CHAPTER ELEVEN

Risk and Reliability

In this chapter we consider the concepts of risk and reliability and how they can be considered in engineering planning and design. The concepts of risk and reliability are defined and illustrated in relation to engineering problems. Reliability-based design and the selection of safety coefficients are explained in detail. The concepts of resilience, vulnerability and robustness are also introduced. Methods for evaluating the reliability of engineering components and engineering systems are explained.

11.1 INTRODUCTION

Risk is inherent in all human activity. For example, we risk personal accident, injury and even death whenever we travel in a car, go for a jog, or cross the street. The levels of such everyday risks depend, in part, on the way individuals choose to conduct their lives. Generally, such risk levels are very low in modern society, unlike the risks faced daily by our ancestors in pre-historic times. The probabilities associated with the risks associated with various everyday activities have been estimated in a number of studies (US Nuclear Regulatory Commission, 1975; Stone, 1988; Morgan, 1990; BC Hydro, 1993). Some of these probabilities are given in Table 11.1.

Risk is also inherent in all engineering work, as was explained in Chapter 3, and part of the role of the engineer is to manage risk levels and to keep them to the very low levels that are acceptable to society.

11.2 LEVELS OF RISK

Dougherty and Fragola (1988) define *risk* as the combination of the probability of an abnormal event or failure and the consequences of that event or failure to a project's success or a system's performance. This combination of probability (or likelihood) and consequences is used in tables of risk ratings such as Table 11.2.

In Table 11.2 catastrophic consequences would involve loss of life, major consequences include serious injury or major economic loss, moderate consequences include minor injuries or moderate economic loss, and minor consequences include minor economic loss. Efforts to minimise risk should give priority to the activities that have an extreme or high risk rating.

Table 11.1 Annual probability of death to an individual.

Source of risk	Annual probability of death	Source of information
Car Travel	1 in 3,500	Morgan (1990)
	1 in 4,000	US Nuclear Regulatory Commission (1975)
	1 in 10,000	Stone (1988)
Air Travel	1 in 9,000	Morgan (1990)
	1 in 100,000	US Nuclear Regulatory Commission (1975)
Drowning	1 in 30,000	US Nuclear Regulatory Commission (1975)
Drowning (UK average)	1 in 100,000	Morgan (1990)
Fire (UK average)	1 in 50,000	Morgan (1990)
Household Electrocution (Canada)	1 in 65,000	Morgan (1990)
Electrocution	1 in 160,000	US Nuclear Regulatory Commission (1975)
Fire (U.K. average)	1 in 50,000	Morgan (1990)
Lightning	1 in 2,000,000	US Nuclear Regulatory Commission (1975)
	1 in 5,000,000	Morgan (1990)
	1 in 10,000,000	Stone (1988)
Nuclear Reactor Accidents	1 in 5,000,000	US Nuclear Regulatory Commission (1975)
Structural Failure	1 in 10,000,000	Morgan (1990)

Table 11.2 Risk ratings. (Reproduced with the kind permission of Neill Buck and Associates)

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Moderate	High	Extreme	Extreme	Extreme
Likely	Low	Moderate	High	Extreme	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Insignificant	Low	Moderate	Moderate	High
Rare	Insignificant	Insignificant	Low	Low	Moderate

For example, the risk levels that are applied in the planning, design and construction of a city office building vary widely. The structural design objectives are to provide a system which will have adequate safety against collapse, as well as good serviceability under normal working loads. These objectives are quantified using minimum performance levels. In regard to serviceability, a maximum allowable deflection is prescribed for the floors and is not to be exceeded when the design working loads are applied. In regard to safety against collapse, minimum levels of overload due to live load, wind and earthquake are prescribed that the structural system must be able to withstand. It will be clear that the consequences of exceeding the deflection criterion will be at most minor, whereas not meeting the minimum strength requirements could well be catastrophic. For this reason the acceptable probability of excessive deflection is much higher than the acceptable probability of collapse.

Risk of gastroenteritis among young children who consume rainwater in South Australia

Eighty-two percent of rural households in South Australia have rainwater tanks as their main source of drinking water. There are some risks associated with the consumption of rainwater as it may be contaminated by pathogens from birds or animals. A study was carried out to assess whether there was a significant difference in the risk of gastroenteritis among 4- to 6-year old children who drank rainwater compared to those who drank treated mains water.

Over 1000 children were included in the study which was carried out over a six-week period. Parents of the children were asked to keep a diary of gastrointestinal symptoms. The occurrence of gastroenteritis was based on a set of symptoms (defined as a highly credible gastrointestinal illness or HCGI). It should be noted that most incidences of gastroenteritis were mild.

Based on the raw data, the incidence of HCGI was 4.7 episodes per child-year for those who only drank rainwater compared to 7.3 episodes per child-year for those who only drank mains water. However, when adjustments were made for other risk factors, there was no significant difference in the incidence of HCGI between the two groups. The study concluded that consumption of rainwater did not increase the risk of gastroenteritis compared with mains water for 4- to 6-year old children. One possible reason for this conclusion is the acquired immunity by the children who drank rainwater, as they had all done so for at least a year prior to the study and could have developed immunity to a number of microorganisms during this period.

Source: Heyworth et al., 2006

11.3 RELIABILITY BASED DESIGN

The *reliability* of an engineering component or system is defined as the probability that the system will be in a non-failure state. The possible modes of failure need to be defined for each particular system under consideration. For example, for a water supply system, one failure mode would correspond to running out of water, although a more likely mode would occur with the imposition of extreme water restrictions on household consumers and industry. Yet another mode would be the provision of water of an unacceptable quality to consumers. For a freeway system, failure could correspond to extreme congestion associated with low vehicle speeds and long delays.

In this section, a simplified example of reliability-based design will be explained using a simple structural element in tension. The same principles apply to many other types of engineering systems.

In structural engineering, probabilities of failure are rarely calculated for design calculations. The usual practice is apply overload factors to the load quantities and understrength terms to the resistance quantities. However, the probability of failure is taken into account in evaluating these “safety factors”. This approach will be demonstrated for the design of simple tension members. Some examples of these are shown in Figure 11.1.

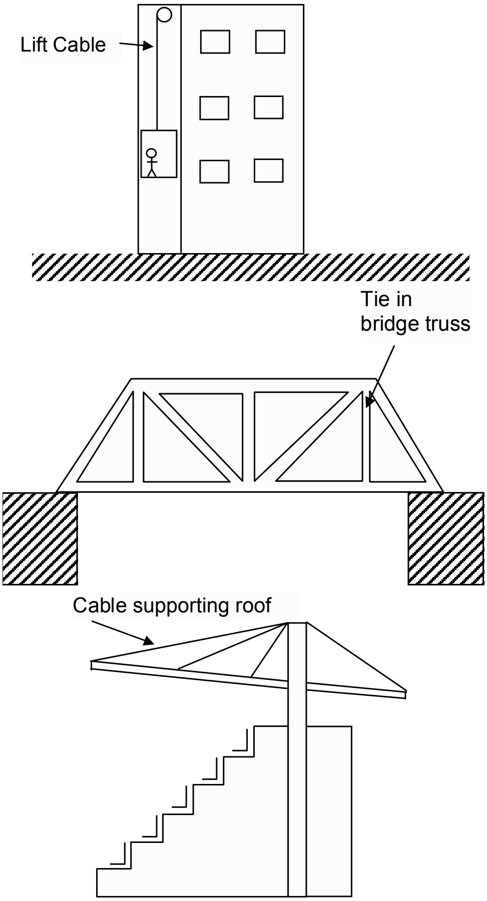

Figure 11.1 Examples of tension members (Lift cable, tie in a bridge truss, and cable supporting a roof).

Consider the analysis of a tension member (or tie) of cross-sectional area, A, as shown in Figure 11.1. If the maximum force that will be applied to the member during its lifetime, S, is known, the maximum stress in the member, σ, can be calculated using the equation:

$$\sigma = \frac{S}{A} \tag{11.1}$$

where A = the cross-sectional area of the member. If σ is less than the stress that will cause failure of the member, σ_f, the member will not fail. In the design situation, the failure stress of the steel and the maximum applied force are assumed to be known, hence the required cross-sectional area of the member, A, can be determined by rearranging Equation 11.1 to give:

$$A \geq \frac{S}{\sigma_f} \tag{11.2}$$

However, this approach does not take into account uncertainty in S, σ_f, and A. Clearly the maximum force that will be applied to the member during its lifetime is not known with certainty. There can also be variations in the failure stress of the steel that comprises the member due to variations in the manufacturing process. Finally, the actual cross-sectional area of the member may vary from the value specified in the design due to variations in production of the member.

One approach that provides some margin of safety in the design is to use a *safety factor*. If we define T, the resistance of the member, as:

$$T = \sigma_f A \tag{11.3}$$

We require T to exceed S by some margin to allow for the possibilities of overloads and understrength. We define the safety factor, γ, as follows:

$$\gamma = \frac{T}{S} \tag{11.4}$$

where γ is typically in the range 1.5–3.0 depending on the loading conditions, material and likely mode of failure. The cross-sectional area of the member is then determined by combining Equations (11.3) and (11.4) as follows:

$$A \geq \frac{S\gamma}{\sigma_f} \tag{11.5}$$

The single safety factor approach is no longer commonly used in structural engineering design, but is still used in geotechnical engineering. Structural engineers now use a reliability-based approach to structural design. This approach explicitly recognises the uncertainties in the various factors involved in the design. In the reliability approach, we define the difference between T and S as the *safety margin*, Z.

i.e.: $$Z = T - S \tag{11.6}$$

We expect variations in T and S due to some of the factors described previously. We will assume that T and S are normally distributed random variables that are independent of each other. Typical distributions of these variables are shown in Figure 11.2. This figure shows some small but finite probability that either T or S is negative. Clearly negative values of T or S are physically impossible, as the normal distribution is only an approximation to the true distributions of the resistance T and maximum applied force S.

Let the means of *T* and *S* be designated by $\mu(T)$ and $\mu(S)$ (respectively) and the standard deviations of *T* and *S* be designated by $\sigma(T)$ and $\sigma(S)$ (respectively). Then, if both *T* and *S* have normal distributions, so will *Z*. The mean and standard deviation of *Z* can be determined using Equations (11.7) and (11.8).

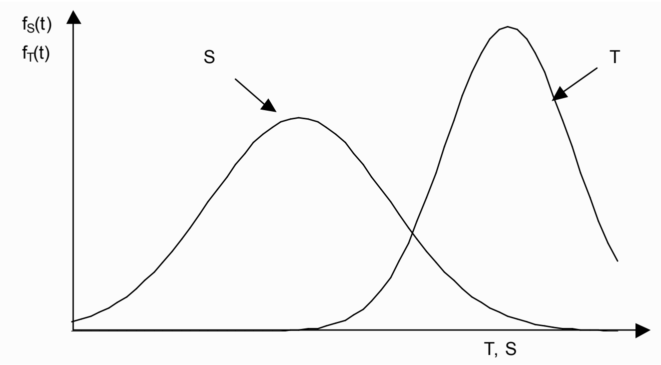

Figure 11.2: Probability distributions of resistance *T* and applied force *S*.

$$\mu(Z) = \mu(T) - \mu(S) \tag{11.7}$$

$$\sigma(Z) = \sqrt{\sigma(T)^2 + \sigma(S)^2} \tag{11.8}$$

The probability distribution of *Z* is shown in Figure 11.3.

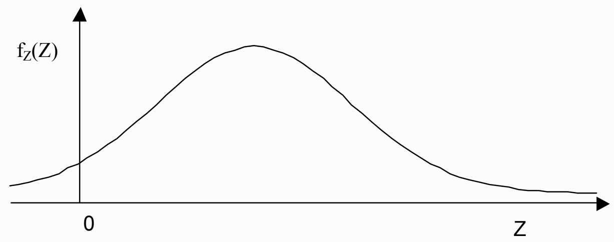

Figure 11.3 Probability distribution of the safety margin, *Z*.

If *Z* is negative, the member will fail, if it is positive, the member will not fail. The probability of failure, P_f, is given by Equation (11.9):

$$P_f = P[Z < 0] \tag{11.9}$$

As stated earlier, the reliability of a system, *R* is defined as the probability that the system will be in a non-failure state. Hence:

$$R = 1 - P_f = 1 - P[Z < 0] \tag{11.10}$$

A commonly used measure of safety is the safety index, β, which is defined as:

$$\beta = \frac{\mu(Z)}{\sigma(Z)} = \frac{1}{V(Z)} \qquad (11.11)$$

where $V(Z)$ = the coefficient of variation of $Z = \sigma(Z)/\mu(Z)$. For the case where Z follows a normal distribution, β is related to the probability of failure as indicated in Table 11. 3.

Table 11.3 Relationship between safety index and the probability of failure for a normal distribution (adapted from Warner et al., 1998).

Safety Index β	2.32	3.09	3.72	4.27	4.75	5.20
Probability of failure, P_f	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}

As T and S are now both considered to be random variables, the safety factor defined in Equation (11.4) may be expressed in terms of the mean values of T and S.

i.e., $$\gamma_0 = \frac{\mu(T)}{\mu(S)} \qquad (11.12)$$

where γ_0 is called the central safety factor. Warner et al. (1998) show that β is related to γ_0 by the following expression:

$$\beta = \frac{\gamma_0 - 1}{\sqrt{\gamma_0^2 V(T)^2 + V(S)^2}} \qquad (11.13)$$

where $V(T)$ and $V(S)$ are the coefficients of variation of T and S (respectively).

Hence in order to maintain the same safety index (and hence probability of failure) γ_0 must vary depending the values of $V(T)$ and $V(S)$.

As noted previously, a major weakness of using γ_0 is that it does not take into account variations in T and S. This may be overcome to some extent by using more extreme values of T and S. For example, define S_k as the value of the applied load S that has a 5% chance of being exceeded. Furthermore, define T_k as the value of the resistance T that has a 95% chance of being exceeded. Then the “nominal” safety factor is given by the following equation:

$$\gamma = \frac{T_k}{S_k} \qquad (11.14)$$

thus, we use a high value of the applied load and low value of the resistance in assessing the nominal safety factor.

Figure 11.4 shows the relationship between the distributions of T and S and the values of T_k and S_k. Modern structural codes of practice use partial safety coefficients to allow for the variabilities in T and S separately. The partial safety coefficients are applied to T_k and S_k to obtain design values T_d and S_d as follows:

$$T_d = \frac{T_k}{\gamma_T} \tag{11.15}$$

$$S_d = \gamma_S S_k \tag{11.16}$$

Thus a safe design requires:

$$T_d > S_d \tag{11.17}$$

$$T_k > \gamma_T \gamma_S S_k \tag{11.18}$$

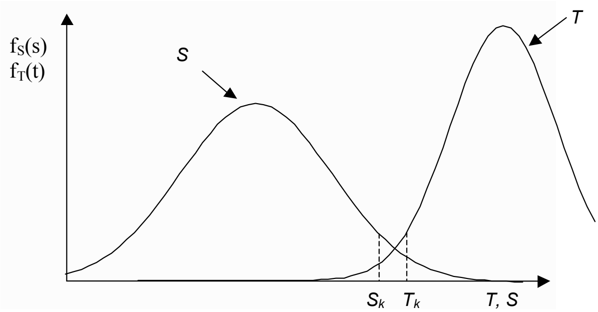

Figure 11.4: Relationship between *T* and *S* and the values of T_k and S_k.

Values of the partial safety coefficients, γ_T and $\gamma_{S,}$ are selected to ensure that that the probability of failure, P_f, given by Equation (11.9) lies within an acceptable range.

It should be noted that the approach outlined above is based on a number of simplifying assumptions such as that *T* and *S* are independent and have normal distributions. Furthermore, even in the simple case of a tensile member, the variability in *T* can be due to variations in materials properties as well as variations in the actual dimensions of the member compared to those assumed in the design. For this reason, the probability of failure determined is usually referred to as a nominal probability of failure.

A similar approach to that outlined above can be used for other structural elements such as beams, columns and frames or other engineering components such as electrical transformers, items of machinery or distillation columns.

Of course, the analysis of an entire system is more complicated. For example, a building structure may have many components, alternative load paths and inbuilt redundancies as well as many different modes of failure.

Furthermore, it should be noted that the above analysis assumes that structural failure will occur due to unusually high loads or low resistance of the structural member itself (due to lower than expected material properties or dimensions). In reality, it has been observed that most structural failures occur due to human error caused by factors such as:

- gross errors in the design of the structure;
- loads applied to the structure that were not anticipated in the design (e.g. an aircraft crashing into a building); or
- inappropriate construction methods.

This underlines the need for proper quality control in engineering design and construction including appropriate work practices, supervision and checking.

11.4 SELECTION OF SAFETY COEFFICIENTS

As outlined in Chapter 3, most engineering design work is guided by codes of practice that specify minimum levels of safety to ensure that the frequency of failure is within limits that are acceptable to the community. The setting of these levels of safety involves a balancing act between overly conservative design on the one hand and unconservative design on the other. If the levels of safety chosen lead to overly conservative design, money will be spent on achieving these high standards that could be better employed elsewhere in the economy (e.g. building new hospitals or purchasing additional medical equipment). If the levels of safety are too low, failures (and the consequent loss of life and/or economic loss) will occur more frequently than is acceptable to the community and there will be a public outcry.

Following Warner et al. (1998), it is appropriate to consider the choice of the optimum probability of failure for a particular class of structure (e.g. highway bridges). Clearly as the probability of failure, P_f increases the cost associated with the failure of all bridges also increases as shown in Figure 11.5. On the other hand, increasing the probability of failure is associated with reducing the margin of safety and hence the cost of constructing all bridges as shown in Figure 11.5. The total cost is the cost of failures plus the cost of construction of all highway bridges. The value of P_f that corresponds to the minimum total cost is the optimum probability of failure. In practice, this value may be quite difficult to identify and values of the partial safety coefficients, γ_T and γ_S are often specified in codes of practice based on experience with previous successful design procedures and comparison with a number of standard design cases.

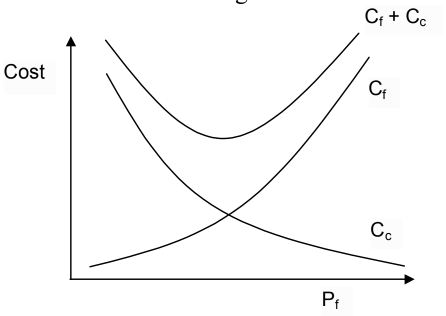

Figure 11.5 Tradeoff between cost and probability of failure, where C_c = cost of construction and C_f = cost of failures (adapted from Warner et al., 1998).

11.5 RELIABILITY, RESILIENCE, VULNERABILITY AND ROBUSTNESS

The **reliability** of an engineering system is defined in Section 11.3 as the probability that it is in a non-failure state at any point in time. Reliability is clearly an important performance indicator for most engineering systems. However, it does not give the total picture. Hashimoto et al. (1982) identified the following three performance measures of a water resource system: reliability, resiliency and vulnerability.

Hashimoto et al (1982) defined *resiliency* as the probability of a system returning from a failure state to a non-failure state in a single time step. This is equal to one divided by the average length of time that a system's performance remains unsatisfactory after a failure. Clearly this definition of resiliency does not apply if system failure corresponds to a catastrophic collapse (e.g., of a building or other structure) from which recovery is impossible. However, it is applicable to systems where failure corresponds to economic loss or inconvenience. For example, the imposition of water restrictions in a city, flooding of an urban area or severe traffic congestion that causes significant delays on a road network. In these cases, it is possible for the system to recover from the failure and perform in a satisfactory manner for an extended period thereafter.

Note that the terms "resilience" and "resiliency" tend to be used interchangeably in the literature. From this point onwards, we will use the term resilience throughout. A more general definition of *resilience* is the ability of a system to recover from large perturbations without changing its basic structure (Fiksel, 2003). This definition is commonly applied to ecological (Holling, 1973) or socio-economic systems (Resilience Alliance, 2010). This is related to the concept of *stability* for mechanical systems. A system is said to be in a stable state if, when perturbed, it returns to that state.

The consideration of resilience in the planning or design of an engineering system leads to a fundamentally different approach to that based purely on system reliability. Reliability-based design considers the system's performance during periods when it is subject to standard loading conditions and the required performance criteria are expected to be met. Hence, reliability-based design is aimed at avoiding failure or providing "fail-safe" performance. Conversely, resilience considers performance during periods when the required performance criteria are not met (i.e. the system is in a failure state). Hence the aim of resilience-based design is to recover from failure and to ensure that the system is "safe to fail" (Butler et al, 2016).

The structural design of buildings in areas with significant likelihood of the occurrence of earthquakes is an example of resilient design. Such structures are designed to withstand the loads imposed by a specific design earthquake with minimal damage. However, in recognition that it is possible that a larger earthquake could occur, the beams, columns and joints of the structure are designed to be ductile, so that, should failure occur, it will not result in a catastrophic collapse of the building. As shown in Figure 11.6, large deformations of the structure may occur, but, provided its structural integrity is maintained, there will be a good chance that the occupants will survive the earthquake.

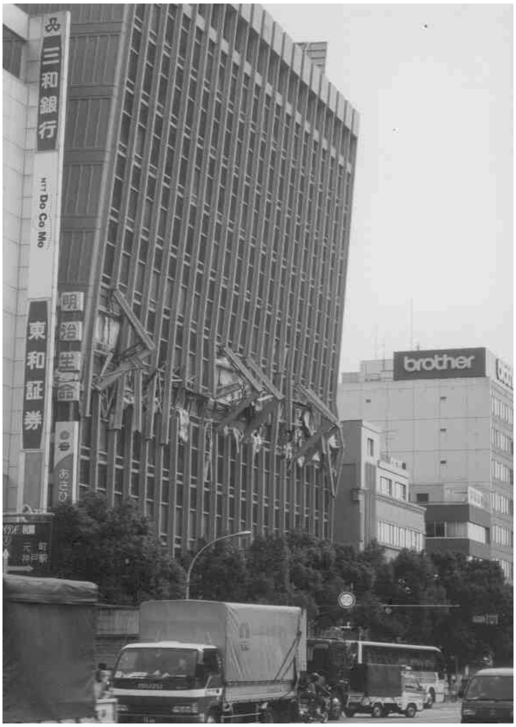

Figure 11.6 A building in Kobe, Japan that failed in the 1995 earthquake but did not collapse due to ductility in its beams and columns (© M. C. Griffith).

Hashimoto et al. (1982) defined *vulnerability* as the average magnitude of failure of a system, given that it does fail. This is sometimes expressed as a percentage of the average demand or load on the system, so that it is dimensionless. It is desirable for a system to have high values of reliability and resilience but a low value of vulnerability. However, Hashimoto et al. (1982) showed that, for a water resource system there is usually a trade-off between the three measures, so that the system that has the lowest vulnerability is unlikely to have the highest reliability or the highest resilience and vice versa.

Another concept related to system performance is *robustness*. Robustness is a measure of the insensitivity of the performance of a given system or plan to uncertain future conditions (Maier et al., 2016). Hence a robust system or plan is one that performs well over a wide range of future conditions or scenarios. The concept is illustrated by the example given in the following interest box.

Reliability, Vulnerability and Robustness of Southern Adelaide's Water Supply System

Paton et al. (2014) carried out a multi-objective planning study of future water supply options for Southern Adelaide, south Austrialia. The population of the area is approximately 600,000 people. In 2009 the city's water supply was provided primarily from reservoirs in the nearby Mount Lofty Ranges and inter-basin transfers from the River Murray (70 km to the east of the city). Future water supply options considered were combinations of the following: a desalination plant (of various capacities), a number of stormwater harvesting schemes (for non-potable supply) and household rainwater tanks. The planning horizon was from 2010 to 2050. The objectives considered were to: (a) minimise the present value of capital and operating costs of the system; (b) minimise the total greenhouse gas emissions; and (c) minimise vulnerability of the system (maximum shortfall in supply). Each of these was evaluated for the full planning horizon.

The system reliability was constrained to be greater than or equal to 95% and the average maximum duration of failure (corresponding to the imposition of severe water restrictions) was constrained to be less than or equal to 365 days. The average maximum duration of failure is the inverse of the resilience of the system according to the definition of Hashimoto et al. (1982).

The optimisation was carried out for the most likely climate change scenario and a medium level of population growth. A post-optimality analysis of system robustness was carried out for selected plans that were identified in the multi-objective optimisation. The aim of this analysis was to consider how the various plans performed under changes in meteorological factors due to climate change and changes in demand due to different population projections. Each plan was evaluated under 252 possible scenarios. These were combinations of 7 possible global circulation models, 6 emissions scenarios and 6 projections of future population for the city. Robustness for each plan was defined as the percentage of the 252 scenarios under which the plan exhibited acceptable performance. Acceptable performance was defined as follows: (a) reliability greater than or equal to 95%; (b) maximum duration of failure less than or equal to 365 days; and (c) maximum vulnerability less than or equal to 27% of demand.

A summary of the objectives and performance measures for the six selected plans is given in the table below. The selection of a final plan requires the use of multi-criteria analysis methods (Section 12.7) considering all six objectives and performance metrics.

Solution number	2010 NPV total system cost ($billion)	Total system GHG emissions (millions tonnes CO_2e-)	Average maximum annual vulnerability (% of demand)	Reliability (%)	Average maximum resilience (days of failure)	Robustness (% of scenarios exhibiting acceptable performance)
1	3.16	6.28	23.7	95.1	92.9	64.8
2	4.31	5.09	23.5	95.5	116.6	43.9
3	3.27	6.82	14.7	95.1	73.6	63.9
4	4.14	8.94	0.0	100.0	0	78.7
5	5.08	7.59	0.0	100.0	0	80.6
6	6.23	5.27	7.3	97.3	28.5	78.7

11.6 RELIABILITY OF ENGINEERING COMPONENTS

Many engineering systems contain a large number of components, any one of which can fail at a particular point in time with varying consequences to the overall system performance. For example, a water supply system for a city may consist of thousands of pipes, hundreds of pumps and valves and tens of tanks. The impact of the failure of each one of these will vary depending on its function and location in the system, its capacity, the time of day and of the year, the number of customers affected and so on. We now want to consider how the reliability of system components may vary over time.

Figure 11.7 shows a commonly observed pattern for failure rates of engineering components (Agarwal, 1993; Hyman 1998). This is the so-called "bath tub" model of component failures.

The probability of failure per unit time is high initially during the "break in period", as some components fail due to poor materials or workmanship as they are placed under stress for the first time. During the mature phase of operation, a small number of failures occur due to unexpected causes such as occasional high loads or localised weak points. During this period, the failure rate per unit time is approximately constant. As the components begin to reach the end of their useful lives, the failure rate starts to increase as the effect of corrosion and fatigue take effect. This is the so-called "wear out period".

A simple analysis can be carried out for the mature phase by assuming that the probability of a component failure per unit time is constant and equals λ. Under these conditions, Hyman (1998) derives the following equation for the reliability of a component:

$$R(t) = e^{-\lambda t} \qquad (11.19)$$

where *R(t)* is the probability that the component does not fail in the time period 0 to *t*.

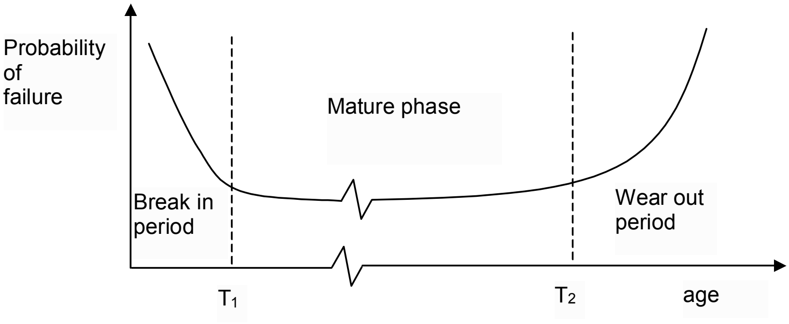

Figure 11.7 Typical failure rates for engineering components.

Another important measure is the mean time to failure, *MTTF*, which is defined as the average time that a component will be in service before failure occurs. Hyman (1998) shows that the following relationship holds:

$$MTTF = \frac{1}{\lambda} \tag{11.20}$$

Example: Light bulbs manufactured by a particular company have a mean time to failure of 250 hours. Assuming that the bulbs have a constant probability of failure, what is their reliability for a period of 100 hours? 250 hours?

Answer: Applying Equation (11.20),

$$\lambda = \frac{1}{MTTF} = \frac{1}{250} = 0.004 \text{ hour}^{-1}$$

therefore:

$$R(100) = e^{-0.004x100} = 0.670$$
$$R(250) = e^{-0.004x250} = 0.368$$

Thus, only 36.8% percent of the light bulbs are expected to last to the mean time to failure and 67% will last 100 hours or more. The apparently high failure rate in the first 100 hours (33%) is a consequence of the assumption of a constant failure rate. In reality, they are more likely to have a low initial failure rate that gradually builds up over time.

11.7 SYSTEM RELIABILITY

As noted earlier, an engineering system is composed of a large number of non-identical components that interact in some defined way. The failure of individual components can have different consequences on the performance of the system as a whole, depending on the nature of the components and how they are connected together. We will consider two simple cases to demonstrate this effect.

Series System

Consider a system that consists of a set of components in series. For example, consider a chain comprised of n links. The failure of any one of the links will cause the chain to fail. From elementary probability theory, the probability that the system does not fail is the product of the individual probabilities of non-failure (assuming that the failure of each component is independent), i.e.,

$$R_{series} = R_1 \times R_2 \times R_3 \times \dots R_i \times \dots R_n \tag{11.21}$$

where R_{series} is the reliability of the series system and R_i is the reliability of component i. Therefore, a series system has a reliability that is less than the lowest reliability of any of its components.

In the special case that each component has a failure rate that is constant with time, Equation (11.19) gives:

$$R_i = e^{-\lambda_i t} \qquad (11.22)$$

and hence Equation (11.21) becomes:

$$R_{series} = e^{-\lambda_1 t} \times e^{-\lambda_2 t} \times e^{-\lambda_3 t} \times \ldots e^{-\lambda_i t} \times \ldots e^{-\lambda_n t} \qquad (11.23)$$

hence:

$$R_{series} = e^{-\lambda_s t} \qquad (11.24)$$

where the failure rate of the series system per unit time is given by:

$$\lambda_s = \lambda_1 + \lambda_2 + \ldots + \lambda_i \ldots\ldots\ldots + \lambda_n \qquad (11.25)$$

Thus, in a series system where each component has a constant failure rate, the system failure rate will also be constant and will equal the sum of the individual failure rates.

Parallel Systems

A parallel system will not fail unless every component of the system fails. An example is a set of parallel pipes supplying water to part of a city. Clearly if one pipe fails, water can still be supplied to the city (presumably at a reduced pressure or level of service). However, if failure is defined as having no water available, all pipes must fail before system failure occurs.

For a parallel system with n components, the probability of system failure is the probability that all components fail. Therefore, (assuming independence of the individual components) the probability of failure for the system as a whole is given by:

$$P_{f.parallel} = P_{f1} \times P_{f2} \times \ldots P_{fi} \times \ldots P_{fn} \qquad (11.26)$$

where $P_{f.parallel}$ is the probability of failure of a parallel system and P_{fi} is the probability of failure of component i. As reliability is defined as one minus the probability of failure, Equation (11.26) becomes:

$$\left(1 - R_{parallel}\right) = (1 - R_1) \times (1 - R_2) \times \ldots (1 - R_i) \times \ldots (1 - R_n) \qquad (11.27)$$

It can be shown that the reliability of a parallel system is always greater than the reliability of its most reliable component. Given this high level of reliability, why don’t we design all engineering systems as parallel systems? The answer is that there is a high cost of providing redundancy. Parallel systems are used when high levels of reliability are required. For example, all hospitals have an emergency power supply consisting of a motor-generator set that will start if the regular supply of electricity fails. This ensures that patients on life support systems are not at risk in the event of a power failure. Most pumping stations are designed to have a number of pumps in parallel. This not only allows for the flow provided by the pumps to vary as the demand on the system varies, but also allows for redundancy should one of the pumps break down.

Unlike series systems, parallel systems do not have constant failure rates per unit time, even if all of their components do.

Mixed Systems

Many real engineering systems do not correspond to simple series or parallel systems. They are described as mixed systems. A mixed system can be analysed by breaking it into a set of series and parallel systems and calculating the reliability one step at a time. For example, Figure 11.8(a) shows a mixed system. Figures 11.8(b) through 11.8(e) show thesteps involved in computing its reliability.

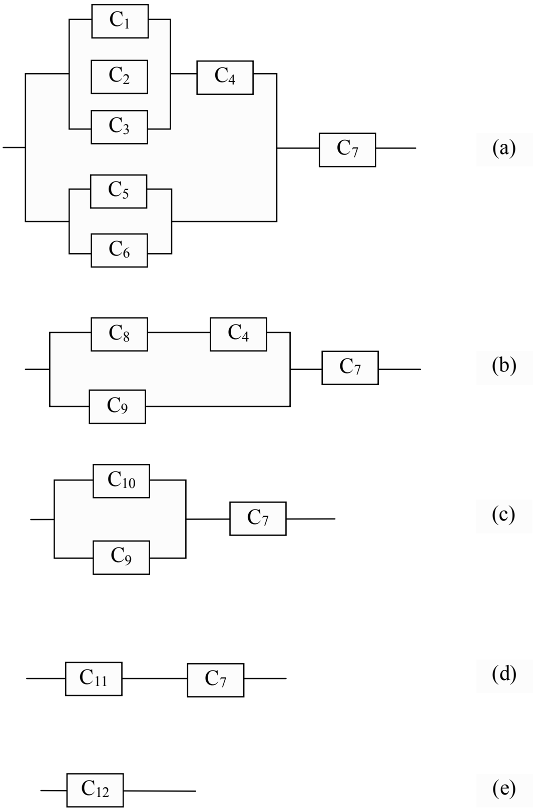

Figure 11.8 Steps involved in reducing a mixed system to a simple system.

11.8 SUMMARY

Knowledge of the concepts of risk and reliability are fundamental to the planning and design of engineering systems. Risk involves two components: the likelihood of an abnormal event or failure occurring and the consequences of that event or failure. All humans face risks on a daily basis. While the probability of failure of engineering systems cannot be reduced to zero, it is the role of the engineer to ensure that this probability is kept within bounds that are acceptable to the community.

The reliability of a system at a particular point in time is the probability that it will be in a non-failure state at that time. Engineering systems can be designed to achieve a specified level of reliability due to known hazards, although there are often unexpected hazards that are impossible to quantify. In the latter case, planning and design must rely on past experience or obtaining additional information that can help quantify the risks. Identification of the appropriate level of reliability of an engineering system may be viewed as a trade-off between the cost of construction or manufacture and the expected cost due to failure.

In addition to reliability, resilience, vulnerability and robustness of a system may also be important in planning and design. Resilience is the probability of the system returning from a failure state to a non-failure state in a single time step. Vulnerability is the average magnitude of failure of a system, given that it does fail. A system with a high reliability does not necessarily have a high resiliency or low vulnerability and vice versa. Robustness is a measure of the insensitivity of the performance of a given system or plan to uncertain future conditions.

Most engineering components wear out over time. Knowledge of this behaviour can be used to assess the reliability of a system or component over a specified period and hence to plan the repair or replacement of components in an optimal fashion.

An engineering system is usually composed of many different components, each with its own reliability. The reliability of the system can be determined based on the reliabilities of its individual components and the manner in which they are connected. However, the calculations can be very complex. Series systems and parallel systems represent simple cases of engineering systems.

PROBLEMS

11.1 A cable is used to raise and lower a hopper in a mine shaft. The properties of the cable are given in Table 11.5.

Table 11.5 Properties of cable for mine hopper.

Characteristic	Mean value	Standard deviation
Cross-sectional area (mm^2)	10	0.8
Failure stress (MPa)	300	30

The maximum load applied to the cable has a mean value of 2000 kN with a standard deviation of 400 kN. Assume all random variables are normally distributed and independent of each other.

(a) Estimate the mean and standard deviation of the resistance of the cable. Note if X and Y are two independent random variables with means m_x and m_y and coefficients of variation V_x and V_y (respectively) and $W = XY$, then the mean of W, m_w, and the coefficient of variation of W, V_w, can be found using the following equations (Benjamin and Cornell, 1970):

$$m_w = m_x m_y$$
$$V_w^2 = V_x^2 + V_y^2 + V_x^2 V_y^2$$

(b) What is the mean and standard deviation of the safety margin, Z?
(c) What is the value of the safety index, β?
(d) What is the probability of failure?
(e) If the coefficient of variation of the cross-sectional area remains constant at 8%, what is the mean value of cross-sectional area that corresponds to a probability of failure of 0.01? (Hint: Try trial-and-error using a spreadsheet.)

11.2 A computer part has a per unit failure rate of 0.002 failures per day.

(a) What is the probability that this part will fail in it first year of operation?
(b) What value of the per-unit failure rate will ensure a probability of failure of less than 5% in the first year?

11.3 A power generating system has four components with probabilities of failure of 0.003, 0.0025, 0.004 and 0.001 (respectively). The system only fails if all of the components fail. What is the reliability of the system?

11.4 Four system components (A, B, C and D) have the following reliabilities: 0.99, 0.90, 0.95 and 0.92 (respectively). Determine the reliabilities of the following systems:

(a) A and B combined in series.
(b) C and D combined in parallel.
(c) A and B combined in parallel and the resulting system combined in series with C and D.

11.5 A water pump has a reliability of 0.85. How many pumps should be combined in parallel so that the total system has a reliability of 0.95?

REFERENCES

Agarwal, K.K., 1993, Reliability engineering. (Kluwer Academic Publishers, Dordrecht, The Netherlands).

BC Hydro, 1993, Guidelines for Consequence-Based Dam Safety Evaluations and Improvements, Report number H2528, (BC Hydro: Hydroelectric Engineering Division).

Benjamin, J.R. and Cornell, C.A., 1970, Probability, statistics and decision for civil engineers. (McGraw-Hill, New York, NY.)

Bernstein, P.L., 1998, *Against the Gods. The Remarkable Story of Risk,* (New York, John Wiley & Sons).

Buck, N. And Associates, 2006, *Company Directors Course. Module 8: Risk Issues for the Board*, Australian Institute of Company Directors, Sydney.

Butler, D, Ward, S, Sweetapple, C, Astaraie-Imani, M, Diao, K, Farmani, R and Fu, G, 2016, Reliable, resilient and sustainable water management: the Safe & SuRe approach, *Global Challenges*, Open Access, John Wiley & Sons Ltd.

Dougherty, E.M. and Fragola, J.R., 1988, *Human Reliability Analysis,* (New York, John Wiley & Sons).

Fiksel, J., 2003. Designing resilient, sustainable systems. *Environ. Sci. Technol.*, 37(23), 5330–5339.

Hashimoto, T., Stedinger, J.R. and Loucks, D., 1982. Reliability resiliency and vulnerability criteria for water resource systems performance evaluation, *Water Resources Research,* 18(1), 14-20.

Heyworth, J.S., Glonek, G., Maynard, E.J., Baghurst, P.A. and Finlay-Jones, J. , 2006, Consumption of untreated tank rainwater and gastroenteritis among young children in South Australia, *International Journal of Epidemiology*, 35, 1051–1058.

Holling, C. S., 1973, Resilience and stability of ecological systems, *Ann. Rev. Ecol. Systems*, 4, 1-23.

Hyman, B., 1998, *Fundamentals of Engineering Design,* (Upper Saddle River, New Jersey, Prentice Hall).

Maier, H.R., Guillaume, J.H.A., van Delden, H., Riddell, G.A., Haasnoot, M. and Kwakkel, J.H., 2016, An uncertain future, deep uncertainty, scenarios, robustness and adaptation: How do they fit together?*, Environmental Modelling and Software*, **81**, 154-164, DOI: 10.1016/j.envsoft.2016.03.014

Morgan, G.C., 1990, Quantification of risks from slope hazards, Proceedings of GAC Symposium on Landslide Hazard in the Canadian Cordillera.

Paton, F.L., Maier, H.R. and Dandy, G.C., 2014, Including adaptation and mitigation responses to climate change in a multiobjective evolutionary algorithm framework for urban water supply systems incorporating GHG emissions, *Water Resources Research,* 50 (8), 6285-6304.

Reid, S.G., 1989, Risk acceptance criteria for performance-oriented design codes, Proceedings of ICOSAR'89, the 5th International Conference on Structural Safety and Reliability, (San Francisco).

Resilience Alliance, 2010, Assessing resilience in social-ecological systems: Workbook for practitioners. Version 2.0. Online: http://www.resalliance.org/3871.php

Stone, A. 1988. The tolerability of risk from nuclear power stations. *Atom 379,* May, 8–11.

U.S. Nuclear Regulatory Commission, 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* WASH-1400 (NUREG 75/014).

Warner, R.F., Rangan, B.V., Hall, A.S. Faulkes, K.H., 1998, *Concrete Structures*, (Melbourne: Longman).