1

Safety within the legal framework

Men are only clever at shifting blame from their own shoulders to those of others

Titus Livius (59BC–AD12)

1.1 Introduction

Most industrial activities are regulated, and this includes military and civil aviation safety management. Ethical considerations and an increasingly litigious society regarding product liability have become driving factors in changing the way we conduct the initial safety certification (which leads to the release of a system) and manage the continuing safety of the system (including operations and maintenance).

Laws are a system of rules, which are intended to reflect social values, and are enforced through the courts (e.g. it is unacceptable to steal, kill, etc.). Laws can be considered as a compilation of rights, duties and obligations – the violation of which could give rise to legal liability.

In the aftermath of an accident, there is an increasing issue of corporate liability of the CEO and the board of the blamed (e.g. the design authority, maintainer, operator, etc.) – with both fiscal and penal punishments for failure. In today's world, litigation is very expensive and the duty of care of the board exposes them, through their accountabilities, to the possibility of corporate liability – or even to charges of corporate manslaughter.

The content of this chapter is based on English law and is intended to draw engineering management's attention to the legal aspects affecting system safety – it is not meant to be, and should not be regarded as, a complete or accurate statement of the current law. Legislation in this area is developing throughout the world, and is likely to continue to do so for some time. Under English law, legal liability is enforced in two ways: criminal liability and civil liability.

1.2 Criminal liability[1]

This is the law of offences (i.e. crimes) against the state and those under its protection. Prosecution is usually started by the state and it aims to punish and to act as a deterrent through fines, imprisonment, orders and disqualification from holding office. Guilt is determined through the application of the 'beyond all reasonable doubt' principle.

1. See also *Introduction to System Safety Engineering and Management,* University of York.

One example of the impact of criminal law affecting the work of engineers is from the legislation by government through the agency of the Health and Safety Executive. The Health and Safety at Work Act[2] (HSWA) of 1974 imposes duties on persons who design, manufacture, import or supply articles for use at work to ensure (so far as reasonably practicable) that they are 'safe'; to test them; provide proper information; carry out research with a view to eliminating risks, etc.

The HSWA established the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE). Whilst the HSC defines policy, the HSE is responsible for the day to day monitoring and enforcing of the HSWA. The HSE[3] has delegated powers to serve Improvement Notices (requires remedial action) and Prohibition Notices (stops a process). Failure to comply can lead to prosecution. The HSWA affects product safety as well as workplace safety and is based on the 'as low as reasonably practicable' (ALARP[4]) principle, where 'practicable' refers to what is possible to do, and 'reasonable' requires a balance of costs, time, and trouble against the risk.

Reported in *Aerospace International* (RaeS, Nov 2005): 'Henry Perrier, a former head of the Concorde division at Aerospatiale, has been placed under criminal investigation in connection with the crash of the (Concorde) airliner in July 2000. He may face a manslaughter trial for flaws in the aircraft which could have contributed to the disaster'.

1.3 Civil liability[5]

Criminal law does little for the victims of a crime. Civil law regulates the relationship between individuals and thus provides the mechanism whereby the wrongdoers have to compensate the victims. Guilt is determined through the application of the 'balance of probability' principle.

Civil Law comprises Contract Law, Tort (civil wrong), the Law of Property, Succession and Family Law, etc. Action is started by a person (which, in law includes a corporate body such as a company) and it has the aim to compensate (and to deter).

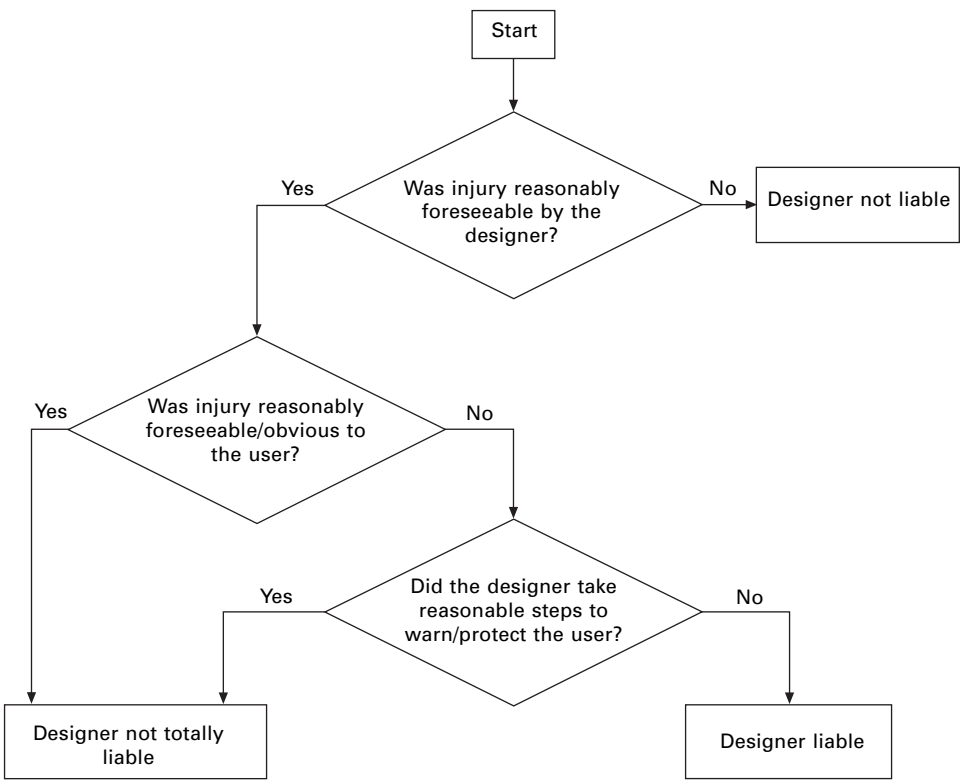
Civil liability for a defective system can arise under the laws of contract, misrepresentation, tort, other common law doctrines and under current UK legislation. Liability can fall on the manufacturer, supplier, distributor or certifier of products (Falla, 1997). In practice, such a supplier or manufacturer is a company and is

2. The principal health and safety legislation in Great Britain is the Health and Safety at Work etc. Act 1974 (HSWA). This sets out in general terms the health and safety duties of employers, employees, and manufacturers, suppliers, and designers of articles for use at work. The HSWA applies to all workplaces (including the MoD and the self-employed). It provides protection for workers and general public.
3. The HSE has subsidiary organisations (e.g. Nuclear Installations Inspectorate (NII), Her Majesty's Railway Inspectorate (HMRI)).
4. See also Chapter 4.
5. See also *Introduction to System Safety Engineering and Management,* University of York.

regarded as a legal entity who can sue or can be sued in its own right. Suppliers of components can also be liable. In cases where the component is used in products which are exposed to the general public the extent of such liability can be enormous.

Under Civil Law (Tort), individuals can claim compensation if they can show that a duty of care was owed, this duty has been breached, and that a loss has been suffered. An example of this process is illustrated in Fig. 1.1. Plaintiffs have to prove that they were owed a duty of care, that there was a breach of that duty, and that the loss or damage was a direct result of that negligence. The claimant does not have to prove negligence[6] on the part of the supplier. All professional work is done under contracts containing either an express or implied term that professional persons will use reasonable skill and care in the performance of the work.

Under the Consumer Protection Act of 1987 (see section 1.4.1), a supplier is liable if there is a causal link between a defect and an injury (this is referred to as the 'Liability of Tort'). A product is defective if it does not provide the safety that people are generally entitled to expect, taking into account all circumstances (all circumstances



1.1 Duty of care vs. liability.

6. Negligence is the failure to exercise the degree of care that is required by law in the particular circumstances. Negligence can occur by an act or omission.

include 'the manner in which and the purpose for which the product has been marketed'). Products are defined very loosely, and without a doubt includes all aviation products – from substances, materials, components, through to systems and platforms. Furthermore, a product consists not only of the product itself, but also of the literature and warnings (i.e. instructions for, or warning of, doing or refraining from doing anything with the product) which accompany it.

1.4 Sentencing trends

1.4.1 Consumer Protection Act

The Consumer Protection Act, 1987, was enacted in the UK to fulfil obligations to implement a European Directive designed to protect consumers across member states. It introduces so-called 'strict liability' (as opposed to 'fault liability' in contract and tort) for defective products supplied in the course of a business. Where damage is caused by a defect in a product then the producer is liable to compensate the injured party whether or not he is at 'fault' (Falla, 1997).

Falla (1997) also highlights the fact that the removal of the fault criteria means that the Consumer Protection Act imposes the highest 'standard of care' on a producer. If a producer is not liable under the Act it is unlikely he will be found liable in negligence. Only damage of a specific type may form the basis of an action under the Consumer Protection Act. The damage may be death, personal injury or damage to property. However, only property which is of a type ordinarily intended for private use[7] may be the subject of a claim and property damage must exceed £275.[8]

A plaintiff who brings an action under the Consumer Protection Act must show that, as a result of the defect in the product, it was reasonably foreseeable that an injury of the type suffered would occur. This is unlikely to be difficult in the context of a safety-critical system: if it is not safe, it is reasonably foreseeable that persons will be injured and property damaged as a result.

1.4.2 Legal charges

The legal consequence of product failures that subsequently cause harm and/or loss might include criminal actions (e.g., manslaughter, Health & Safety at Work charges, corporate manslaughter, corporate manslaughter by gross neglect) or civil actions (e.g., on the contract, trespass (person), trespass (property), negligence, strict liability actions).

---

7. Therefore, if a chemical plant were to explode because of a faulty computer control system the damage to any surrounding office buildings or to the chemical plant itself could not be the subject of a claim under the Act. Office buildings are not ordinarily intended for private use. However, if the homes or possessions of nearby individuals were also damaged, liability to pay compensation would arise for the damage to those houses and possessions under the Consumer Protection Act.
8. Or such other figure as substituted by legislation from time to time.

1.4.3 Fines

Fines under HSWA (sections 2–6) can be up to £20,000, with the average fine in 1997–1998 being £6,223.

> A judgment in the Court of Appeal (*Regina* vs. *F Howe & Sons*, Nov. 1998): 'a fine must be large enough to bring home to those who manage a company, and their shareholders, the need for a safe environment for workers and the public. While a fine should not generally be so large as to imperil the earnings of employees or create a risk of bankruptcy, there may be cases where an offence is so serious that the defendant ought not to be in business.'

Fines have been increasing under the civil law (HSWA), e.g., £5.1 million in March 2001 for a boy made quadriplegic (civil). Fines have also been increasing under the criminal law (HSWA), e.g., £1.2 million fine on Balfour Beatty in Feb 1999 due to collapse of train tunnels in Heathrow Express Rail Link.

1.4.4 Prosecutions

At the extreme, accidental loss of life could result in individuals and companies being prosecuted for manslaughter under the criminal law. Any company is represented by senior members (e.g. the main board) who could be subject to imprisonment or fines.

> Kite and OLL (1996): Death of school children in canoeing accident in Lyme Bay. Kite was one of only two directors, and was jailed as the 'controlling mind'.

Manslaughter is an unusual crime where the prosecutor does not have to establish intent, but has to show reckless disregard of accepted practices, gross negligence (or 'such disregard for life'), or conscious wrong doing before it is a criminal act. However, determining the extent of individual responsibility on the 'controlling mind' has led to many unsuccessful prosecutions. Hence the Law Commission report in 1996, which recommended[9] laws on:

- Corporate killing, applicable to companies: this is intended to make a company accountable in criminal law where conduct falls far below that which can be reasonably expected in the circumstances. The proposed maximum penalty here is for an unlimited fine and a remedial order that is designed to prevent the original cause of the accident. In addition, directors might well be liable to disqualification.

9. The UK Home Secretary has made it clear that he intends to reform the law to make it easier to identify and convict those responsible for corporate killing. It is generally accepted that a company and/or a corporation must operate responsibly but the current debate on corporate killing really starts with the current involuntary manslaughter law, which has proved to be ineffective when applied to corporate killing.

- Reckless killing and killing by gross carelessness: this is applicable to individuals, including company directors, where:
  - reckless killing typically involves an individual knowing that there is a risk that their product or conduct will cause a fatality or a serious injury and that it is not reasonable to take that risk. In this instance the maximum penalty is quoted as life imprisonment.
  - A person is guilty of gross carelessness when the risk that the product/conduct could cause death or serious injury is obvious to a reasonable person in his position. The individual concerned should have been capable of appreciating the risk and that their conduct fell far below what could reasonably be expected of them in the circumstances. Or they intended their action to cause an injury, or they unreasonably took a risk that it might cause an injury. Killing by gross carelessness could lead to a maximum penalty of ten years in prison.

The Law Commission's suggested text states:

4 (1) A corporation is guilty of corporate killing if:
  (a) a management failure by the corporation is the cause or one of the causes of a person's death; and
  (b) that failure constitutes conduct falling far below what can reasonably be expected of the corporation in the circumstances.
(2) For the purposes of subsection (1) above:
  (a) there is a management failing by a corporation if the way in which its activities are managed or organised fails to ensure the health and safety of persons employed in or affected by those activities.
  (b) Such a failure may be regarded as a cause of a person's death notwithstanding that the immediate cause is the act or omission of an individual

1.5 Organisational responses

1.5.1 Legal liability for dangerous or defective systems

Manufacturers, suppliers, importers and designers of articles (which includes equipment for use at work) must (refer HSWA Section 6) in so far as they are matters within their control:

- ensure that articles for use at work are designed and constructed to be safe at all relevant times, i.e., when they are being set, used, cleaned or maintained by persons at work
- arrange for testing and examination to ensure compliance with the above
- provide persons supplied by them with adequate information about:
  - the uses for which such articles are designed or tested
  - any conditions necessary to ensure that the articles will be safe at all relevant times and when being dismantled or disposed of
- update the information referred to above as necessary, upon discovering that anything gives rise to a serious risk to health and safety.

An issue which should exercise the mind of any supplier of a critical system is the question of exposure in law should the system fail.

Directors

A director of a company will operate under some form of service contract which will include, either explicitly or implicitly, a term that the director will take reasonable care in the exercise of his or her duties. A director has authority to exercise the powers which the company has given him. If in the exercise of such powers he breaches his duty of care either through negligence or by a deliberate act or omission, the director may be held liable for the breach, the consequences of which could vary from the death of an unconnected individual to financial loss by the company's creditors. The degree of fault required to impose liability on a director varies according to the consequence of the breach. This will depend upon whether he is liable under civil or criminal law.[10] Breach of this contract will have the effect that the company could in theory sue the director, but the damages available to the company will be limited by the director's resources. In addition, the company may have difficulty showing that the company's loss is a consequence of the director's breach of contract.

Employees

Negligent employees and independent contractors may also be held liable in contract and in tort, but again the damages available will be limited by the individual's resources. The distinction between an employee and a contractor does not depend solely on whether the contract declares a worker to be an independent contractor. Each case will depend on its own facts but account will be taken of the ownership of equipment, the chance of profit and the risk of loss on the worker's part.

1.5.2 Organisational response to the criminal law

The standard 'as far as reasonably practicable' is that used in the HSWA case law. The standard has acquired the meaning that the risk of adverse effect (e.g. death or injury) must be balanced against the cost, time and physical difficulty of taking measures to

10. There have been recent moves for directors to be made personally liable in criminal cases, e.g., manslaughter. Although there have only been a few reported cases, there is a definite trend towards making directors more accountable. The one hundred delegates (refer to www.healthandsafety.co.uk (10 January 2004)) to the recent British Safety Council conference (2004) heard its Director General David Ballard warn that 'Time is running out for those who, through blatant disregard of the law, allow employees to be killed or injured and yet are punished with fines in the low thousands'. Ballard continued 'Every senior executive and health and safety director should be extremely concerned about the new offences. This may even deter some from taking jobs that carry heavy responsibilities. Executives working under the threat of possible imprisonment for safety lapses will simply have to be more alert and better trained to appreciate risks. The public's desire for retribution is a strong consideration for any change to the law but, in the end, the purpose of any legislation has to be to improve health and safety performance.'

reduce the risk. If the quantified risk is insignificant compared with the measures needed to mitigate the risk, then no action needs to be taken to satisfy the law. However, increased risk will require robust justification to support a choice of no action.

All organisations must publish Health and Safety Policy, covering:

- risk assessment, identification and minimisation
- procedures and facilities for safe handling, storage and transportation
- product integrity regime
- surveillance (information, instructions, supervision)
- emergency procedures.

Corporate response must include:

- a safety management system (SMS)
- safety management plans and procedures/processes (including those to deal with product integrity).

Milan Linate Airport (Oct. 2001), 118 casualties:
A high-speed collision in severe fog between a Scandinavian Airlines Boeing MD-87 and a private Cessna Citation CJ2 occurred because the CJ2 was on the wrong taxiway and then crossed the active runway without permission. Four people were judged guilty (subject to appeal) of negligence and manslaughter and ordered to pay court costs, to pay compensation to the victims' families and disqualified for life from public service. Prison sentences: the Tower Controller and the Airport Manager each received 8 years, an official at Italy's National Agency for Civil Aviation (ENAC) received 6.5 years, as did the managing director of Italy's air traffic services. One of the issues criticised in the accident report was the lack of a safety management system: there were systematic faults in the sense that the [management] system had either not noticed them, or it had tolerated them.
Source: *Flight International* (27 Apr.–3 May 2004)

The Act also requires:

- a director in charge with explicit responsibilities for training, inspection (prevention) and investigation
- an explicit chain of authority and identification of responsibilities (often normal management chain and separate line to responsible manager)
- regular auditing.

1.5.3 Organisational response to the civil law

Project teams, contractors, consultants, software houses, advisers, independent auditors, test houses, manual producers, operators, maintainers, regulators, etc., all make for one big happy family until it goes wrong and there is a big hole in the ground (e.g. after the Concorde crash in France, the defendants included BAe systems, Air France, Continental, Middle River, GE, Goodyear, EADS, etc.). Then the lawyers reach for

their law reports and legal liability will surely arise. Each party will then try to devolve their liability to the producers, operators, maintainers, contractors, consultants, advisers, integrated project teams (IPTs), independent advisers, regulators, etc.

The crucial question will be whether there was a failure of management to provide for safety. In terms of criminal liability, all companies have to look very carefully at their management systems.[11] Management need to take the following actions to discharge a duty of care and to reduce the chance of product liability:

- Establish an effective safety management system/process. Nominate key roles/responsibilities. Define approval signatories – especially for safety reports. Establish independent verification/audit to reduce chance of undetected error. Establish a workforce-wide commitment to product integrity. Learn from previous mistakes.
- Initiate a documentary audit trail (identify, log and track all hazards). Airworthiness and safety must be foremost in the minds of the entire organisation. Furthermore, as many legal cases turn on documentation, it is essential that risk assessment activities and choices are documented and that records are kept.[12]
- Spread the risks, either via contract terms, or via insurance (see section 1.5.4).
- Insurance can give limited protection against some civil claims; specific advice should be sought from brokers specialising in this field.

1.5.4 Organisational responses to the Consumer Protection Act

Section 10 of Part II of the Consumer Protection Act 1987 makes it a criminal offence to supply any consumer goods[13] which do not comply with the 'general safety requirement' of it being reasonably safe with due regard to all circumstances. Organisations will have to ensure, so far as reasonably practicable, that the hardware and software are designed and constructed for safe operation of the system (*Safety-*

11. It seems likely that a chief executive will be able to reduce the chance of a corporate killing prosecution through employing a competent health and safety director who is directly responsible to a board. But a company will need to introduce a watertight health and safety plan which will cover worker participation and reports of all near misses which will have to be reviewed at Board level. Busy Directors will be forced into expanding their energies into risk identification and elimination and, it is a fact, that many organisations will have to provide additional resources towards providing a safer workplace. In fact, the forthcoming legislation could well create the ethic of putting safety ahead of any cost considerations. And there is no guarantee that a jail sentence will not be imposed on the most safety-conscious executive in a safety-conscious organisation arising from circumstances where the risk was not obvious or appreciated by anybody from shop floor upwards in an organisation.
12. In a recent court case in England, the judge stated that any form of retrievable information, no matter how that information may be stored, is a document. Letters, internal memos, drawings, films, videos, e-mails, note books, personal dairies, log books, reports, etc., are all food for litigation. Document management is thus essential. According to Williams (2003), the elements of an effective document management system are: their preparation; their storage; ease of retrieval; destruction management; training
13. 'Consumer goods' are defined for the purposes of Section 10, as 'any goods which are ordinarily intended for private use or consumption', but exclude a number of products, such as motor vehicles and aircraft, food, water, gas, drugs and (of course) tobacco.

related systems, Guidance for Engineers, Aug 2002, page 14). This includes undertaking all necessary research, testing and examination. It may not be necessary to repeat tests, examinations, certification carried out by other parties in the supply chain, provided that it can be demonstrated that the system is appropriate for the purpose for which it is supplied. All information necessary for the safe operation of the system must be provided.

The practical scope for a manufacturer or supplier to exclude or restrict their liability under the Consumer Protection Act is very limited. According to Falla (1997), the only practical step which a manufacturer or supplier can take is to 'pass the buck' by seeking an indemnity through contract from the person who supplied them. The person who is likely to end up with the liability is, therefore, the person at the beginning of the supply chain.[14]

A producer may be able to rely on the following defences:

- that the defect did not exist when the producer supplied the product
- that the state of scientific and technical knowledge at the time was such that a producer of the same type of product could not be expected to have discovered the defect[15]
- that the component was supplied in accordance with instructions from the producer and the component would not contain a defect had the overall product been designed properly with the component in mind. This defence protects the component manufacturer against a claim arising from a defect in that component which they would otherwise be liable for.[16]

---

14. Whether an indemnity from the persons at the beginning of the chain is of any financial value is, of course, something that must always be borne in mind.
15. This is the so called 'development risk defence' (Falla, 1997). The test is applied at the time when the product was under the producer's control. The wording of UK legislation seems to point to the defence being based upon what a reasonable producer would do. However, a producer should not rely upon this being the case, as the wording of the underlying Directive provides that the defence will apply only if the scientific and technical knowledge was not such as would allow the defect to have been discovered at all. In practice therefore a prudent producer needs to take all the steps possible in order to be sure that they have a defence. The legislation places the burden of proof on the defendant and so it is for the producer to prove that it is impossible to discover the defect.

    Manufacturers and suppliers of hardware and software must take notice of (and comply with) those standards which do exist in the industry. Similarly, manufacturers should ensure that adequate verification and validation procedures in the production of hardware and software are followed. They should also take note of any other procedures and draft standards generally followed by cautious manufacturers. Such actions would be seen as evidence in support of this defence, although would not necessarily absolve the defendant from liability.
16. This defence has the following limitations (Falla, 1997): (i) it is available only to the manufacturer of a *component*; (ii) the component manufacturer must receive instructions from the producer of a product which incorporates his component; (iii) the component manufacturer must have actually complied with those instructions; and (iv) the component manufacturer must be able to show that the defect is wholly attributable to his compliance with those instructions.

    Falla (1997) advises that, from a practical point of view, it is unlikely that this third defence will operate in many circumstances. In most situations, manufacturers of complete products will not give instructions which are so detailed as to enable a component manufacturer to take advantage of the defence, particularly since the defence only arises in the defect is wholly attributable to compliance with instructions.

Note that Section 10 of the Act does not apply to goods intended for export or to second-hand goods (refer *Safety-related systems, Guidance for Engineers*, Aug. 2002, page 15). Nor does it apply to retailers if they had no reasonable grounds for believing that the goods failed to comply with the general safety requirement. Defendants who can demonstrate that they follow 'good practice' will usually have a defence to an action founded on the case of negligence (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 18). This is because the test for negligence is based on a test of 'reasonableness' and following 'good practice' will usually be synonymous with taking reasonable care. However good practice may not be a sufficient defence for complex, integrated safety critical systems. Instead, a 'best practice' argument may be required and a well prepared safety case, safety assessment and/or safety argument would be essential.

1.5.5 Contracts

An agreement between parties forms the basis of a claim in contract. Contractual relationships frequently exist despite the lack of a written document or prior to signing, provided that there is an agreed common intention to form legal relations (Falla, 1997). For a contract to exist there must be:

- an agreement between parties which is formed from an offer given by one and accepted by another
- a consideration which supports the agreement, e.g., money payable or a promise in return for the promise to perform the contract
- an intention to create legal relations (this is presumed in most agreements).

Under legislation which regulates the 'sale of goods' and 'supply of services' and which invariably applies to the supply of hardware and software, there are terms implied in the supply contract. Most important of the provisions are under sections 13 and 14 of the Sale of Goods Act 1979 as amended by the Sale of Goods (Amendments) Act 1994 and the equivalent sections 8 and 9 of the Supply of Goods and Services Act 1982:

- Section 13 states that the goods supplied must correspond with their description. For example, if a computer system has a description that it will 'perform X number of functions per second' or that the software complies with specified standards, the supplier will be in breach of this implied term if the system or software is not as described.
- Section 14 states that the goods must be of satisfactory quality[17] and that they are reasonably fit for the buyer's purpose. The latter part of this implied term applies where the buyer expressly or by implication makes known to the supplier any

17. The Sale of Goods (Amendments) Act 1994 introduced a new subsection to section 14, i.e., subsection (2D). This provides that the quality of goods includes both state and condition, and includes a non-exhaustive list of factors for taking into account when assessing whether goods meet the requirements of satisfactory quality. Primarily buyers will now find it easier to complain if there are a number of minor defects.

particular purpose for which the goods are being bought (whether or not that purpose is one for which the goods are commonly supplied). In many circumstances, such as in the supply of safety-critical systems, the purpose arises by implication. In circumstances where it would be unreasonable for the buyer to rely on the skill and judgement of the seller, or he did not in fact rely on the seller's skill, then this term is not implied. In the safety-related field it is also likely that a particular purpose will be expressly stated.

Certain clauses (so-called 'exclusion clauses') are commonly relied on to exclude or restrict the liability of a party arising through the failure to perform a contract. The Unfair Contract Terms Act 1977 limits this ability to exclude or restrict liability in certain contracts. In particular, it is never possible to exclude or restrict liability in negligence, or in relation to failure to take reasonable care in the performance of a contract, for personal injury or death by reference to any contract term.[18] A contract sets the parameters of liability, and the rules of privity (i.e. only a party to the contract is able to sue) limit the persons who can claim for loss or damage under a contract. Where, however, a duty of care can be established between a person who has manufactured or supplied a product and the person injured then this injured party may be able to sue in tort for the negligence of the manufacturer or supplier (Falla, 1997).

Falla advises that, in order to have a good cause of action in negligence, a plaintiff must establish that:

- the defendant (manufacturer or supplier) owed the plaintiff a duty of care
- there has been a breach of this duty which caused the injury or damage
- the kind of damage sustained was reasonably foreseeable as a consequence of that breach.

For a duty of care to exist it must be reasonably foreseeable that in the absence of reasonable care in the preparation of a product the consumer (or the innocent bystander) may suffer injury to his (or her) life or property. This duty will occur when the product is intended to reach the ultimate consumer in the state in which it left the manufacturer. In practice, it is not usually difficult to find one or more persons who owe a duty of care in the circumstances of the supply of a safety-critical system.

Case law on negligence in product manufacture and supply has established a number of areas where a lack of reasonable care would constitute a breach of duty (Falla, 1997):

- the design and construction of the product should be done with the care appropriate to the likely dangers in its use
- the component parts should be inspected or otherwise examined to ensure that if properly used in the end product, the end product can be safely used by the consumer

18. On 1 July 1995 the Unfair Terms in Consumer Contracts Regulations came into force. They only apply to consumer contracts and not to business contracts. Unlike the Unfair Contract Terms Act 1977 the regulations apply to all unfair contract terms and not just unfair exception clauses.

- the container used for the product must be suitable
- the product must be labelled to take account of its dangers
- proper instructions must be given for the safe use of the product.

The manufacturer may raise a number of defences, which could include (Falla, 1997):

- that the manufacturer took all reasonable care whilst making the product to ensure that the defect was not present
- that the product was not initially dangerous but became so because of the action of some intervening person
- that the manufacturer made it clear that the products should not be used before being tested.

Products where computer software is a component present a further level of difficulty. It is not clear, for instance, what the software supplier needs to do to take 'reasonable' care in the design of the system.[19] In practice, an injured party may face significant hurdles establishing a lack of reasonable care. Furthermore, the injured party must also prove that the damage which occurred was a reasonably foreseeable consequence of the breach.

1.6 Implications on the engineer[20]

The *Code of Professional Practice on Engineers and Risk Issues* (hereafter referred to as the Code) became effective on 1 March 1993 and applies to all registrants of the Engineering Council. A member of the engineering profession knowingly and voluntarily undertakes a responsibility to others, and in doing so shoulders certain personal, social and professional responsibilities. Because of their involvement and understanding, engineers have a central role in the control of risk. Their professional duty rightly includes the exercise of competence[21] and integrity.

It is evident that engineers can be held legally accountable for their actions, or for a failure to act. Consequently, all engineers need to acquire an understanding of the law and its relevance to risk issues. Although absolute safety can never be guaranteed, this fundamental limitation is under no circumstances an excuse to avoid professional responsibility. The Code sets out duties of a professional engineer working with safety related systems. These general duties are often supplemented by law (e.g. Health and Safety at Work Act), industry specific regulations (e.g. JAR25.1309) and local codes of practice applicable to a particular task. These all have the following requirements in common:

- to take all reasonable care
- to do all that is reasonably practicable to ensure safety
- to show due diligence to prevent danger.

19. Note the disclaimer notice contained in many licences issued by software suppliers.
20. See Engineering Council, *Guidelines on risk issues.* See also (http://www.iee.org/policy/areas/scs/hazpub.cfm
21. For more on competence, see paragraph 4 of *Safety-related systems, Guidance for Engineers*, Aug. 2002, The Hazards Forum, 1 Great George St, London, SW1P 3AA, ISBN 0 9525103 0 8.

The above three points are usually summarised in some sort of safety case, safety assessment, safety justification or safety argument, which has the following main purposes:

- firstly, and most obviously, to justify to others the confidence which designers and intended purchasers and users have in the safety of the system
- secondly, to provide evidence that, even though an event may occur which was not foreseen or considered when the system was designed, all reasonably determinable safety related concerns were considered and dealt with appropriately in the design and certification of the system. This may provide an important legal defence.

An in-depth assessment from first principles and a cost-benefit analysis are not needed for every job. The extent of consideration should match the nature of the hazard and the extent and uncertainty of the risk and the measures necessary to avert it. In many cases it will be sufficient to identify and comply with the appropriate regulations. However, with hindsight (e.g. after an event) others may challenge actions/decisions, and an engineer may have to establish the facts in the face of a hostile situation. Ultimately, a decision may have to be defended on judgement and so, particularly where decisions or recommendations are finely balanced, the consideration should be documented and, if possible, corroborated.

Individual engineers[22] need to be aware of their limitations and not undertake tasks for which they are not competent (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 2). However, there is the possibility that:

- some engineers however well-intentioned, ethically minded, and otherwise competent, might not appreciate their limitations for particular tasks which are, without them being aware of it, differ in some respects from those for which they have proved themselves competent in the past
- some engineers are instructed to perform tasks for which they know or suspect they are not competent enough.

For these circumstances, it is management's responsibility to continually ensure that all practitioners have qualifications, experience and qualities appropriate to their duties and that they are provided with the required resources and authority to perform their duties. Furthermore, sufficient diversity of input/participation will also ensure the intended integrity of the task.

Engineers should be aware of the potential for conflicts of interest, and for differences of opinion between themselves and their employing organisation. In such circumstances, they are advised (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 25) to maintain written records, kept in a safe place, of any disagreement and the course of action that was taken.

22. Regarding professional/chartered engineers it is worth noting the following: in many countries (but not yet in the UK) certain positions of engineering authority can be occupied only by registered professional/chartered engineers. Just as medical doctors can be struck off the medical register, so these engineers face being struck off the engineering register if found guilty of professional misconduct or neglect. Loss of professional/chartered registration thus has a severe impact on future career prospects.

Words of wisdom

- 'Do not believe, prove it for yourself'
- 'Do not ignore the feelings in your bones'
- 'Stand by the technical truth, however great the political or commercial pressures'
- '*Non fici facio – vera prae ceteres* (don't give a fig – truth above all)'

David, P.D. (1920–2003),
(Chief Test Pilot for UK CAA for 33 years until his retirement in 1982)

1.7 Discussion

The Engineering Council advises that engineers should, within the constraints of their work responsibility, seek to identify possible hazards and ways to reduce risk. They should not take the attitude that risk management is someone else's business; rather, they should take the initiative. There is no substitute for professional practice in this regard. A systematic and documented approach will be more cost-effective, auditable and more likely to come to the right conclusions. As a minimum, key risk decisions together with their reasoning should be recorded. It should not be an unreasonable burden. If it is unnecessarily bureaucratic, the system must be modified to be more flexible and so that it can cost-effectively contribute to product quality.

To maintain professional integrity, as well as to avoid legal repercussions, specialist input must be obtained where necessary – even if it has to be bought in. Engineers should not exceed, nor ask others to exceed, their level of competence where the result may put people at risk. Similarly, it is important to validate the competence of contractors and sub-contractors. Professional judgement is by far the most important tool in risk management. Judgement is particularly important in the initial assessment of risks and deciding on their tolerability. Formal safety assessments methods should be used as aids to judgement, not as substitutes for it.

Effective training is essential to success in almost every area of engineering, and risk management is no exception. The key to quality and efficiency is professionalism, which is a combination of expertise and attitude:

- training and experience provide the expertise, while
- company culture and experience shape the attitudes.

In the event of an accident people want someone to blame. We feel unsafe and the only way to feel safe again is to blame somebody. We want one name or entity to blame, who unlike the rest of us, caused us to feel unsafe. The truth is that it never is one name. But still we feel much safer if there is someone to blame. And if the finger is pointed at us, our only defence will be accurate and measurable records of our company's safety policy and its achievements.

If companies involved in fatal accidents face the risk not only of paying compensation, but also having their employees prosecuted, then accurate and measurable records of a company's safety policy and its achievements become important evidence. Remember that actions and decisions may be challenged by others with the benefit of hindsight. And hindsight is well known to be an 'exact science'. Our decisions may have to be

defended on the basis of judgement of the issue under concern, and, wherever possible, our decision making process must be documented and validated. How would your records face up to third party scrutiny? How would you be able to demonstrate that you have taken reasonable care as a professional engineer/manager should you be faced with a court appearance?

> The ultimate measure of a man is not where he stands in moments of comfort, but where he stands at times of challenge and controversy.
>
> Martin Luther King Jr (1929–1968)

1.8 Further reading

Chapter 2 in Falla, M. *Advances in Safety Critical Systems, Results and Achievements from the DTI/EPSRC R&D Programme in Safety Critical Systems,* June 1997.
http://www.comp.lancs.ac.uk/computing/resources/scs/#APPENDICES

Safety-related systems, Guidance for Engineers, Aug 2002, The Hazards Forum, Institute of Electrical Engineers, 1 Great George St, London, SW1P 3AA, ISBN 0 9525103 0 8.
http://www.iee.org/policy/areas/scs/hazpub.cfm

Engineers and Risk Issues, Engineering Council's Code of Professional Practice, 1992, Engineering Council, UK.
http://www.iee.org/policy/areas/scs/hazpub.cfm