Assessing risk in engineering, work and life

About this free course

This free course is an adapted extract from the Open University course T193 *Engineering: frameworks, analysis, production*: http://www.open.ac.uk/courses/modules/t193.

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –

Assessing risk in engineering, work and life

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Contents

Introduction 4
Learning Outcomes 5
1 Risk and why it is important 6
1.1 Engineers and risk 6
1.2 Evaluating risk 7
1.3 Assessing risk 8
2 Accidents 12
2.1 Accident triangle 13
2.2 Human error 15
2.3 Analysing ‘incidents’ 16
2.4 After the accident 19
2.5 Risk perception 20
3 Risk measurement and risk management 25
3.1 Expressing probability 25
3.2 Calculating probability 29
3.3 Probability in everyday life 37
3.4 Risk management 39
Conclusion 43
References 43
Acknowledgements 44

Introduction

All human activities carry some risk that the activity will lead harm to people, the wider environment or have some other unwanted effect. This is true for everything from crossing a road to operating a major oil refinery. We all do these risky things because they carry benefits; crossing a road allows someone to get to the place they need to be at and we all rely on the products from oil refining every day of our lives.

This free course, *Assessing risk in engineering, work and life,* outlines the issue of risk, which is something that must be taken into account at all times. This is essential to ensure the safety of colleagues, employees, the general public, you and your families. However, risk is not just about health and safety or environmental protection; there are a variety of other risks which could be economic, societal or political. In addition, the failure of a project might itself be 'risky'. The important thing is to recognise what is meant by risk and, as a result, plan for it as much as possible.

Section 1 examines what is meant by risk and why it is important. Section 2 includes case studies of major accidents to illustrate some important aspects of risk and how we perceive it. Section 3 introduces probability as a method for evaluating risk, and finishes by considering risk management.

This OpenLearn course is an adapted extract from the Open University course T193 *Engineering: frameworks, analysis, production*.

Learning Outcomes

After studying this course you should be able to:

- understand what is meant by risk
- carry out a basic risk assessment
- understand how accidents can be caused
- use probability to assess risk and minimise the occurrence of undesirable outcomes.

1 Risk and why it is important

Risk is a word that seems to be ever-present in the language of both the engineering profession and the general public. It is a word of such common usage that people tend to assume that they know its meaning.

- Before continuing, write down your own definition of risk.
- The *Oxford English Dictionary* (2016) gives many definitions of risk. For example, the definitions of 'risk' as a noun include:
  - The possibility that something unpleasant or unwelcome will happen.
  - A person or thing regarded as a threat or likely source of danger.

  But also, perhaps more interestingly, the definitions of 'risk' as a verb include:
  - Act in such a way as to bring about the possibility of (an unpleasant or unwelcome event).
  - Incur the chance of unfortunate consequences by engaging in (an action).

Risk is something that is accepted as part of everyday life. The safety that people seek is constantly balanced against the benefits that they desire, which come with an associated risk. Perhaps a good example here is driving. All drivers think of their driving as safe, but most drivers have performed an overtaking or other manoeuvre which, in retrospect, would be considered 'risky'. This section investigates how engineers can identify, assess and manage risks, and looks at what part they play in this process.

1.1 Engineers and risk

The role of the engineer in identifying and managing risks has been recognised by the engineering profession. Among its aims and objectives, the UK's Engineering Council stresses the importance of a proper balance between efficiency, public safety and the needs of the environment when carrying out engineering activities. The Council's guidance for institutional codes of conduct expects engineers to address risk thoroughly – applying in-depth, long-term thinking – so that they may help to encourage greater awareness of risk in others with whom they work. The key elements of the Engineering Council's Guidance on Risk are listed below.

1. Apply professional and responsible judgement and take a leadership role.
2. Adopt a systematic and holistic approach to risk identification, assessment and management.
3. Comply with legislation and codes, but be prepared to seek further improvements.
4. Ensure good communication with the others involved.
5. Ensure that lasting systems for oversight and scrutiny are in place.

6 Contribute to public awareness of risk.

(Engineering Council, 2011, p. 2)

Points 4 and 6 are often neglected, but are an important part of the engineer's role. Without good communication of the risks, the public, politicians and regulators may prevent a low-risk project from taking place or allow a dangerous project to proceed. The communication of risk is covered in Section 2.

For now, you need to think about the situations where you are likely to be considering risk at work. A few examples are:

- the risk of failure of a structure
- health and safety risk, such as exposure to harmful chemicals or things you might trip over
- the risk of whether a cheaper solution to a problem will still do the job without compromising safety, quality, profitability, environmental protection, and so on.

Figure 1 outlines some of the different aspects of risk you could encounter in your professional life.

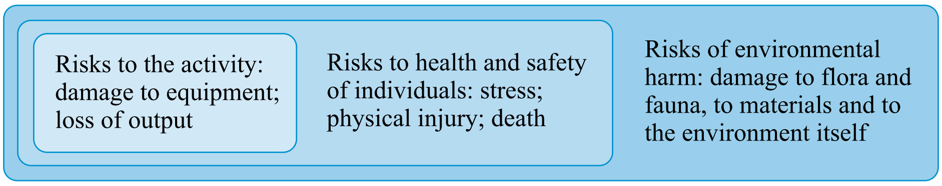


Figure 1 Risks to various systems

Some of the risks mentioned in Figure 1 are important because of their economic consequences, such as loss of production, equipment failure, increased maintenance costs or perhaps early replacement. But these are not the only concerns. Health and safety risks in the engineering profession can be substantial. What can happen if things go wrong? Well, in the very worst case, as a result of actions, decisions or perhaps inactions, people may die or suffer serious injuries, or serious environmental damage may be caused.

1.2 Evaluating risk

Sadly, workplace fatalities and injuries happen far too often. Taking the UK in the year April 2016 to March 2017 as an example, according to data from the Health and Safety Executive (HSE), across all industries 137 people died as a result of their work. Furthermore, 92 members of the public were fatally injured in accidents connected to work (HSE, 2016). These fatalities are broken down by sector in Table 1. Many of these deaths occurred in sectors where the main activities can be described as engineering, or in areas employing large numbers of engineering professionals. This shows that the importance of assessing and working to reduce risks is a vital part of the work of all engineers that cannot be overstated.

This table raises the questions of how professionals, policymakers and the public evaluate risk in a particular industry, and how it can be decided what is 'risky' to a particular individual.

Table 1 UK work-related fatal injuries, April 2016 to March 2017

Main industrial sector	Workers	
	Total	**Per 100 000 employees**
Agriculture	27	7.73
Mining and quarrying	4	[a]
Manufacturing	19	0.66
Gas, electricity and water supply	3	[a]
Waste management and recycling	14	12.69
Construction	30	1.37
Services	40	0.16
Total	**137**	**0.43**

Notes: [a] Not calculated because employment estimates are too small or otherwise too unreliable to produce meaningful statistics.

(Source: data taken from HSE, 2017)

1.3 Assessing risk

Engineers and other professionals need to be able to assess potential risks. This is the first stage in the process of deciding which risks are acceptable. This in turn allows priorities to be assigned to developing and implementing strategies to reduce risks.

- What types of risk might you look at in a health and safety context?

  (*Hint*: think about your own workplace, places you visit and your home and the kinds of things that could go wrong.)

- Perhaps the most obvious areas to consider are:

  - accidents – any unintended occurrence, regardless of whether it leads to damage or, if so, the type of damage
  - injuries – any harm (physical or non-physical) to a person due to an accident
  - illnesses – any detriment to a person's well-being from accidents, exposure to harmful substances, poor working conditions, mental stress, etc. (generally speaking, illness covers longer-term issues than injuries, but the two areas do overlap)
  - near misses – any incident that could easily have resulted in harm (for example, a person trips but manages to avoid falling).

The first stage in assessing and managing risk is to identify the hazards. A hazard can be thought of as anything that might cause harm. There are many hazards both in the workplace and in life in general – for example, toxic or harmful chemicals, electricity, falling off a ladder or standing in an inappropriate area like a busy access road.

Risk

The risk associated with a particular hazard is the chance that somebody could be harmed, together with an indication of how serious the harm could be. Hence risk is often expressed in the form of an equation:

risk = severity of harm × likelihood of occurrence

A common way to use this equation is to rank both severity and likelihood on a scale of 1 to 5, and to set thresholds for action based on the result.

Table 2 shows some of the criteria that can be used in order to rank both the severity and the likelihood of a given risk, in order to use the risk equation.

Table 2 Risk assessment ranking

Severity	**Likelihood**
1 – Trivial, e.g. bruise or bump	1 – Remote (almost never)
2 – Minor, e.g. small cut or abrasion	2 – Unlikely (rare)
3 – Moderate, e.g. strain, sprain, off work <5 days	3 – Possible (could occur but not common)
4 – Serious, e.g. fracture, incapacitation, off work >5 days	4 – Likely (will probably occur once)
5 – Fatal or life-changing, e.g. permanent injury such as blindness or loss of mobility	5 – Imminent (will occur regularly)

You may see the same idea expressed as a matrix, using a ‘traffic light’ system to indicate the acceptability of different risks. An example is shown in Figure 2, but note that different industries will use different criteria for what is acceptable.

Severity	Life-threatening	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Trivial	1	1	2	3	4	5
			1	2	3	4	5
			Remote	Unlikely	Possible	Likely	Imminent
			Likelihood				

Figure 2 Risk assessment matrix (in this example green represents low risk, yellow is medium risk and red is high risk)

As you can see, the overall risk is given by multiplying the two factors together. Once this has been done for a particular activity or process, a threshold for action is required. For example:

- Low risk (1–8) – No immediate action is needed, but the activity should be reviewed if any changes occur.

- Medium risk (9–12) – Safe systems of working and controls should be put in place to minimise risk as far as is reasonably practicable.
- High risk (13–25) – The activity should not be allowed to take place. New controls or ways of working must be introduced to reduce the risk before the activity can be permitted to take place.

Example 1 Assessing risk

An employee is working on a machine floor workshop where oil spillages could occur. The oil is slippery and the workshop floor is concrete. Use the matrix in Table 2 to rank the risk and determine the need for remedial action.

Solution

The likelihood of slipping on oil and having an accident could be quite high in these circumstances, hence the likelihood could be rated at 4 or 5. However, in a well-regulated workshop, 3 would be a reasonable value.

The question of severity is even less clear-cut. It could range from a minor bruise (rated 1) through to a fall leading to a broken leg that results in several weeks' loss of work (rated 4).

Taking the optimistic view where the severity is considered to be 1, the risk is given by $3 \times 1 = 3$, requiring no immediate action but review. On the other hand, the pessimistic approach (where a fracture is a real possibility) gives a risk of $3 \times 4 = 12$. This calls for the implementation of controls and safe systems of work to minimise the risk. For instance, it might initiate the construction of a simple bund (a barrier to contain the spill) round the storage tanks, machines and other areas where spills might occur. This would prevent the spills from being a hazard, potentially reducing the risk to 1×1 – a most desirable outcome.

If experience of the workshop justifies an even more pessimistic view, the likelihood could be increased to 5 and the severity to 4. This would give a risk of 20, meaning that work should stop until improvements in practice and control measures are implemented.

Activity 1 Assessing risk

Allow approximately 15 minutes.

A new system has been built in a factory to provide steam for industrial cleaning operations. Steam is stored under pressure in an insulated vessel and released when needed through a valve. If this valve were to fail, the vessel would vent rapidly and cause fatalities if people were nearby. People do not normally work near the vessel but walk past it on their way to other parts of the building. Out of every 10 000 valves made, one is expected to fail during its 20-year design lifetime. How would you assess this risk?

Discussion

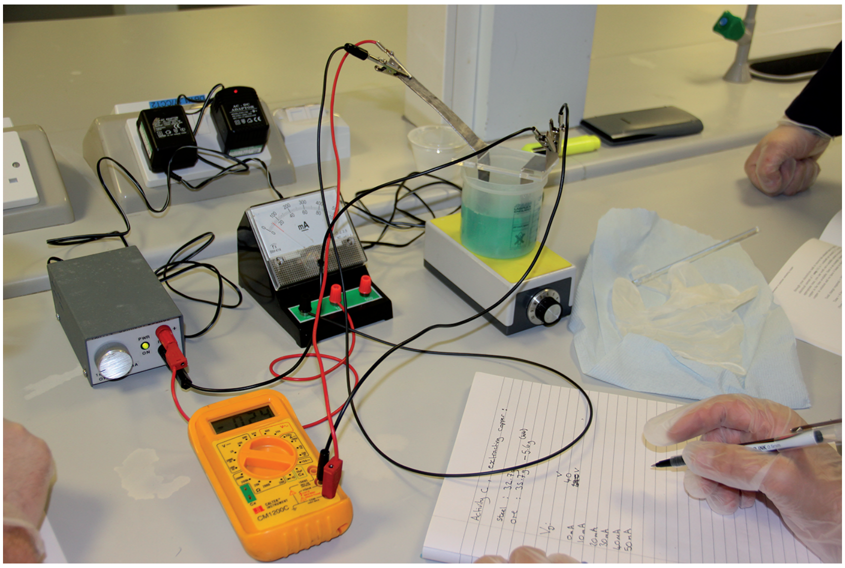
The valve will have a severe impact if it fails when someone is close by, so the severity of failure has to be rated at 5. Evaluating the likelihood of failure is more complex. If 1 in 10 000 valves fails during its design lifetime, it could be argued that this is a rare event (likelihood of 2); equally, the event could be classed as 'could occur but is not common' (ranking of 3). This gives a risk rating of between $2 \times 5 = 10$ and $3 \times 5 = 15$.

Taking the prudent approach, a rating of 15 means that the activity should not take place. In the short term, use of the vessel should cease while measures are put in place. This could involve relocating the system outside the building or in an isolated room, finding an alternative to steam cleaning or steam storage, or installing a higher-specification valve.

This matrix method of assessing risks is widely used in many industries. Figure 3(a) gives an example of its use in assessing one of the laboratory activities carried out by Open University engineering students during a residential school, as shown in Figure 3(b).

Step 2 Hazard Type	Location and Type of Hazard (Is there an OU Guidance Note in operation ? if so give reference code in final column)	*Step 3* Risk Level (Table 1) Tolerable Risk	Moderate Risk	Serious Risk	Intolerable Risk	Guidance Note Reference
Chemical	Sulphuric acid (2% solution in water) – corrosive to skin and eyes.		✓			a
	Simulated copper ore (clay and copper II carbonate) fine powder – irritant dust.		✓			b
	Ethanol – irritant to eyes and respiratory system		✓			c
	Ammonium hydroxide (25% solution in water) corrosive to skin and eyes. Irritating to respiratory system.		✓			d
	Decon-90 (lab detergent)		✓			e
Electrical	Mains powered vacuum pump, d.c. power supply and stirrer	✓				f
Other (state)	Lead strip (solid) – Activity briefing for activity must cover issue of safety of lead and lead solders for expectant women and women of child-bearing age. See additional note below. Gloves must be worn at all times.		✓			g
	Safety spectacles MUST be worn AT ALL TIMES by students and anyone demonstrating working on or in the vicinity of the activity.					
	Bags to be stored under the benches clear of walkways					
	Hands to be washed and dried on leaving laboratory					

(a)



(b)

Figure 3 (a) Use of a risk assessment matrix; (b) laboratory activity related to this risk assessment

This type of assessment is fine for most normal workplaces. In industries where the results of an incident can be far more severe (such as oil and gas production, chemical manufacture, nuclear power generation), a more complex evaluation system is used, but it is still based on combining likelihoods and severity.

The fact that risks need to be assessed does not mean that all risks must be eliminated – indeed, that would be impossible. The aim is normally to reduce risk *as far as is reasonably practicable* (discussed in Section 2), which means that the risk in a particular activity or environment can be balanced against the time, trouble, cost and physical difficulty of taking measures to avoid that risk. Normally a variety of calculations are used to decide what is practicable. These are not covered in this course, but would generally include an economic assessment of reducing a risk against accepting the risk, and use an equation linking the severity of a risk and its likelihood.

When it comes to evaluating an environmental risk, the calculation might be a little different. In this scenario, evaluation would not normally cover the risk of one event or one consequence. Instead, there may be many inputs over an extended time period that go into the calculation of risk, and many outcomes – some related to harm to humans, but others concerning harm to the environment. This could include impacts on water courses, on air quality, or perhaps on neighbouring industries including farms or other food production. Such assessments might involve considering threats of serious or even irreversible damage on a large scale.

2 Accidents

Where there is risk, there are likely to be accidents.

- What is your understanding of an 'accident'?
- Everyone has their own ideas of what an accident is and the *Oxford English Dictionary* (2016) defines an accident as:
  - An unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury.
  - An event that happens by chance or that is without apparent or deliberate cause.

The Health and Safety Executive in the UK defines an accident as 'any unplanned event that resulted in injury or ill health of people, or damage or loss to property, plant, materials or the environment or a loss of business opportunity' (HSE, 1999, p. 8).

There are many different ways to define an accident, but the key characteristics of any event that could be described as an accident seem to be:

- the degree of expectedness – the less the event is expected, the more it is regarded as an accident
- the avoidability – the less likely it is that the event can be avoided, the more it is seen as accidental
- the lack of deliberateness – the less a person or persons are involved in causing an event to occur, the more it is viewed as an accident.

This gives the impression that an accident is unfortunate, but also more importantly that it could not be foreseen. But is that always true – is every accident unavoidable?

In fact, many 'accidents' are preventable or avoidable. Typically before an accident there may have been warning signs. These might be 'near misses' where the accident nearly happened, or where something dangerous happened but luckily no one was hurt. It is very rare for an accident to occur without any previous incidents or concerns. You will look at this in more detail in the next section.

2.1 Accident triangle

The first detailed study of the cost of accidents was made by Herbert Heinrich (1886–1962). As part of this work, Heinrich (1931) developed the concept of a non-injury accident. He defined this as an unintended event that causes property loss by damage to plant, equipment or materials, but does not cause actual injury, although it may have the potential to do so. In his work with around 1500 organisations, Heinrich concluded that for every major injury, there are 29 minor injuries and 300 accidents where no injury takes place. This is illustrated in the 'accident triangle' in Figure 4. Other versions of the triangle include another stage at the base that quantifies the even larger number of 'near misses' – events that could easily have led to accidents.

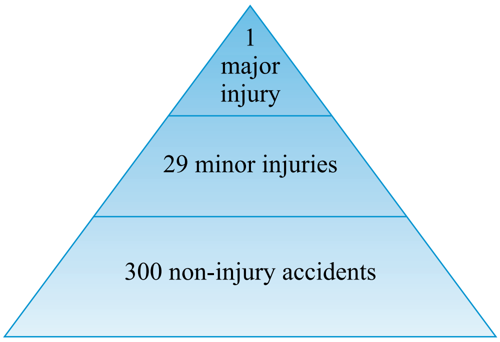


Figure 4 Accident triangle derived by Heinrich in 1931 from a study of 1500 organisations

This triangle illustrates the idea that before the one accident that causes major injury, there are many other incidents that occur leading up to it. For example, if a trip hazard in a workplace is not removed, then many people will stumble but not hurt themselves, a few will trip up and suffer from minor bruising or perhaps a sprain, but one person might fall and break a limb. In terms of health and safety, the role of engineering practice is to recognise the non-injury and minor injury events as they occur, and to put in measures to prevent them from reoccurring. This in turn helps to prevent the major injury events at the top of the triangle from happening.

- A commonly asked question at interviews for people seeking chartered engineer status is 'who is responsible for health and safety in your organisation?' How would you answer this question in relation to your workplace, another organisation that you may be involved with, or your home?
- It is tempting to talk in terms of organisational charts or perhaps to name the safety manager, but a better answer is to simply say 'everybody'. All staff, subcontractors and even visitors have a responsibility to behave in a safe manner and to report potential accidents that they notice.

Deepwater Horizon

Deepwater Horizon was an offshore drilling rig designed to drill holes into the ocean floor to explore for oil. In 2010 it was operating on the Macondo well in the Gulf of Mexico off the coast of Louisiana, USA when, according to BP's accident investigation report:

> On the evening of April 20, 2010, a well control event allowed hydrocarbons to escape from the Macondo well onto Transocean's Deepwater Horizon,

> resulting in explosions and fire on the rig [Figure 5]. Eleven people lost their lives, and 17 others were injured. The fire, which was fed by hydrocarbons from the well, continued for 36 hours until the rig sank. Hydrocarbons continued to flow from the reservoir through the wellbore and the blowout preventer (BOP) for 87 days, causing a spill of national significance.
>
> […]
>
> The team did not identify any single action or inaction that caused this accident. Rather, a complex and interlinked series of mechanical failures, human judgments, engineering design, operational implementation and team interfaces came together to allow the initiation and escalation of the accident. Multiple companies, work teams and circumstances were involved over time.
>
> (BP, 2010, pp. 3, 5)

Figure 5 The Deepwater Horizon accident

The investigation found that there were eight interlinked events that were found to contribute to the overall accident:

- A cement barrier designed to isolate the hydrocarbons in the well was inadequate.
- A valve designed to prevent hydrocarbons from entering the well casing failed.
- The results of a pressure test that indicated there was a problem were misinterpreted.

- The readings from pressure sensors that showed there was a problem were not identified or acted on until hydrocarbons were escaping from the BOP.
- The escaping fluids were diverted to the mud gas separator (MGS) rather than to the overboard diverter line. Had the diversion been to the diverter line, this may well have given those involved more time to respond, thereby reducing the consequences of the incident.
- Diversion to the MGS meant that hydrocarbons were vented onto the rig, increasing the likelihood of them coming into contact with a source of ignition.
- The fire and gas control system was inadequate.
- Three methods for operating the BOP in emergency mode all failed to seal the well.

The large accident occurred because of the failure in all these smaller but interlinked events, demonstrating the importance of preventing even the most apparently minor incidents.

2.2 Human error

There is one more aspect to discuss in identifying the cause of accidents. Engineers can work hard at making sure they have the right designs, the right materials, the right working approaches and the right safety systems. As already highlighted, very few accidents are caused by one event or failure; there are potentially various interactive small failures, which eventually coincide to cause the event. However, there is also another consideration: the majority of accidents are caused not by materials or safety systems, but by people. This is known as 'human error' – that is, errors made by people rather than by equipment or systems. In fact, according to Heinrich, 80–90% of accidents are due to human error (Heinrich et al., 1980).

Similarly, an often quoted study of severe and fatal industrial accidents by Salminen and Tallberg (1996) found that 84–94% were due mainly to human error. A national survey of traffic accidents in the USA found that of over two million road accidents, some 94% were due to human error (NHTSA, 2015); only 2% were attributed to vehicles and 2% to the environment. So human error is not a trivial factor to consider.

The influence of human error in a chain of events leading up to an accident can occur despite the best training, standard operation protocols or systems available. Many major accidents were initiated by human error. For example:

- Chernobyl, a nuclear reactor explosion in 1986 that caused around 50 immediate deaths, a currently unknown (but hotly disputed) number of future deaths and the contamination of a massive area of land (WHO, 2006)
- *Piper Alpha*, a fire on a North Sea oil production platform in 1988 that caused the deaths of 167 of the 228 people on board (HSE, 2004)
- Texas City, an oil refinery explosion in 2005 that caused 15 deaths and 180 other injuries (CSB, 2007).

As human error is difficult to eliminate completely, it is important that any design, system or approach takes this into consideration. People make mistakes, or they simply forget to do things, or sometimes they decide not to do things because they do not understand their worth.

Returning to the Deepwater Horizon disaster, the team that investigated the events concluded that a series of eight failures led to the accident. Of these eight, at least three were governed by human decisions: the results of a seal test were misinterpreted, raised flows were not identified as a leak, and there were weaknesses in the BOP testing and maintenance management system. As a result, human error was a significant contributory factor to the overall incident.

2.3 Analysing 'incidents'

You have seen that there may be many causes that contribute to an incident, and that investigators often have to look at many interlinked issues that may have led to an accident. These issues include the failure of management controls relating to human factors, job factors or event component failure. There may also be a lack of knowledge, skills or training among the people involved, or there may be inadequacies in work standards, design, maintenance, and so on. The sequence of 'soft' events that can lead to an incident occurring has been likened to a 'domino effect', as illustrated in Figure 6.

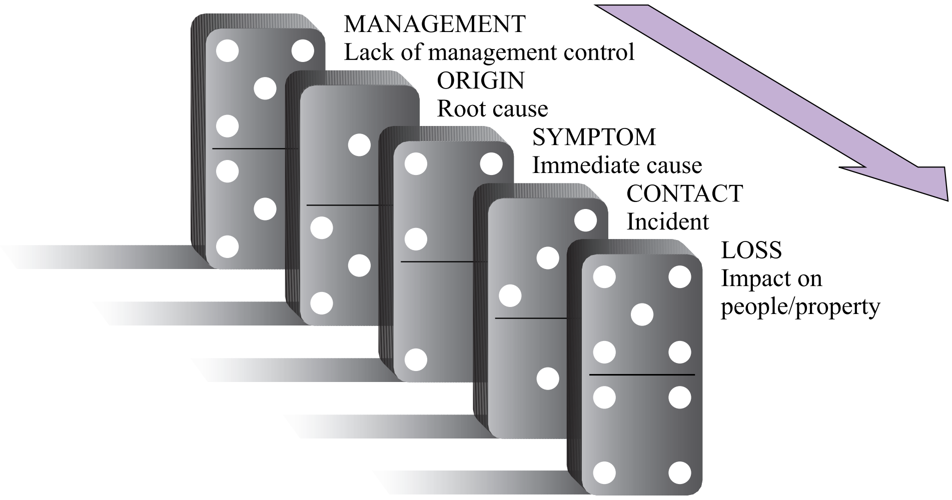


Figure 6 The domino effect

You are in fact considering what the 'causes' of accidents are. With a wide variety of factors having a knock-on effect, it is clear that it is essential to address possible failures at any level. You have already learned that many interlinking factors may result in accidents, so you may need to think about multiple causes that look relatively small in isolation but have the capacity to contribute to a much larger incident. Note that the domino model implies that there is a single pathway to failure – in reality, many situations are more complex, with several potential pathways that could lead to an accident.

- What is your understanding of 'cause' in the context of accidents?
- The *Oxford English Dictionary* (2016) defines a 'cause' as both a noun and a verb:

  A person or thing that gives rise to an action …

  Make (something, especially something bad) happen.

The idea of different causes is illustrated in the following case study.

The Buncefield oil storage depot

In 2005, there was a large explosion and fire at an oil storage depot near Hemel Hempstead, UK. This is how the incident was described in a report from the Health and Safety Executive:

> On the night of Saturday 10 December 2005, Tank 912 at the Hertfordshire Oil Storage Limited (HOSL) part of the Buncefield oil storage depot was filling with petrol. The tank had two forms of level control: a gauge that enabled the employees to monitor the filling operation; and an independent high-level switch (IHLS) which was meant to close down operations automatically if the tank was overfilled. The first gauge stuck and the IHLS was inoperable – there was therefore no means to alert the control room staff that the tank was filling to dangerous levels. Eventually large quantities of petrol overflowed from the top of the tank. A vapour cloud formed which ignited causing a massive explosion and a fire that lasted five days [Figure 7].
>
> (HSE, 2011, p. 4)

Figure 7 The Buncefield oil storage depot accident

The HSE report goes on to comment (emphasis added):

> Failures of design and maintenance in both overfill protection systems and liquid containment systems were the *technical causes* of the initial explosion and the seepage of pollutants to the environment in its aftermath. However, underlying these immediate failings lay *root causes* based in broader management failings:
>
> - Management systems in place at HOSL relating to tank filling were both deficient and not properly followed, despite the fact that the systems were independently audited.
> - Pressures on staff had been increasing before the incident. The site was fed by three pipelines, two of which control room staff had little control over in terms of flow rates and timing of receipt. This meant that staff did not have sufficient information easily available to them to manage precisely the storage of incoming fuel.
> - Throughput had increased at the site. This put more pressure on site management and staff and further degraded their ability to monitor the receipt and storage of fuel. The pressure on staff was made worse by a lack of engineering support from Head Office.
>
> (HSE, 2011, p. 4)

As the case study clearly shows, the Buncefield incident had multiple causes that illustrate the domino effect well. There was a lack of management, there were technical issues, other human factors were present, and they coincided in a chain of events that led to the largest explosion in peacetime Europe. Some of the issues were engineering problems – faulty switches and gauges – but their interaction with operators, and the management of technical equipment, was equally important in determining the cause(s) of the incident.

Whatever view of the causal structure of incidents is taken, the aim should be to look beyond the obvious cause and identify more fundamental ways of eliminating the hazard or reducing the risks by looking at multiple causes and their interactions. Figure 8 puts this into context.

Starting from the accident result at the bottom of the figure, notice that an accident resulting in personal injury or property damage, for example, may be attributed to an unplanned release of energy or material, as discussed previously. However, the root cause of the incident can be human error or management failure, through aspects such as lack of training or supervision.

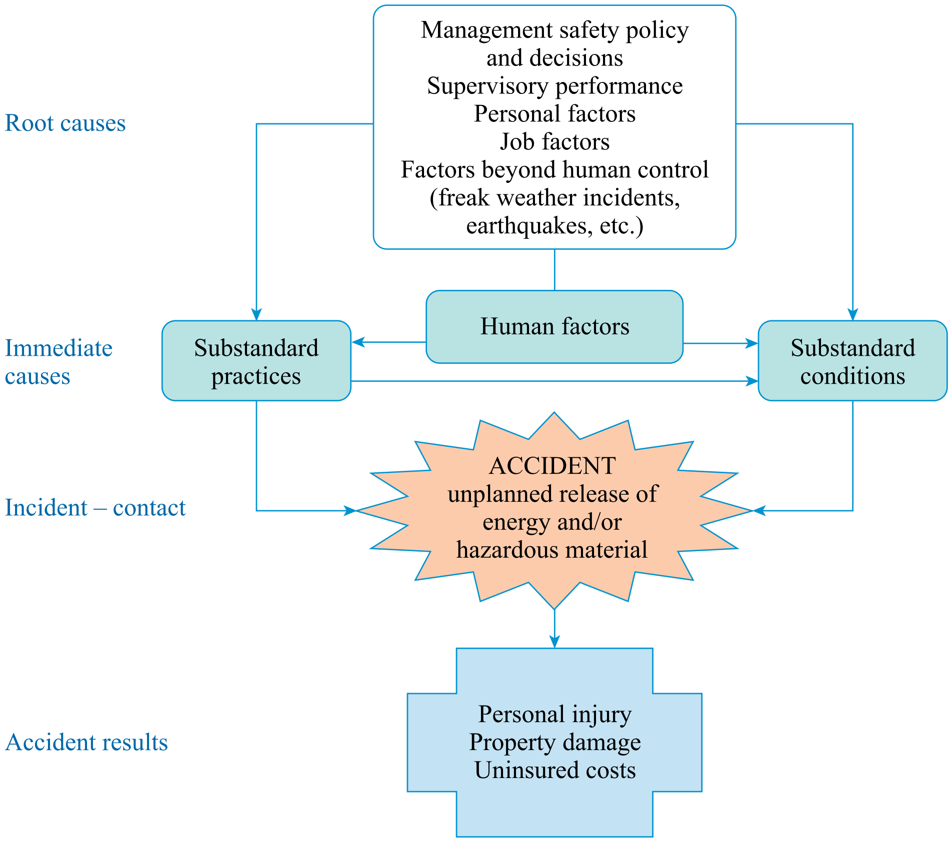


Figure 8 Causes of incidents

2.4 After the accident

Accidents are much more than the initial event. They have far-reaching consequences, but also costs. As part of his work with 1500 organisations, Heinrich examined many thousands of insurance records and interviewed many staff members. He found that the uninsured costs (which he called the indirect costs) were typically four times higher than the direct costs covered by insurance. This relationship is commonly represented as an iceberg (Figure 9).

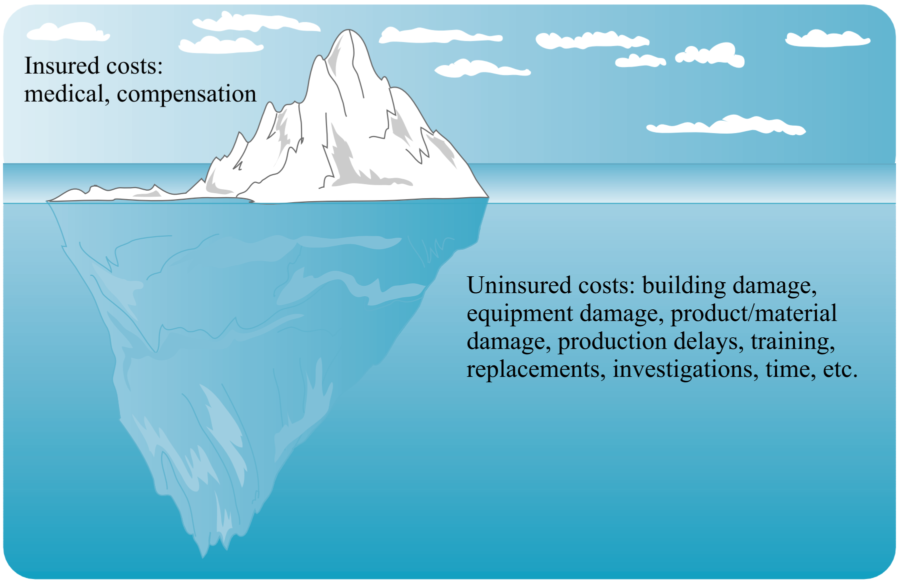


Figure 9 Insured costs are the tip of the iceberg

- List some of the additional uninsured costs of a workplace accident.
- You may have thought of the following:
  - the damage to an organisation's reputation, leading to loss of customers
  - fines levied by the courts if the organisation is found to be negligent
  - increased insurance premiums in future years
  - increased scrutiny from regulators
  - difficulty in obtaining permits and planning for future developments.

Later work by the UK HSE's Accident Prevention Advisory Unit (APAU) on non-injury accidents included all unintended events causing loss, even when there was no potential for causing personal injury. It found that the ratio of uninsured costs to insured costs was substantially greater than Heinrich's 4:1 ratio, ranging from 8:1 to 36:1 (HSE, 1999, p. 56). Clearly, the mix of industrial activities, the management and training within the organisations, and the definitions of accident categories have contributed to different results between the studies since Heinrich's time. Taking Buncefield as an example, after a four-month trial at St Albans Crown Court, five companies were found guilty of various offences and ordered to pay a total of £9.5 million in fines and costs over and above the initial incident costs.

The other aspects of potential loss depend on many factors related to the original incident. How these other 'uninsured losses' might be dealt with may depend on the availability and cost of cover, as well as the organisation's perception of the risks of such losses. For the present, however, it is enough to accept that major industrial incidents have important consequences in terms of death, ill health, and environmental and economic impact beyond the initial incident.

2.5 Risk perception

In their everyday lives, people become aware of a variety of events, ranging from the local but relatively small-scale (such as a serious road traffic accident in a town's main street) to the remote but large-scale (Figure 10). A local incident is of great and direct concern to a given group of individuals. On the other hand, major incidents (regardless of how geographically remote they are) receive the greatest publicity and raise more general concerns about the risks of technology. In fact, perceptions of risk are not based solely on quantitative measures but also include subjective value judgements. An individual's perception is influenced by the degree to which the risk is imposed upon them rather than accepted voluntarily, their knowledge of the problem, their trust in the 'management' of the risk, and so on. The net result is that reaching a consensus view over what constitutes a risk can be difficult.

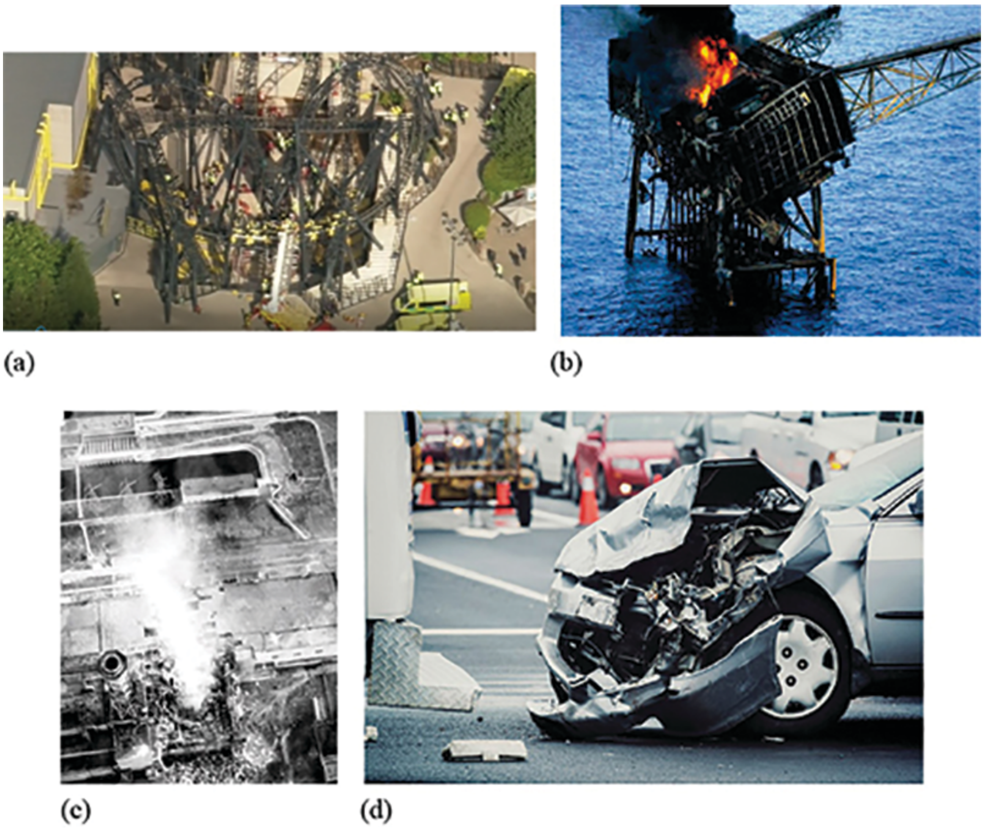


Figure 10 Local and large-scale incidents: (a) rollercoaster crash at Alton Towers theme park (2015); (b) fire on the *Piper Alpha* oil production platform (1988); (c) nuclear reactor explosion at Chernobyl (1986); (d) road traffic accident

The issues that affect people's perception of risk can be summarised broadly as follows:

- Voluntary risks are accepted more readily than imposed risks.
- Risks under individual control are accepted more readily than those under corporate or government control.
- Risks that seem fair are accepted more readily than those that seem unfair.
- Risk information from untrustworthy sources is less readily believed than that from trustworthy sources (people who trust regulators and their government in general are more likely to accept the regulator's assessment of a risk).

It is important to remember that public perception of risk and scientific evaluation may well not agree. Research consistently shows that people's perception of risk is a function not just of the possible harm, but also of the attributes of the hazards and benefits associated with the thing in question. So how can you decide what risk is reasonable and on what evidence something is safe?

ALARP

One concept of risk tolerability requires that measures be taken to reduce the likelihood of hazards and to limit their consequences until further reduction of risks cannot be justified. Putting it another way, the risks to individuals and to society should be as low as reasonably practicable (ALARP). When this approach was first developed in the area of pollution control in the UK in the 1860s, process operators had to use the best practicable means (BPM) to eliminate or control pollution. This concept was later adopted by the European Union as the principle of BATNEEC, or best available techniques not entailing excessive cost.

The principle of ALARP is illustrated in Figure 11, which indicates two regions of unacceptable and acceptable risk separated by a region where the risk is acceptable only in exceptional circumstances. The terms used (1 in 1000, etc.) are explained later in the course.

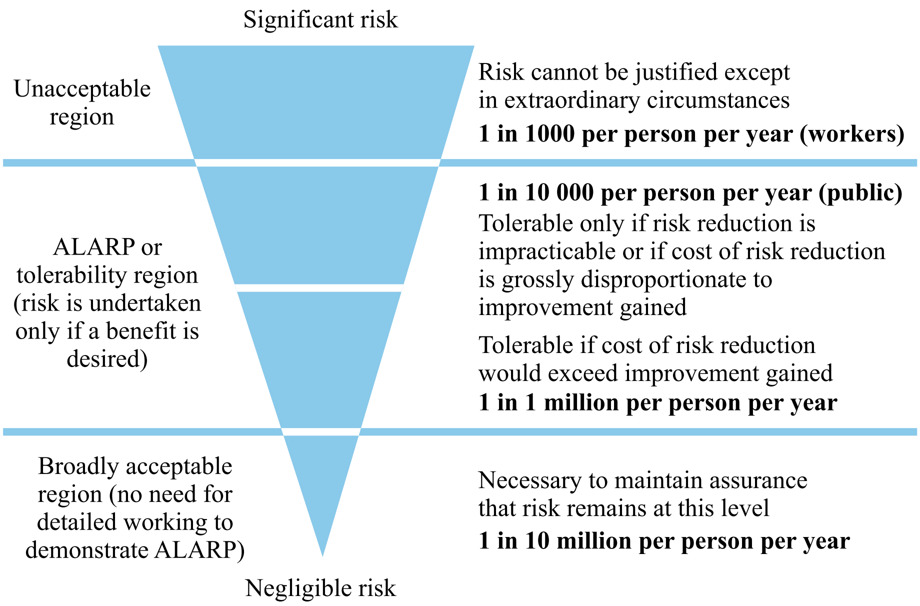


Figure 11 The ALARP concept

The core of ALARP is 'reasonably practicable'; this involves weighing a risk against the trouble, time and money needed to control it. In some cases 'good practice' can be referred to, but in other situations deciding whether a risk is ALARP can be challenging, as it requires a degree of judgement as well as an economic evaluation.

Communicating risk

In general, risk comparisons can help people to comprehend probabilities or magnitudes. Most people find it hard to relate low-risk probabilities or proportions, such as 'one in a million', to their everyday experience. It can help to communicate risk by making quantitative comparisons between familiar and less familiar risks. For example, the risk of a UK nuclear power station undergoing a radiation release that kills 100 people is similar to the risk of dying as a result of cycling 10 miles on UK roads. An even better approach can be to use analogies: one in a million is approximately equivalent to 30 seconds in a year, 1 drop of liquid in 70 litres, or 1 centimetre in 6.4 miles/10.3 kilometres. Another solution might be to express risk in terms of the number of persons who might be affected per year or per hypothetical 70-year lifetime.

Even more difficult to communicate is the fact that a one-in-a-million risk estimate is not an estimate of actual risk, but an upper bound on the likelihood of a risk. That is, the actual risk is likely to be much lower, and it could be zero, but it is quite unlikely to be higher.

In communicating risk, it is important to ensure that the audience appreciates the logarithmic nature of risks expressed in terms of powers of 10. This is shown in Figure 12. Starting with a baseline risk of 1 in 1000 (or 1×10^{-3}), this is shown in the first column and is allocated 100%. Reducing the risk by a single order of magnitude to 1 in 10 000 (1×10^{-4}), gives a reduction in risk of 90% represented by the second column in Figure 12 which stands at 10%. A second reduction of one order of magnitude from 1 in 10 000 (1×10^{-4}) to 1 in 100 000 (1×10^{-5}), gives a reduction that is one-tenth of the first reduction – thus reducing the *original* risk to 100 - 90 - 9 = 1 as shown in the third column of Figure 12. A further reduction results in a (probably) insignificant reduction in the overall risk.

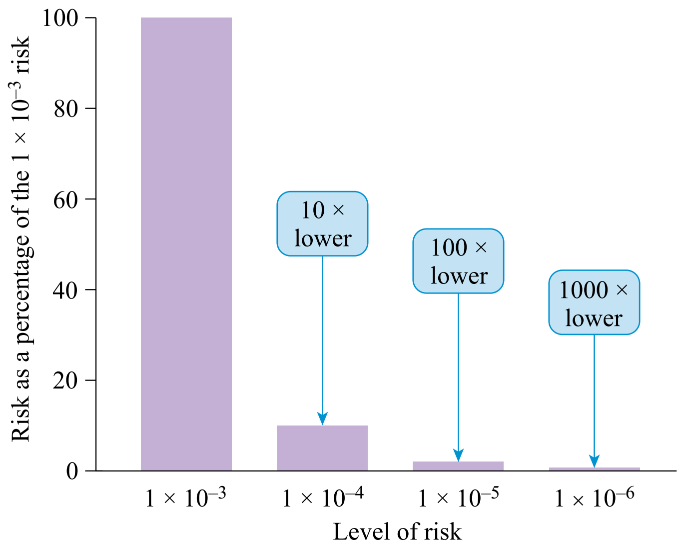


Figure 12 Scales of risk reduction

The scientific community has a very important role to play in measuring risks and in presenting this information in as clear a manner as possible, with appropriate cautions about uncertainty. It is then a responsibility of society as a whole, with no particular group having a more privileged position by right, to determine what is tolerable and acceptable based on social, political, cultural and even economic considerations. Clearly, there are areas where the risk is so high as to be manifestly unacceptable, and others where it is so low as to be negligible. Of course, most debate is in the grey area in between. Legislation, attitude and hence behavioural change are important channels for reducing risk. Many hazards cannot be abolished in the sense that they are completely eliminated. Therefore, reducing risk is often a question of reducing exposure.

In the UK, the logic for reducing occupational risks to health is to achieve a situation whereby exposure is controlled to a level to which nearly all the population could be exposed day after day, without adverse effects on health. An important test of any engineering (or other) system is whether the community affected will regard a risk as being acceptable to them. Only under these conditions can it be said that something with low risk levels is also safe.

Example 2 Assessing the acceptability of risk

In 2015, the NHS estimated that around 100 000 people die as a result of smoking each year in the UK (NHS, 2015). According to the UK's Office for National Statistics, in 2014 19% of the British population (around 12 million people) were smokers (ONS, 2016). Is this risk acceptable to smokers, and would a similar risk from travelling on the railways be acceptable?

Solution

Many smokers would say that this risk is unacceptable and that they are trying to give up smoking, but some smokers do consider the risk to be acceptable and have no intention of giving up.

There are about 2.9 million rail season ticket holders in the UK. Applying the same rate of fatalities (100 000 per 12 million or 1 in 120) this would equate to over 24 000 deaths on the railways each year. Clearly this would be completely unacceptable to rail travellers, the population as a whole, the rail industry, politicians and the international community.

The difference is that the risk from smoking is, at least to some extent, voluntary, while the risk from rail travel is completely outside the passengers' control.

Activity 2 Acceptability of risk

Allow approximately 15 minutes.

Decide whether each of the following factors would be likely to make a risk more or less acceptable to people.

- The effect is immediate rather than long term.
- There are many alternative ways of achieving the intended aim.
- The risk is unknown or not known with certainty.
- Exposure is an essential part of life (rather than a 'luxury').
- The risk is unexpected.
- The hazard is a common one.
- Only sensitive people are affected by the risk.
- The consequences of the risk are reversible.

Answer

Greater acceptability:

- The effect is immediate rather than long term.
- Exposure is an essential part of life (rather than a 'luxury').
- The hazard is a common one.
- The consequences of the risk are reversible.

Lower acceptability:

- There are many alternative ways of achieving the intended aim.
- The risk is unknown or not known with certainty.
- The risk is unexpected.
- Only sensitive people are affected by the risk.

The way people treat risks depends on their perception of how those risks relate to them and things they value. This evaluation might relate not only to physical harm, but also to social and political beliefs and degree of trust in the information provided. Members of the public and experts often disagree. Engineers are engaged in this process occupationally, or perhaps in relation to a project they are involved with or any associated evaluation of that activity and appropriate communication. However, it is important to remember that there is no such thing as absolute safety!

So far you have looked at definitions and perception related to risk. To approach the estimation of risk in a more scientific and calculated manner, it is now worth studying the statistical aspects of risk as described by probability.

3 Risk measurement and risk management

Probability is a way of expressing, in mathematical terms, the likelihood that a particular event will happen. Risk assessments are generally concerned with the probability of something bad happening (the risk that a component will fail, for example), but probability can equally well apply to positive events or outcomes.

Before looking at the rest of this material, you need to take note of two important warnings. First, the fact that a component in a particular machine has lasted for 15 000 hours of use doesn't mean that the equivalent component in a similar machine won't fail after only 5000 hours of use. Or, in the words of the financial services industry:

> Past performance is no indication of future performance.

Second, it is equally true that the fact that a component fails long before the end of its expected life doesn't mean that a replacement component won't also fail prematurely. Or, in the words of Ecclesiastes in the Christian and Jewish scriptures:

> What has happened before will happen again.

In other words, it is important to be aware of the worst-case scenario: a component failure indicates the possibility of other failures in the future, yet a lack of failure does not mean similar components will not fail.

3.1 Expressing probability

Probability can be expressed mathematically in a number of ways. The following all show an equal probability:

- as a proportion (e.g. 1 in 8)
- as a decimal number between 0 and 1 (e.g. 0.125)
- as a fraction (e.g. one divided by eight)
- as a percentage (e.g. 12.5%).

An impossible event has a probability of 0, while an event that is certain to happen has a probability of 1. For instance, the probability of dying (eventually) is 1.0 (or 100%) for everyone.

Figure 12 illustrated scales of risk reduction. This is revisited in Table.3, where probabilities (or risks) are expressed in the different standard forms, including scientific notation as a useful reminder.

Table 4 Expressions of risk

Proportion	Decimal	Fraction	Percentage	Scientific notation
1 in 2	0.5		50%	5×10^{-1}
1 in 5	0.2		20%	2×10^{-1}
1 in 10	0.1		10%	1×10^{-1}
1 in 100	0.01		1%	1×10^{-2}
1 in 1000	0.001		0.1%	1×10^{-3}
1 in 10 000	0.0001		0.01%	1×10^{-4}
1 in 100 000	0.000 01		0.001%	1×10^{-5}
1 in 1 000 000	0.000 001		0.0001%	1×10^{-6}
1 in 10 000 000	0.000 000 1		0.000 01%	1×10^{-7}

Professional risk analysts often quote various figures showing the risks associated with everyday activities in comparison to risks in which they have an interest. Some examples from one published table of risks are included in Table 4. However, remember that all such tables and figures are based on historical information and cannot always be relied upon for future predictions.

Table 5 Levels of fatal risk in the UK (approximate averages), given as the chance of each event occurring per year

Risk of dying in a year	Activity
1 in 100	Five hours of solo rock climbing every weekend
1 in 1000	Working in a high-risk group within the more hazardous industries
1 in 10 000	General travelling by road or on foot
1 in 100 000	Working in the very safest parts of industry
1 in 1 000 000	Fire caused by a cooking appliance at home
1 in 10 000 000	Being hit by lightning

(Source: HSE, 1992)

One obvious reason why future risks cannot be predicted easily is that all professions are constantly working to improve safety. Therefore the two industrial death probabilities quoted above will now be lower. The number of car accidents, for example, has diminished rapidly in recent decades in the UK, and injury rates have also decreased with the mandatory use of safety belts and the installation of airbags, impact-protected body shells and better tyres. Improvements to road design and layouts have also played a part here. These improvements do not mean that we should be complacent; there are almost always additional ways in which death and injury rates can be reduced yet further.

Activity 3 Risk in scientific notation

Allow approximately 20 minutes.

Complete the following table to express the risks shown in terms of a decimal, a fraction and scientific notation.

Table 6 Risks shown in decimal, fraction and scientific notation

Decimal	Fraction	Scientific notation
0.05		
		1.6×10^{-2}

Answer

Table 7 Answers for risks shown in decimal, fraction and scientific notation

Decimal	Fraction	Scientific notation
0.05		5×10^{-2}
0.016	or	1.6×10^{-2}
0.006 67		6.67×10^{-3}
0.000 000 333		3.33×10^{-7}

The important thing is to understand that although there might be a ‘1 in 10 million’ risk of death by lightning, or a ‘1 in 100’ risk of death from five hours of solo rock climbing every weekend, these figures may not show an accurate measure of risk from that activity. There are many other factors that might change these estimates – for instance, an individual might be a very safety-conscious rock climber or might make a habit of standing under trees during lightning storms.

Example 3 Reading a logarithmic scale

One representation that often arouses public interest is the probability of dying from different causes in a year for an ‘average person’. Figure 13 compares the risks associated with a number of differing possibilities.

Reading these probabilities is a little challenging because of the logarithmic scale. The trick is to remember that this scale behaves normally if you calibrate it with respect to the exponent. So the first step is to read the value off the scale as if it were just calibrated in terms of the power of ten. This is demonstrated in Example 3.

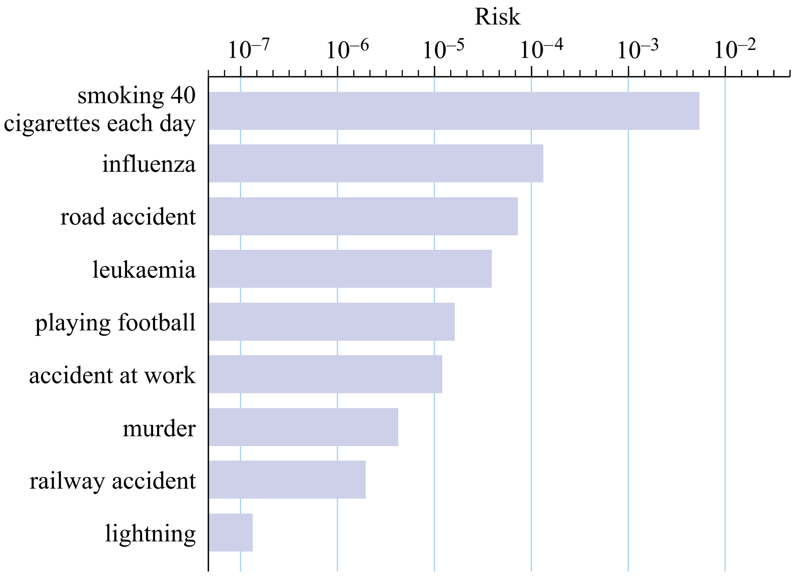


Figure 13 The probability of dying from particular causes for an average British citizen in one year

Use Figure 13 to estimate the probability of dying from influenza.

Solution

The bar representing death from influenza lies between 1×10^{-4} and 1×10^{-3}, with an exponent of about −3.9. So you need to find the value of $10^{-3.9}$.

Using a calculator to convert this to a number (in many calculators this is done by typing 3.9, changing the sign, and then pressing the button marked '10^x', but other calculators may use a different sequence) gives $1.258... \times 10^{-4}$.

It's difficult to estimate the uncertainty in this figure (you could enter estimates of the upper and lower limits and calculate the values), but it's unlikely to be much better than 3 significant figures.

So the risk of dying from influenza is approximately 1.26×10^{-4}.

Activity 4 Estimating probability

Allow approximately 20 minutes.

Use Figure 13 to estimate the probability of dying from

(a) smoking 40 cigarettes each day
(b) playing football.

Roughly how much more likely is it that a heavy smoker will die in a given year than a non-smoking football player?

Answer

From Figure 13:

(a) The risk of death from smoking 40 cigarettes each day is approximately $1 \times 10^{-2.3} = 5.01 \times 10^{-3}$ (to 3 significant figures – s.f.).
(b) The risk of death from playing football is approximately $1 \times 10^{-4.8} = 1.58 \times 10^{-5}$ (to 3 s.f.).

The ratio of the two risks is given by

So smoking is approximately 316 times more dangerous than playing football. This ignores the health and social benefits of playing football (due to the exercise and interactions with other people), which will also offset the risk. Note that the result is extremely sensitive to small changes in the values you selected for the exponents so your answers may well be different from these.

Notice that two potential causes that often excite media interest and public comment – murder and railway accidents – are both relatively unlikely. By comparison, smoking and influenza are relatively common causes of death. It is such perceptions that make the identification of acceptable risk so difficult.

An estimate of the probability of a catastrophic accident in a nuclear power station has been put at once every 10 000 years – catastrophic being something like the incident at the Chernobyl nuclear reactor in 1986, when there was a large release of radioactive material. (Note, though, that the safety of nuclear reactors has improved considerably since the Chernobyl reactor was designed. All current indications are that the Fukushima nuclear incident following the tsunami off the coast of Japan in 2011 was far less severe than Chernobyl.) This probability figure of 1 in 10 000 years (or 0.0001 per year) sounds reassuring, but remember that it is for a single reactor. In mid-2016, there were about 450 civil nuclear reactors operating across the world.

Regulators apply what is known as the *de minimis* concept, which assumes that there is a level of risk that is so low it can be reasonably ignored. Its name is derived from the common law maxim *de minimis non curat lex*: ‘the law does not concern itself with trifles’. A one-in-a-million level of increased risk over a lifetime is often used as a reasonable criterion for separating high-risk problems (which warrant attention) from negligible-risk problems (which do not). Of course, you can try to quantify such risks, but still your perception of whether that is acceptable might differ from someone else’s.

3.2 Calculating probability

Coins and dice provide good examples for considering probability, as there is a limited but well-defined number of possible outcomes in each case (Figure 14).

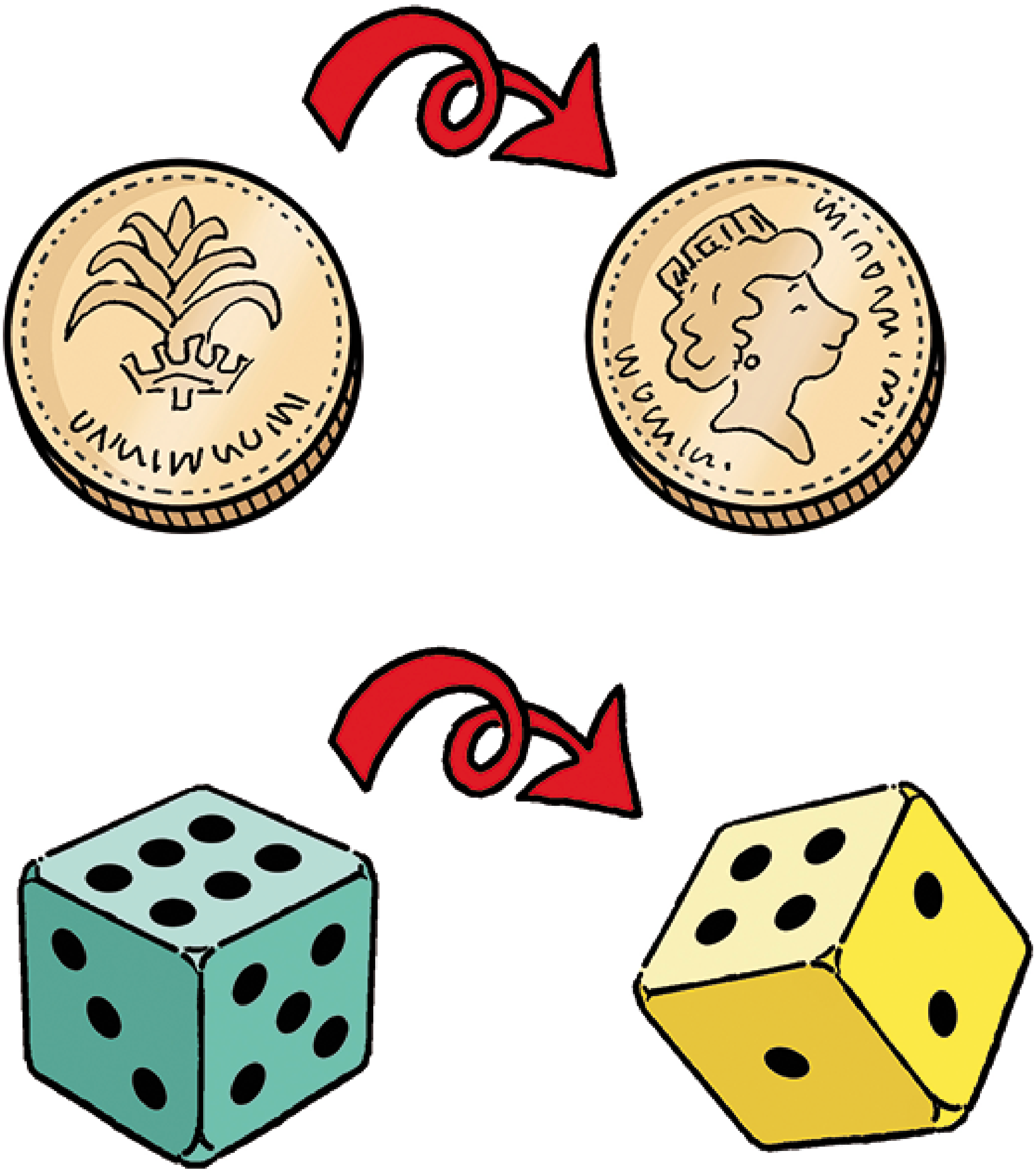


Figure 14 Tossing coins and rolling dice

Finding the probability of a particular outcome

To calculate the probability of a particular outcome from an event:

1. Count the total number of possible outcomes.
2. Count the number of times the outcome of interest occurs.
3. Express the two numbers as a proportion, a fraction, a decimal or a percentage in its simplest form.

For example, if a person tosses a coin, there are two possible outcomes: ‘heads’ and ‘tails’. If the coin is ‘fair’ and has not been tampered with, these outcomes are equally likely. So the probability that a single toss gives ‘heads’ can be described as 1 in 2, , 0.5 or 50%.

In standard mathematical notation, the probability of a particular event happening is expressed as

where means that the value of lies in the range 0 to 1. So the probability of tossing a coin that lands showing ‘tails’ would be written as .

Example 4 Probability of scoring an even number

What is the probability of scoring an even number by rolling a die?

Solution

There are six possible outcomes from rolling a die, and three of them will give an even number (2, 4 and 6).

So the probability is 3 out of 6, which can be simplified to 1 out of 2.

This can be expressed as 1 in 2, , 0.5 or 50%.

Activity 5 Calculating probability

Allow approximately 20 minutes.

Calculate each of the following. Express your answers as a proportion, a fraction, a decimal and a percentage (to 2 s.f. where appropriate).

(a) The probability of scoring a 2 when rolling a die once.

(b) The probability of scoring higher than 2 when rolling a die once.

Answer

(a) There are six possible outcomes, and only one of these results in a 2. This means that the probability of rolling a 2 is 1 in 6, , 0.17 or 17%. (The probability of any one of the other numbers occurring is, of course, also 1 in 6.)

(b) The total number of outcomes is six, and four of these meet the condition of scoring higher than 2, so the probability is 4 out of 6 or 2 out of 3. This can be expressed as 2 in 3, two divided by three , 0.67 or 67%.

Combining probabilities

In risk assessments, it is rare to be concerned with the probability that a single event will happen or a single component will fail. As you saw in the Deepwater Horizon case study, several failures led to the incident. Therefore it is often necessary to look at the probability of combined events.

Combining independent probabilities

For any event that has probability , the probability that does *not* occur is written as . If the probability is expressed as a fraction or a decimal then . This can be represented using a 'probability space diagram', as shown in Figure 15(a). The circle represents the probability that occurs, while the space outside the circle represents the probability that it does not occur.

If two events are independent (the outcome of one does not influence the outcome of the other), the probability of both events occurring is given by

For more than two events, the overall probability is given by multiplying the probabilities of each of the events expressed as a fraction or a decimal.

Using standard probability notation,

where the symbol means AND. This expression can be read as 'the probability of and occurring is equal to the probability of occurring multiplied by the probability of occurring'. Again, this can be represented using a probability space diagram, as shown in Figure 15(b). Here there is one circle representing the probability of occurring and another representing the probability of occurring. The intersection of the two circles (shaded darker blue) represents .

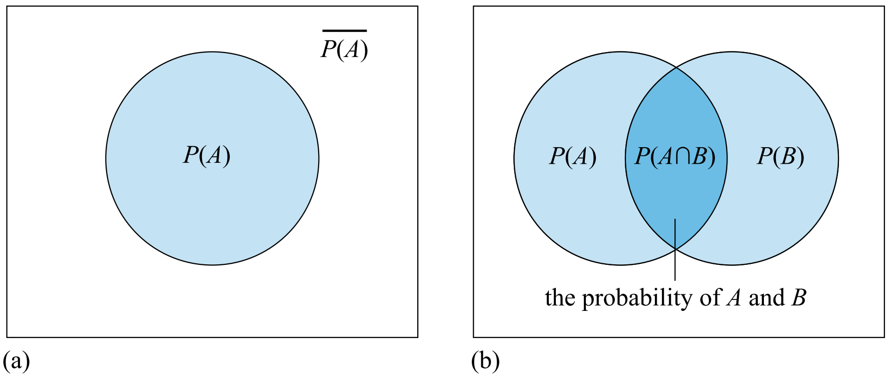


Figure 15 Probability space diagram for (a) ; (b)

Note that if two probabilities are dependent (the outcome of one *does* influence the outcome of the other), a different method has to be used to combine them, which is beyond the scope of this course. For example, suppose you draw two cards from a single pack of 52 playing cards – what is the probability that they will both be queens? The probability of the first card you draw being a queen is straightforward: there are four queens in a pack of 52 cards, so the probability is 4 in 52, or 1 in 13. However, when you draw the second card, the probability of drawing a queen will either be 3 in 51 (if the first card was a queen) or 4 in 51 (if the first card was not a queen). So the first event is affecting the outcome of the second – the events are dependent.

Example 5 Combining two independent probabilities

When tossing a coin twice, what is the probability of getting heads both times?

Solution

Using the formula, the probability of each toss scoring a head is 1 in 2, 0.5 or , and the probability of scoring two heads is

0.5 × 0.5 = 0.25,

or

This can be checked by working from first principles. Tossing two coins (or one coin twice) gives the following four possible outcomes:

- heads, heads
- tails, tails
- heads, tails
- tails, heads.

From this, it can be seen that the probability of getting two heads is 1 in 4, , 0.25 or 25%.

Activity 6 Combining probability

Allow approximately 20 minutes.

Calculate the probability of the following:

(a) scoring two 6s by rolling two dice

(b) scoring six 6s by rolling six dice.

Express your answers as both a fraction and a decimal (to 2 s.f.).

Answer

(a) The probability of scoring a 6 with one roll of a die is . For two dice, applying the formula gives an overall probability of

(b) Similarly, for scoring six 6s, the overall probability is

Note that if you were to carry out these calculations using the rounded decimal value of 0.17 for the probability of a 6 (as calculated in Activity 5), you would have got the values 0.029 and 0.000 024, respectively. As this demonstrates, using rounded figures in calculations can have a significant effect.

Probability of failure

The probability of a component failing is calculated in a similar way. However, it can be hard to assess what this probability means, in practical terms. For instance, suppose that an oil storage tank is fitted with a level-detecting device that shuts off the valve that lets oil into the tank when it is full. An assessment of the device suggests that there is a 1 in 10 000 probability that it will fail each time the tank is filled. If the tank is filled every day, how often is failure likely?

This isn't a question you can answer, since the device might never fail. What you can say is that after a given interval, there is a particular probability of failure. For instance, you could assess the probability of a failure within 25 years. It will be assumed here that regular maintenance checks ensure that the device does not deteriorate significantly, so that the probability of failure stays constant over time.

To calculate this, consider what the probability would be if the tank were filled twice. That would give three possible outcomes: the level detector doesn't fail, it fails once or it fails twice. Since for any event , , the calculation that the level detector doesn't fail on any single occasion is 1 minus the probability that it does fail – that is,

Now you have the probability of no failure for one occasion. How about two occasions? That is given by the product of the two individual probabilities, which is 0.9999^2 in this case. Working this way, you avoid any complications from multiple failures entering the calculation.

So how about the probability over 25 years? In 25 years, the number of times the tank will be filled is the number of days, 25 × 365 = 9125 (ignoring leap years). It is acceptable to round this to 9000 without having to worry about accuracy, but you cannot round the 0.9999 or your answer will always be 1. So you need to calculate 0.9999^{9000} to estimate the probability of no failures:

This is the probability of no failures, so the probability that there is a failure is given by 1 − 0.41 = 0.59. So there is a 59% probability of failure during 25 years of operation.

If the Health and Safety regulators decided that failure of the device could trigger an event similar to that at Buncefield, they might require the operators to fit a second device (the same as the first) to the tank. For the tank to overfill now requires both devices to fail at the same time.

Activity 7 Probability of failure

Allow approximately 15 minutes.

With two safety devices installed, calculate the probability that both devices fail at the same time within 25 years.

Answer

You need to go back to the original problem and look at the probability of failure for one safety device, which was 1 in 10 000 or 10−4. This means the probability of two such failures simultaneously is 10−4 × $10^{-4} = 10^{-8}$

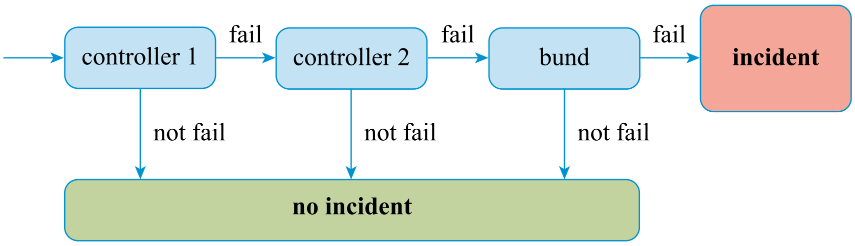
Taking $1 - 10^{-8}$ = 0.999 999 99 and raising this to the power 9000 gives 0.9999 (to 4 s. f.). So you now have a probability of 1 − 0.9999 = 0.0001, or 1 in 10 000, over 25 years.

The calculation you carried out in Activity 7 assumes that the two devices would fail independently (through some random fault, perhaps). However, if the failure was due to (say) a breakdown in the power supply to the tank control system, or because the devices had both been over-insulated and overheated, or even because both devices came from a faulty batch, then adding the second device would have little if any effect in reducing the probability of an incident.

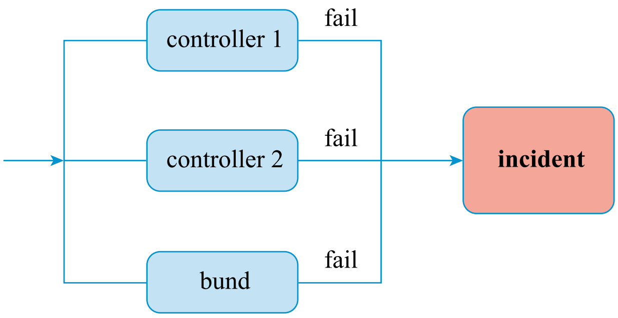
Even if you can assume independent failure of the two devices, this only implies a reduced *probability* of failure. In reality, failure could take much longer or, conversely, could happen the day after commissioning the installation. This is why other safety precautions would be taken, including the provision of some kind of containment system – such as an impermeable retaining wall or bund surrounding the tank – that would retain any spillage. In addition, the electrical equipment in the area would be certified as safe for use in potentially explosive atmospheres. This concept of multiple redundancies is a key way of achieving safe operation in the engineering industries.

Series and parallel

So far, these calculations have looked at the probability of several events all happening. For instance, in the situation described above, a leak would occur only if both detectors failed *and* the bund failed. In effect, the control systems are working in series (Figure 16a). However, in other instances, an undesired outcome might take place if any one of a number of events occurred. In such a case, the control systems would be working in parallel (Figure 16b). For example, a house could be burgled if either the door was left unlocked or a ground-floor window was left open.



(a) Series protection – incident occurs only if all three fail



(b) Parallel protection – incident occurs if only one fails

Figure 16 Controls in series and parallel

Probability of at least one event occurring

The method for calculating the probability of one or more of a number of events occurring is to calculate the probability of *none* of the events occurring and then subtract this answer from 1.

For the special case of either or both of two events occurring (*A* or *B*), the probability is given by

In probability notation, this is expressed as

where the symbol denotes OR.

Note that the probability of both events occurring has to be deducted to avoid double counting. When the probability of occurring is calculated, those occasions when and both occur are also included. Similarly, when the probability of occurring is calculated, the probability of both and occurring is included. Deducting one of these eliminates this double counting, as shown in the probability space diagram in Figure 17.

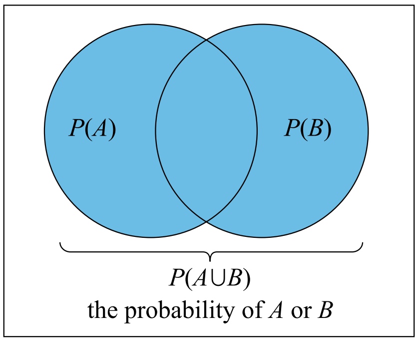


Figure 17 Probability space diagram for

Example 6 Calculating the probability of at least one event occurring

What is the probability of each of the following?

(a) Scoring at least one 2 by rolling two dice
(b) Scoring at least one 2 by rolling three dice

Solution

The probability of scoring any given number when rolling one die is 1 in 6.

(a) The probability of scoring two of any given number by rolling two dice is given by

Using the formula, a probability of at least one 2 is given by

(b) For the second case, with three dice, it is necessary to look at the probability of each event not occurring. This is 5 in 6 for each die. So the probability of not scoring any 2s is

So the probability of scoring at least one 2 is

Activity 8 Probabilities

Allow approximately 25 minutes.

If a person tosses a coin once and rolls a die once, what is the probability that they get one head and/or one 6? Express your answer as a percentage.

Answer

The probabilities of scoring a head and rolling a six are 1 in 2 and 1 in 6, respectively, so the probability of both occurring is

Applying the formula, the probability of at least one of the two events occurring is

In other words, at least one of these events would be expected to occur on just over half the occasions. As a percentage, this is a probability of 58%.

A company manufactures bolts. The probability of a bolt having a defective thread is 2×10^{-3} (2 in 1000). The probability of a defect in the head is 2×10^{-5} (2 in 100 000).

Calculate:

(a) the probability of a bolt having both a defective head and a defective thread

(b) the probability of a bolt having a defective head or a defective thread (remember that when discussing probability, the term 'or' means either or both)

(c) the probability that a bolt has no defects.

Answer

(a) The probability that a bolt has both defects is the product of the two probabilities:$2 \times 10^{-5} \times 2 \times 10^{-3} = 4 \times 10^{-8}$

This is very small indeed.

(b) To find the probability of a bolt having either (or both) of the defects, you need to use the formula for the probability of at least one event occurring. This is the sum of the two probabilities, minus the probability of both:

This is approximately the same as the probability of a thread defect, which is the dominant defect, so the result shouldn't surprise you.

(c) In Part (b) you calculated the probability of a defect, cap p of defect . So the probability of no defects is given by

3.3 Probability in everyday life

Here are some interesting probability examples. You may like to try working out the answers yourself to enhance your understanding, or you can use them to entertain your family and friends!

Activity 9

Allow approximately 25 minutes.

Winning the UK National Lottery

The UK National Lottery operates a number of 'games' each week. In the main game, participants choose six different numbers from 1 to 59. When the draw is made, six numbered balls are selected at random from a pool of 59 balls (ignoring the seventh 'Bonus Ball'). If a participant's selection of numbers matches the six numbers drawn (although the order of the numbers may be different), they win the jackpot, which can be several million pounds. Smaller prizes can be won by matching two or more numbers.

What is the probability of any single entry winning the jackpot?

Answer

The first time a ball is selected, there are 59 to choose from and 6 of these will match the numbers chosen by the participant, so the probability of getting a match is

When the second ball is drawn, there are 58 balls remaining and five of those will match one of the participant's remaining numbers. This means that the probability of getting a match with the second ball is

So overall, the probability of matching two numbers is

which is approximately . If the calculation is continued in this way, the chance of matching all six balls is found to be given by

So there is a probability of about 1 in 45 million that any one National Lottery ticket will win the jackpot. Of course, millions of tickets are sold each week, so it is not suprising that, in most weeks, one or more people win the jackpot.

Monkeys writing Shakespeare

There is an old saying that an infinite number of monkeys sitting in front of (an infinite number of) typewriters would eventually type all the great works of literature, including all of Shakespeare's plays.

If we update this saying and take an infinite number of monkeys that enjoy pressing keys and give them access to monkey-friendly keyboards that contains just 26 keys (one for each letter of the alphabet) what is the probability of one monkey typing the word 'MACBETH' in seven keystrokes?

Answer

Unlike drawing the lottery numbers, the order of the monkey's selection does matter and the same key can be pressed more than once. Taking the first letter, there is a 1 in 26 chance that the monkey hits the 'M' key. Similarly, there is a 1 in 26 chance that the second key is an 'A' so the chance of typing 'MA' in two keystrokes is given by

Continuing this line of reasoning, the chance of writing 'MACBETH' in seven keystrokes is given by

So there is a probability of approximately 1 in 8 million that a monkey would write 'MACBETH' by hitting a typewriter keyboard seven times. Of course, this does not mean that it would not happen, just that it would be highly improbable. If the monkey were to type the meaningless sequence 'KWCPETE', the probability of that coming up would also have been 1 in 8 billion.

Two people sharing a birthday

If you are with a group of your friends, how big would the group have to be for there to be a reasonable (say 50%) probability that at least two of them were born on the same day of the year, but not necessarily in the same year?

When asked this, most people would vastly overestimate the size of the group, but if you think about this carefully you will come up with a result that may surprise you.

Answer

The first person in your group has a birthday on any one of 365 days (if we ignore leap years). The probability that the second person shares that birthday is or, in other words, the probability that the second person's birthday is on a different day is .

Now bring in a third person. The probability that they share a birthday with either of the first two people is , so the probability that they have a different birthday from either of the first two people is . Therefore the probability that the three people all have different birthdays is given by

Therefore, there is only a 1 − 0.997 = 0.003 (or 3 in 1000) chance that this is not the case and that at least two of the three people share the same birthday. This is perhaps not surprising.

Continuing down this path, it can be shown that by the time there are 23 people, the probability that they all have different birthdays is approximately 0.49, because

So the probability that this is not the case and at least two people share a birthday is 1 − 0.493 = 0.507. This means that there is a slightly better than 50% chance that at least two people share the same birthday.

If the size of the group continues to increase, by the time reaches 32 people there is a 75% chance that at least two people will share a birthday, because

so the probability that this is not the case and at least two people share a birthday is 1 − 0.247 = 0.753 or 75%.

3.4 Risk management

Earlier, this course considered what is meant by risk. To recap, assessing risk involves an evaluation of the severity of harm and the likelihood of the risk occurring. The process of evaluating alternative actions and selecting the most appropriate is often called risk management.

Risk management is a practice with processes, methods and tools for managing risks in a project, activity or event. It provides a disciplined environment for decision making to:

- assess continuously what could go wrong (identify risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks.

At this point it is important to note that while the concept of risk, and the idea of risk management, are used in many diverse fields, their meanings differ in different disciplines. When you say you are going to take a risk, you probably mean that you are prepared to take a chance of an adverse consequence in the expectation of a benefit. Implicit in that interpretation is that risk reflects both a likelihood of 'harm' and a measure of the consequence. In everyday life, however, it is consequence that may be of greatest concern, rather than likelihood. Commonly people associate risk with some aspect of 'loss', which could include a health or environmental impact, but could also involve financial loss, societal loss, loss of equipment or operating capacity, product loss or staff loss. Risk management is the decision-making process involving consideration of political, social, economic and engineering information alongside risk-related information that could be applied to many different situations.

Risk management is proactive – that is, you should have identified your potential hazards in any given situation, evaluated whether they are likely to occur and so have an idea of your risk. If you are evaluating health and safety or environmental impacts, the next stage is to manage that risk to 'as low as reasonably practicable' or ALARP, as discussed earlier. This management might include a number of measures to reduce risk, a demonstration that an activity or process is 'safe', or an evaluation of whether it is an acceptable risk. However, whether managing the risk of an adverse health impact, a financial risk or perhaps a product risk, it is important to know that any risk is not merely managed 'once' – generally, risk management is an ongoing process that is regularly reviewed, and revised either over time or when given new or changed information. It is also important to take on board a number of views when managing risk, rather than relying on a single point of information. This may mean consulting with a number of stakeholders.

A stakeholder is anyone who has a 'stake' or interest in a risk management situation. Stakeholders typically include groups that are affected or potentially affected by the risk, the risk managers, and groups that will be affected by any efforts to manage the source of the risk. Who the stakeholders are depends entirely on the situation. The objectives, interests and responsibilities of stakeholders may be varied and contradictory. Questions that can help to identify potential stakeholders include the following.

- Who might be affected by the risk management decision? (Bear in mind that they may not know they are affected.)
- Who has information and expertise that might be helpful?
- Who has been involved in similar risk situations before?
- Who has expressed interest in being involved in similar decisions before?
- Who might reasonably be upset if not included?

Different stakeholders may have different perceptions and concerns. This section has considered hazard, risk and risk perception – it is important to recognise that various opinions will have an impact on how a risk is perceived and how it is managed.

Example 7 Identifying stakeholders

Make a list of stakeholders who might be relevant to an organisation managing a risk that involves the environment around a chemical processing plant facility located 20 km from an urban area.

Solution

Stakeholders could include:

- people who live and/or work in the urban area
- people who live and/or work close to the plant
- the local authorities (district and county level)
- local emergency services
- employees of the company
- customers and suppliers of raw materials and other resources
- community groups
- representatives of different cultural, economic or ethnic groups
- public health agencies
- businesses in the area
- trade unions representing employee groups
- environmental pressure groups
- consumer rights organisations
- religious groups
- educational and research institutions
- regulatory agencies
- trade associations
- those with a financial interest – bankers, investors, insurers, etc. and possibly the national government or assembly.

Activity 10 Considering stakeholders

Allow approximately 15 minutes.

A small company, Automotive Widgets Ltd, makes specialist parts for cars that are shipped out to a major car manufacturer. The company is sited on a local industrial estate, surrounded by other small companies and nearby housing. Around 240 local people work for Automotive Widgets, and local suppliers provide the company with raw materials, components for its widgets and office supplies.

Consider who the stakeholders of Automotive Widgets might be. Include at least four internal and four external stakeholders, aiming for a total of at least ten.

Answer

Internal stakeholders would include:

- the owners
- shareholders
- staff
- contractors.

External stakeholders could be:

- banks/financiers
- insurers
- customers
- regulators
- local community groups
- other companies based on the industrial estate

- utility companies
- material and component suppliers
- office equipment suppliers.

All the individual groups of stakeholders in the example and activity above will have many ways of evaluating the same risk, and may arrive at quite different opinions. Of course, they may also be different groups arriving at the same conclusions. The following factors will usually influence the perceptions of different stakeholders.

- How imminently might the effects be experienced? In other words, are the effects likely to appear in the near future, later on in life, or will they have an impact on future generations?
- How urgent is the need for action? For example, a road tanker carrying flammable solvent that overturns in a residential neighbourhood requires a risk assessment with actions requiring immediate attention; a municipal waste incinerator operating normally in the same area can be assessed bearing longer-term impacts in mind.
- Do different stakeholders have different perceptions and concerns? For example, parents of children at risk from exposure to an industrial pollutant may feel quite differently about a hazard than workers whose income depends on the industry causing the problem. When these are the same people – that is, the parents are also the workers – perceptions of the hazard can be quite complex.

Experience increasingly shows that risk management decisions made in collaboration with stakeholders are more effective and more durable than those that exclude stakeholders from the process. Stakeholders can make a unique contribution to the decision by providing important information, knowledge, expertise and insights for developing workable solutions. They are more likely to accept and implement a risk management decision in which they have some participation. Communicating clear and consistent information to all internal and external stakeholders is essential to building trust.

You can therefore see how risk management involves a multitude of stakeholders. You have also previously seen how human error can have a significant impact on risk. Over time, risk management techniques have evolved to encompass human interaction with engineering systems – that is, to combine predictable, quantifiable, technical risks with the uncertain reactions of human operators or natural systems.

It is also clear that risk assessment and management are information intensive. Large volumes of technical information have to be gathered, processed, analysed and eventually communicated to a broad range of users under quite different conditions, ranging from planning and regulatory activities to incident management.

Finally, management systems may well be needed to assist with risk management. They offer tools for the systematic implementation of policy and strategy. Integrated management systems help to ensure that safety, quality, environmental and business risks are managed right across an organisation. They provide a foundation on which to build continual improvement.

Conclusion

This completes the free course *Assessing risk in engineering, work and life*. You should now have developed your ideas of what is meant by risk in an engineering context and how risk can be assessed in the workplace, home and other situations.

Risk is closely linked to accidents and we have looked at a number of major accidents and the role of human factors in their causes. Understanding how to assess risk and the prevention of accidents are an essential engineering skills. A number of risk assessment and accident prevention methods are considered.

Probability is widely used in assessing risk and this course presents an introduction into probability and its use in risk assessment and at home.

Finally, communicating risk to the wider community is another key engineering skill so ways of presenting risk are presented and the concept of the stakeholder is introduced.

This OpenLearn free course is an adapted extract from the Open University course T193 *Engineering: frameworks, analysis, production*.

References

BP (2010) *Deepwater Horizon Accident Investigation Report: Executive Summary* [Online], BP. Available at www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report_Executive_summary.pdf (Accessed 18 September 2016).

CSB (2007) *Investigation Report: Refinery Explosion and Fire* [Online], US Chemical Safety and Hazard Investigation Board. Available at www.csb.gov/assets/1/19/csbfinalreportbp.pdf (Accessed 18 September 2016).

Engineering Council (2011) *Guidance on Risk for the Engineering Profession* [Online], London, Engineering Council. Available at www.engc.org.uk/engcdocuments/internet/Website/Guidance%20on%20Risk.pdf (Accessed 18 September 2016).

Heinrich, H.W. (1931) *Industrial Accident Prevention: A Scientific Approach*, New York, McGraw Hill.

Heinrich, H.W., Petersen, D. and Roos, N. (1980) *Industrial Accident Prevention*, 5th edn, New York, McGraw Hill.

HSE (1992) *The Tolerability of Risk from Nuclear Power Stations* [Online], London, Health and Safety Executive. Available at www.onr.org.uk/documents/tolerability.pdf (Accessed 18 September 2016).

HSE (1999) *The Cost to Britain of Workplace Accidents and Work-related Ill Health in 1995/96* [Online], 2nd edn, London, Health and Safety Executive. Available at www.hse.gov.uk/pUbns/priced/hsg101.pdf (Accessed 18 September 2016).

HSE (2004) *A Critical Review of Post Piper-Alpha Developments in Explosion Science for the Offshore Industry* [Online], London, Health and Safety Executive. Available at www.hse.gov.uk/research/rrpdf/rr089.pdf (Accessed 18 September 2016).

HSE (2011) *Buncefield: Why Did it Happen?* [Online], London, Health and Safety Executive. Available at www.hse.gov.uk/comah/buncefield/buncefield-report.pdf (Accessed 18 September 2016).

HSE (2016) *Statistics on Fatal Injuries in the Workplace in Great Britain 2016* [Online], London, Health and Safety Executive. Available at www.hse.gov.uk/statistics/pdf/fatal-injuries.pdf (Accessed 18 September 2016).

NHS (2015) *What are the Health Risks of Smoking?* [Online], National Health Service. Available at www.nhs.uk/chq/Pages/2344.aspx?CategoryID=53 (Accessed 18 September 2016).

NHTSA (2015) *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey* [Online], Washington, DC, National Highway Traffic Safety Administration. Available at www-nrd.nhtsa.dot.gov/pubs/812115.pdf (Accessed 18 September 2016).

ONS (2016) *Statistical Bulletin: Adult Smoking Habits in Great Britain: 2014* [Online], Newport, Office for National Statistics. Available at www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/healthandlifeexpectancies/bulletins/adultsmokinghabitsingreatbritain/2014 (Accessed 18 September 2016).

Oxford English Dictionary (2016) [Online], Oxford, Oxford University Press. Available at www.oxforddictionaries.com (Accessed 18 September 2016).

Salminen, S. and Tallberg, T. (1996) 'Human errors in fatal and serious occupational accidents in Finland', *Ergonomics*, vol. 39, no. 7, pp. 980–8.

WHO (2006) *Health Effects of the Chernobyl Accident and Special Health Care Programmes*, Geneva, World Health Organization.

Acknowledgements

This free course was written by Stephen Burnley.

Figure 11 © The Open University

Figure 12 © The Open University

Figure 13 © The Open University

Figure 14 © The Open University

Figure 15 © The Open University

Figure 16 © The Open University

Figure 17 © The Open University

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don't miss out

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.