calculate the reliability of the measurement system if it can continue to function as long as both of the instruments do not fail at the same time.

11.24 In a particular measurement system, three identical instruments with an individual reliability of 0.88 are connected together in parallel.

(a) Calculate the reliability of the measurement system if it can continue to function as long as all of the instruments do not fail at the same time.

(b) What would the reliability of each instrument have to be increased to in order to achieve an overall system reliability of 99.9%?

11.25 In a particular measurement system, two instruments with individual reliability of 0.80 are connected together in parallel.

(a) Calculate the reliability of the measurement system if it can continue to function as long as both of the instruments do not fail at the same time.

(b) How many instruments with this same individual reliability of 80% would have to be connected together in parallel in order to achieve an overall system reliability of 99.5% (assuming that the system can continue to function as long as at least one instrument is still working)?

(c) How many instruments are needed in order to achieve an overall system reliability of 99.95%?

11.26 Calculate the reliability of the measurement system shown in Figure 11.2(b) if the reliabilities of the individual components are:

$R_1 = R_3 = R_5 = 0.98 \quad ; \quad R_2 = R_4 = 0.90$

11.27 (a) Calculate the reliability of the measurement system shown in Figure 11.2(a) if the reliabilities of the individual components are:

$R_1 = R_3 = R_5 = 0.95 \quad ; \quad R_2 = R_4 = 0.80$

(b) Calculate the new reliability if two components in the system (R_2 and R_4) are duplicated as in Figure 11.2(b).

11.28 In order to estimate the number of errors in a new piece of software by applying the error-seeding approach, a programmer puts 10 deliberate (seeded) faults into the program. A second programmer then tests the program and finds 27 errors, of which 8 are confirmed by the first programmer to be seeded errors. Estimate the original number of faults in the program (i.e., excluding the seeded errors).

11.29 The double-testing approach is applied to test a new computer program and the two programmers who do the testing find 31 and 34 errors, respectively. If 27 of the errors found by programmer one are the same as errors in the list produced by programmer 2, estimate the actual number of errors in the program.

11.30 A program is tested and the total number of errors is estimated as 16. The program is then seeded with 20 deliberate errors and further testing is then carried out until all 20 seeded errors have been found.

(a) If no new (previously undetected) errors are found during this further testing to find all the seeded errors, calculate the probability that the program is error-free after this further testing.

(b) How many seeded errors would have to be put into the program and then detected to achieve a 98% probability that the program is error-free?

11.31 In order to estimate the number of errors in a new piece of software by applying the error-seeding approach, a programmer puts 15 deliberate (seeded) faults into the

program. A second programmer then tests the program and finds 35 errors, of which 12 are confirmed by the first programmer to be seeded errors. Estimate the original number of faults in the program (i.e., excluding the seeded errors).

$$D' = 35 \quad ; \quad E' = 12 \quad ; \quad E = 15$$

11.32 The double-testing approach is applied to test a new computer program and the two programmers who do the testing find 31 and 34 errors, respectively. If 27 of the errors found by programmer 1 are the same as errors in the list produced by programmer 2, estimate the actual number of errors in the program.

11.33 The total number of errors estimated after testing a program is 19. The program is then seeded with 25 deliberate errors and further testing is then carried out until all 25 seeded errors have been found.

(a) If no new (previously undetected) errors are found during this further testing to find all the seeded errors, calculate the probability that the program is error-free after this further testing.

(b) How many seeded errors would have to be put into the program and then detected to achieve a 97.5% probability that the program is error-free?

11.34 Three safety systems are connected in parallel in a protection system and a two-out-of-three voting strategy is applied. If the reliability of each of the three systems is 0.90, calculate the overall reliability of the whole protection system.

11.35 A switchable standby safety system is used to increase reliability in a protection system. If the reliability of the main system is 0.90, that of the standby system is 0.91, that of the fault detector/switching system is 0.90, and the reliability of the switch in normal operation is 0.96, calculate the reliability of the protection system.

11.36 Three safety systems are connected in parallel in a protection system and a two-out-of-three voting strategy is applied. If the reliability of each of the three systems is 0.90, calculate the overall reliability of the whole protection system.

11.37 A switchable standby safety system is used to increase reliability in a protection system. If the reliability of the main system is 0.94, that of the standby system is 0.95, that of the fault detector/switching system is 0.96, and the reliability of the switch in normal operation is 0.98, calculate the reliability of the protection system.

References

Bransby, M., 1999. The human contribution to safety—designing alarm systems. Meas. Control 32, 209–213.

BS/ISO/IEC 90003, 2014. Software Engineering: Guidline for Application of ISO 9001 to Computer Software. British Standards Institute/International Standards Organisation/International Electrotechnical Commission.

Dean, S., 1999. IEC61508—understanding functional safety assessment. Meas. Control 32, 201–204.

Fenton, N.E., Bieman, J., 2014. Software Metrics – a Rigorous and Practical Approach. Chapman and Hall.

Fenton, N.E., Pfleeger, S.L., 1998. Software Metrics: A Rigorous Approach. PWS Publishing.

IEC61508, 2010. Functional Safety of Electrical, Electronic and Programmable-electronic Safety Related Systems. International Electrotechnical Commission, Geneva.

Johnson, R., Miller, I.R., Freund, J.E., 2009. Miller and Freund's Probability and Statistics for Engineers. Pearson Education.

Morris, A.S., 1997. Measurement and Calibration Requirements for Quality Assurance to ISO 9000. John Wiley.

Naik, S., Tripathy, P., 2008. Software Testing and Quality Assurance, Theory and Practice. John Wiley.

Pfleeger, S.L., Atlee, J.M., 2009. Software Engineering: Theory and Practice. Prentice Hall.

Shooman, M.L., 2002. Reliability of Computer Systems and Networks: Fault Tolerance, Analysis and Design. Wiley-Blackwell.

Simpson, K., Smith, D.J., 1999. Assessing safety related systems and architectures. Meas. Control 32, 205−208.