MINISTRY OF DEFENCE

An Introduction to System Safety Management in the MOD

Issue 3 **January 2011**

Background

Many of the tasks which MOD undertakes would be considered inherently dangerous in the non-military environment, with increasingly complex systems employed in sometimes hostile environments. In order to ensure the safety of MOD employees and others affected by its activities, it is essential that safety is robustly managed; there must be a clear understanding of all associated risks, continuous vigilance to identify emergent issues and effective processes to manage the risks in an enduring manner. Through the adoption of such an approach, MOD builds on a history of generally good safety practice, supplemented with good practice from other organisations, to ensure that safety is successfully managed and continuously improved in all areas of its responsibility.

The management of safety applies throughout the life of a project, from Concept through to Disposal. Safety risks must be considered both for peacetime and for conflict, although higher risks may be considered tolerable in times of war.

The Secretary of State for Defence issues MOD's Safety and Environmental Policy, which states (inter alia) that MOD and the Armed Forces shall, in their organisation and processes:

Ensure that in the acquisition of materiel, services and equipment of all kinds, safety and environmental management begins at the requirement definition stage and is carried forward through life to disposal. This includes all aspects of maintenance and operation. (July 2009)

Purpose

This booklet is an introduction to system safety management concepts, terms and activities. It is intended to allow MOD and contractor personnel to understand quickly how safety issues affect them.

The contents of this booklet are intended for information and must therefore not be used as the basis for any contract or instruction to contractors.

Acknowledgement

This booklet was written and revised under contract to MOD.
Principal author: Rhys David MA CEng
e-mail: rhys@safetyassuranceservices.co.uk

Suggestions for improvement should be sent to:
Safety & Environmental Protection Group
e-mail: DESSESEP-Acq-Safety@mod.uk

Issue 3.0

Contents

Contents (continued)

1. Introduction

Key Messages
Perfect safety is rare, so risks must be recognised, understood and controlled
People should only be exposed to safety risks if a benefit is expected and the risks are adequately controlled
Safety management allows you to do safely what you want to do: it is not about avoiding doing something just in case it is harmful
Everyone has a part to play in safety management, but senior managers have the key role because of their authority to provide resources, and to establish the right organisation, attitudes and priorities
Safety management systems should exist at various levels in MOD and its contractors
Professional judgement by engineers, managers and military commanders is the most important part of safety management
The safety case provides a way of showing that safety has been considered properly and that decisions are well founded.

1.1 Safety Matters

As individuals we all want to be free from harm, whatever the cause - an earthquake, a plane crash, poison in the environment or an accident at work. However, perfect safety is rare because almost any activity has dangers. We may tolerate these dangers to gain financial benefit, advantages or thrills, but we still want the dangers to be kept under control.

Over time, safety has become more important as the perceived value of life has risen and disasters are seen as avoidable, rather than random acts of God. Accidents have led to the introduction of health and safety legislation intended to prevent them happening again.

Knowledge about what causes harm also grows over time, so that substances and practices which used to be considered safe, are now recognised as being damaging. Examples of this include asbestos, noise exposure and smoking. Where the substance or practice gives a benefit as well as causing damage, it is necessary to have some objective way of balancing the two. For example, medical treatment might have side effects.

Safety is an emotive and subjective topic: many people want all risks eliminated from anything that might affect them personally. Safety management is concerned with having a consistent approach to potential causes of harm and targeting effort where it will have the most benefit.

You often hear the statement that "safety is paramount", especially after a major accident. However, a balanced view must be taken, in which safety does not dominate and prevent effective business, nor is it ignored as has often occurred in the past. Good safety management allows you to do safely what you want to do: it is not about avoiding doing something just in case it is harmful. The Ministry of Defence's (MOD's) "business" involves providing military capability and so it will tolerate some safety risk exposure in order to achieve this: what is important is that the risk exposure is understood, managed to low levels and justified by the benefits gained.

1.2 Why Manage Safety?

Many modern systems are very complex and the consequences of possible accidents from them are enormous in scale. Because of the pace of technological change, it is no longer possible to rely simply on designs and practices which have been perceived as safe in the past.

The investigation of accidents shows that there are often common themes to why they happen. Examples of these include:

- Problems which have previously shown up as minor incidents or near misses but have never been resolved
- No-one ever imagined that the circumstances of the accident could happen, so there were no systems or emergency procedures to deal with them
- People thinking that it is someone else's job to deal with safety
- Sloppy work practices building up over time because they are easier or cheaper
- Equipment being modified or used in ways for which it wasn't designed
- People being scared to report safety concerns because they themselves made a mistake, or they don't want to appear stupid, or there is no easy reporting system

Safety management attempts to deal with these common root causes by putting emphasis on a proactive approach; prevention, rather than just reacting to harm once it has occurred.

Accidents are indications of a failure on the part of management. The official inquiry report on the capsize of the **Herald of Free Enterprise** ferry in which 188 people died included the following statements:

> *"A full investigation into the circumstances of the disaster leads inexorably to the conclusion that the underlying or cardinal faults lay higher up in the organisation. The Board of Directors did not appreciate their responsibility for the safety management of their ships."*

> *"All concerned in management, from the members of the Board of Directors down to the junior superintendents, were guilty of fault in that all must be regarded as sharing responsibility for the failure of management. From the top to the bottom the body corporate was infected with the disease of sloppiness."*

> *"It is apparent that the new top management has taken to heart the gravity of this catastrophe and the company has shown a determination to put its house in order."*

Until quite recently only the people directly involved would have been held to blame for an accident. Now it is recognised that safety is everybody's concern. Individuals are responsible for their own actions, but only managers have the authority to correct the attitude, resource and organisational deficiencies which commonly cause accidents.

The independent review into the loss of the RAF Nimrod XV230 in 2006 concluded that there was:

> *"A failure of leadership, culture and priorities".*

Safety management is intended to bring together all the facets of safety including:

- Engineering design
- Risk management
- Training
- Operation
- Upkeep
- Disposal

The key elements of successful safety management are shown in the following diagram, based on HSG65, the HSE Guide to successful health and safety management. Safety Management Systems (SMSs) embodying these elements should exist at various levels within an organisation like the MOD, from equipment acquisition project, to department, facility, site and organisation-level. Contractors working for MOD also require effective systems for managing safety.

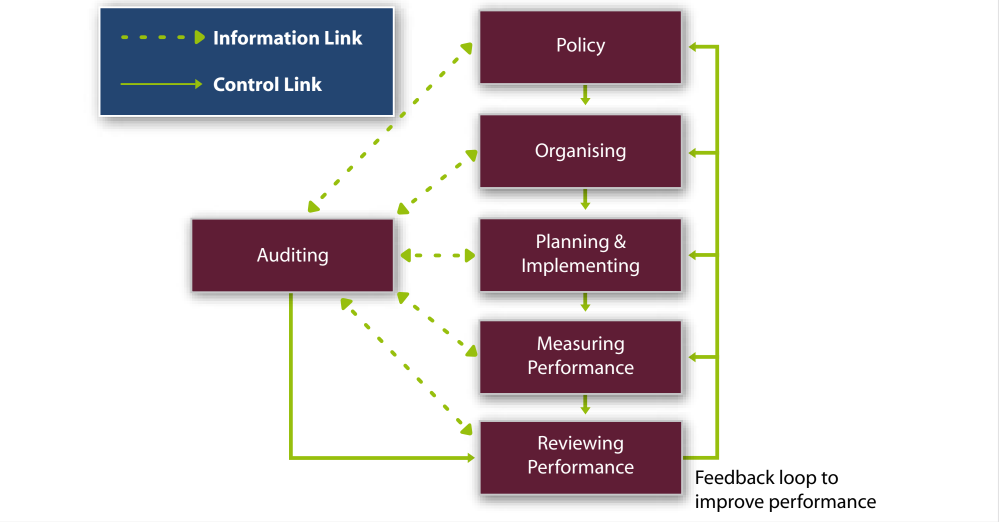


Figure 1: Key Elements of Successful Safety Management (after HSG65)

1.3 Judgement and Evidence

Engineers, managers and military commanders have always used judgement for safety issues. Professional judgement continues to be by far the most important part of safety management. Formal safety assessment methods must be used as aids to judgement and not as substitutes for it. "Safety case" is the term used for the record of safety evidence and the decision process (see Section 7).

Actions and decisions may be challenged by others, sometimes with the benefit of hindsight. A decision may have to be defended on the basis of judgement, and so the decision process must be documented and all judgements and assumptions validated wherever possible. Stating that an event has never happened before is not, on its own, valid evidence that a particular event will not happen; the safety case provides a way of showing that safety has been considered properly and that decisions are well founded.

1.4 How MOD Manages System Safety

MOD has a management system for safety and environmental protection that applies across the whole organisation and covers the key elements identified in Figure 1. This management system is described in Joint Services Publication (JSP) 815, Defence Environment and Safety Management, which also contains the policy statement made by the Secretary of State for Defence (SofS).

A key feature of MOD's safety management system is a governance requirement for clear separation between assurance and delivery. The assurance function is concerned with setting policy and standards and undertaking monitoring and regulation. The delivery (or ensurance) function is responsible for meeting the defined standards.

The SofS's policy statement provides strategic direction to the MOD's Functional Safety Boards. Each board has responsibility for safety policy and assurance in a defined area and they provide documented policy and guidance in a domain-specific JSP. The Functional Safety Boards are each supported by a Functional Safety Management Office, details of which are provided at the end of this booklet.

The SofS's policy statement also provides strategic direction to all the Top Level Budget holders and Trading Fund Agency Chief Executives responsible for the implementation of MOD's safety policy.

They have systems for explicitly delegating down the management chain, the authority for implementing safety policy. Top Level Budget holders and Trading Fund Agencies will also have safety and environmental management systems for their own organisations.

Defence Equipment and Support (DE&S) is responsible for the procurement and support of military systems. DE&S therefore has a key role in ensuring that the systems provided to MOD personnel are, and continue to be, adequately safe for their purpose. This is achieved by following a systematic process through the project lifecycle of all military systems to ensure that safety is "built in" (see Section 9). The safety case approach is the cornerstone of system safety management for MOD and it is described throughout this booklet.

Contractors who supply MOD also play an important part in providing systems which meet MOD's needs, including the need for safety. Defence Standard 00-56 is the contractual document normally used to define the broad safety management approach which MOD wants, and this should be supported by project-specific safety requirements (see Section 5.3).

The Front Line Commands will usually operate and maintain the military systems and it is their personnel who would be exposed to risk of harm. They have a crucial responsibility in managing safety and their safety systems should ensure that the intended level of safety is achieved in practice and that any shortfalls are recognised and corrected. They may need to take difficult decisions about safety risk in operational situations; the safety case should give commanders the right information to make robust judgements.

MOD's safety management system for defence equipment is underpinned by clear policy and organisation, but the key to achieving safety is competent people working co-operatively and from the earliest stage of the system lifecycle.

Key Messages
Safety is concerned with possible harm to people
To understand the safety of systems we need to understand software, human, procedural and organisational aspects as well as system hardware. Interactions with its environment and other systems also have an effect on the safety of the system
Physical safety depends on the components (what the system is) but functional safety depends on what the system does. Assessing Functional Safety requires exploratory analysis to investigate possible failures and malfunctions
Hazards are situations with potential for harm; accidents are unintended events that cause harm
Safety risk is the measure of exposure to possible human harm. Risk combines the severity of harm (how bad) and likelihood of suffering that harm (how often)
Risk is the measure that allows different safety issues to be compared for significance
Risks must be made "As Low As is Reasonably Practicable" (ALARP), but there is a threshold beyond which they are too high to be accepted in any normal circumstances
The user must be involved in safety management throughout the system lifecycle, from setting appropriate safety requirements to managing residual risk and feeding back information on problems in service use

2.1 General

The terminology of safety management includes several words with vague or interchangeable meanings in everyday usage. This section includes definitions of terms such as hazard, risk and accident so that readers can understand the concepts within safety management and risk management. It also introduces the concept of functional safety (sometimes called systematic safety).

2.2 Safety

Safety may be defined as "the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment" (International Electrotechnical Commission - IEC). The injury or health damage referred to here may be immediate or longer term (e.g. from radiation, noise exposure or environmental damage) and it may be acting on an individual or groups of people.

Although safety is concerned with harm to people, other forms of loss such as asset damage, loss of capability, financial costs or environmental impacts are often considered at the same time (material loss for warfighting equipment is an operational risk and MOD may wish to consider this together with safety. Costs of material loss must be considered along with safety and other impacts when judging the costs and benefits of risk reduction options). The MOD uses the Acquisition Safety and Environmental Management System (ASEMS) for all its acquisition projects and this allows safety and environmental protection to be considered in an efficient way (see Section 9.2).

The definition of safety introduces the concept of risk and the idea that some level of risk might be tolerated. Both are considered below.

2.3 What a System Includes

When considering safety, it is vital to recognise that a system includes more than just the equipment hardware. Safety management must cover the software, human, procedural and organisational aspects as well as the system hardware.

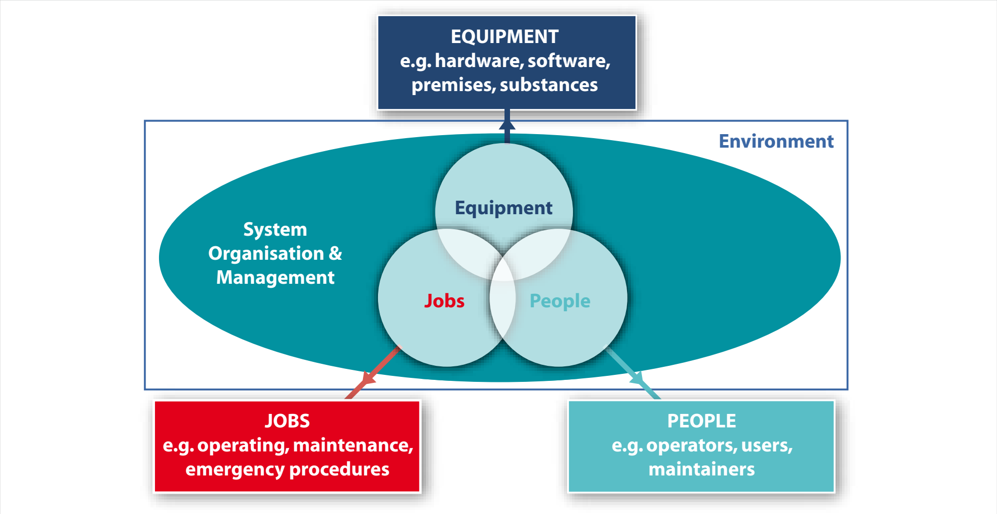

EQUIPMENT
e.g. hardware, software, premises, substances
Environment
System Organisation & Management
Equipment
Jobs
People
JOBS
e.g. operating, maintenance, emergency procedures
PEOPLE
e.g. operators, users, maintainers

Figure 2: A System includes more than just hardware and software

A **system** can be defined as "a combination of physical components, procedures and human resources organised to achieve a function" (Fig 2). This idea that a system is intended to achieve a function leads on to the concept of functional safety discussed below.

The system cannot be considered in isolation from its environment. Assessments must cover how the system interacts with its environment, including the physical environment (e.g. location, weather, vibration) and also the other systems and utilities with which it interfaces. These all have an effect on the safety of the system of interest.

2.4 Physical and Functional Safety

Physical safety concerns issues such as:

- The working environment - noise, lighting, temperature
- Dangerous materials and processes
- Sharp edges, hot surfaces, electrocution, irradiation
- Dropping, falling, crushing
- Fire, explosion

Physical safety aspects are usually directly recognisable by examination of the system and operating environment and they are often governed by prescriptive health and safety legislation. Physical safety issues depend on the components making up the system (**what the system is**).

In contrast, the functional safety of a system depends on the function which it is intended to perform (**what the system does**), rather than the system components. The IEC defines **Functional safety** as "part of the overall safety that depends on a system or equipment operating correctly in response to its inputs". Failure, malfunction or poor performance of the system can lead to safety problems which depend on that function. This means that safety problems may not be directly identifiable without deep investigation of possible malfunctions.

It also means that an item which is "safe" in one application may be "unsafe" in a new application where it is intended to achieve a different function.

Where the function of the system is related to safety, for example an emergency shutdown system, functional safety is strongly linked to system performance and to its reliability.

Computer software is an example of something which cannot have physical safety problems (it can't electrocute, burn or deafen you directly), but it may cause severe safety problems, depending on its function.

Functional safety is generally not well understood. Because its assessment requires exploratory analysis, functional safety cannot be assured just by complying with prescriptive legislation and regulations.

Because MOD has a wide range of complex systems which are required to perform critical functions, there is probably a greater variety of functional safety issues than for any other organisation or industry.

The same processes of risk assessment and safety management should be applied to both physical safety and functional safety, even though they require different analytical techniques.

2.5 Hazards

A **hazard** can be defined as "a situation with the potential for human injury, damage to property/ assets or the environment".

A hazard has the **potential** to cause harm: it is not correct to talk of something being "potentially hazardous". Parachuting does not just become hazardous when the parachute fails and the person hits the ground, it always has the potential for harm.

Some examples of hazards are:

- A cloud of toxic gas
- An exposed high voltage cable
- Loss of radar coverage for air traffic control
- Corruption of IFF (Identification Friend or Foe) data

Physical safety hazards are often already present in the system: functional safety hazards usually require an initiating event (e.g. a failure or an operator error) to put the system from a safe to a hazardous condition.

Once a hazard exists, it does not always turn into an accident and cause harm. Hazard control is concerned both with preventing the hazardous condition from happening and with stopping it from becoming a accident.

It is very important to identify all the hazards which might possibly arise during the life of a system. Clearly, unidentified hazards cannot be assessed and control measures won't be put in place.

2.6 Accidents and Incidents

An **accident** is defined as "an unintended event or sequence of events that causes harm" (Def Stan 00-56). The accident is the undesired outcome, rather than the initiating event or any intermediate state.

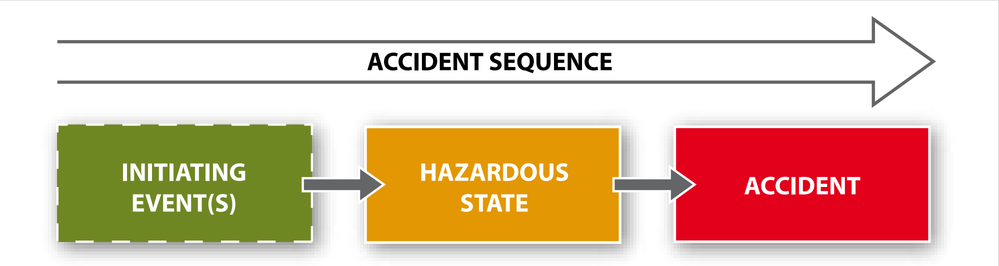


Figure 3: An Accident Sequence

Fig 3 shows with the dotted box that some hazardous states require an initiating event before they exist, but not others. Similarly, a hazardous state won't always lead to an accident, but if it does, this constitutes an "accident sequence". If the sequence is broken at any point, then there won't be an accident and the "accident sequence" is not complete.

An **incident** is defined as "the occurrence of a hazard that might have progressed to an accident but did not" (Def Stan 00-56). "Near misses" are one type of incident and it is often only due to chance that these events did not have harmful consequences. There are usually many more incidents than accidents and both can provide information on ways to improve safety.

2.7 "How Safe is Safe?"

"Is this system safe?" It's a very easy question to ask, but almost impossible to answer in a simple and understandable way. A good starting point to try to answer the question is to look at the safety records for a range of causes (Table 1) and for various industry sectors (Table 2) (the figures are taken from the HSE publication Reducing Risks, Protecting People, dated 2001).

Cause	Annual Risk of Death (over entire population)
All causes	1 in 97
Cancer	1 in 387
Injury and poisoning	1 in 3,137
All types of accidents and all other external causes	1 in 4,064
All forms of road accident	1 in 16,800
Lung cancer caused by radon in dwellings	1 in 29,000
Gas incident (fire, explosion, CO poisoning)	1 in 1,510,000
Lightning	1 in 18,700,000

Table 1: Annual Risk of Death for Various Causes

Industry Sector	Annual Risk of Death
Fatalities to employees	1 in 125,000
Fatalities to the self employed	1 in 50,000
Mining and quarrying of energy producing materials	1 in 9,200
Construction	1 in 17,000
Extractive and utility supply industries	1 in 20,000
Agriculture, hunting, forestry and fishing (not sea fishing)	1 in 17,200
Manufacture of basic metals and fabricated metal products	1 in 34,000
Manufacturing industry	1 in 77,000
Manufacture of electrical and optical equipment	1 in 500,000
Service industry	1 in 333,000

Table 2: Annual Risk of Death from Industrial Accidents

The figures in Tables 1 and 2 are historical averages and can be used to provide a framework against which to judge other quoted probabilities of death. When safety studies produce numerical values they should be treated with caution, since they are only a forecast of what might happen. It is sensible to look at the accuracy of the input numbers and the confidence in the approach (have all credible accident causes been considered?), rather than taking the numbers as representing fact.

It is also important to remember that the figures in Table 2 represent the **total** risk from industrial accidents. Safety assessments are often looking at just one system as a source of risk. Workers may be exposed to several different sources of risk in their working year, and so individual systems should present only a fraction of the total risk that is considered "tolerable".

Accidents are undesired, so time and money are spent trying to make sure that they don't happen or that they don't have serious consequences. But where should that effort be aimed and how far should we go ? This brings us to the concept of safety risk and the process of risk management.

2.8 Risk, Tolerability and ALARP

The term "risk" is used in many contexts but generally it relates to exposure to possible loss. Commonly used risks include:

- **Business risks** such as the financial risk of having insufficient cash flow or the legal risk of being sued
- **Insurance risks** such as the risk of theft, damage to property or unexpected medical bills on holiday
- **Investment risks** such as the risk of losing one's capital by investing in shares whose value goes down
- **Project risks** such as the timescale risk of a project slipping behind the planned schedule, the financial risk of it being over budget or the technical risk of being unable to achieve the required performance
- **Safety risks** which relate to the occurrence of accidents that harm people

Safety risk is often connected with other sorts of risk: an accident can affect insurance and business risks. Good safety management will reduce project risk for systems requiring safety certification prior to use.

Because the term "risk" can be used in so many different contexts, it is a good idea to use "safety risk" if there is any chance (or risk !) of misunderstanding. As this booklet deals with safety, from here on "risk" means the "safety risk".

The concept of risk starts from the premise that perfect safety (i.e. complete freedom from all harm) is not achievable for all but the simplest real-life systems. Risk is the measure which allows different safety issues to be compared according to how significant they are.

Although an individual who is killed is probably not concerned whether he dies alone or with 100 other people, it is important that assessments of risk should take account of the number of people affected. This leads to the concepts of individual and societal risk.

- **Individual risk** is defined by the Institution of Chemical Engineers (IChemE) as "the frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards."
It is usually assessed for the most exposed or a typical average person in the group of people at risk.
- **Societal risk** is defined by the IChemE as "the relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realisation of specified hazards." It therefore takes account of the number of people affected by an accident.
- Assessment of risk should cover both individual and societal risks.

Risk is a combination of the severity of the harm (how bad) and the probability of suffering that harm (how often). Risk therefore relates to accidents (the events causing harm) rather than hazards (the situations with potential for harm). This is often misunderstood and risks are evaluated incorrectly for identified hazards instead of for the harmful outcomes.

The measure or units of the risk must be defined in the most meaningful way for each system. This is done by answering two questions, namely:

- **Risk of what?** - the undesirable consequences (e.g. number of fatalities, number of accidents)
- **Per what?** - the unit of exposure (e.g. per year, per mile, per flight)

For example, the following Table, again using figures from the HSE's *Reducing Risks, Protecting People publication,* lists historical average risks of death for various activities.

These are expressed in units of risk exposure that are relevant to each activity. Using other units, such as "per passenger km" or "per flight", it can be possible to change the apparent safety of different modes of transport. Care must therefore be taken when choosing and interpreting the units for risk.

Activity	Average Risk of Death
Maternal death in pregnancy (direct or indirect causes)	1 in 8,200 maternities
Surgical anaesthesia	1 in 185,000 operations
Scuba diving	1 in 200,000 dives
Fairground rides	1 in 834,000,000 rides
Rock climbing	1 in 320,000 climbs
Canoeing	1 in 750,000 outings
Hang-gliding	1 in 116,000 flights
Rail travel accidents	1 in 43,000,000 passenger journeys
Aircraft accidents	1 in 125,000,000 passenger journeys

Table 3: Average Risk of Death for Various Activities

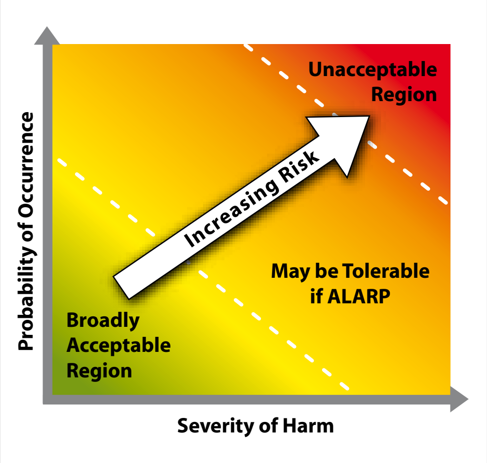

Unacceptable Region
Increasing Risk
May be Tolerable if ALARP
Broadly Acceptable Region
Probability of Occurrence
Severity of Harm

Figure 4: Risk as a Combination of Severity and Probability

Figure 4 shows two risk lines which are the boundaries between the green/amber and amber/red regions. These define the highest level of risk deemed to be broadly acceptable, and the threshold of unacceptable risk. In the red region beyond this threshold, risks must be driven down, as they are too high to be tolerated in any normal circumstances.

In the green region the risk is so low as to be considered "broadly acceptable".

It may be decided to put up with (tolerate) risks in the amber region but they must be justified on a case-by-case basis as being "As Low As is Reasonably Practicable" (ALARP). As well as these "Single Risks" being controlled and made ALARP, the overall risk faced by individuals and groups must be considered and made ALARP.

ALARP criteria may be defined to allow a judgement of how much risk reduction is practicable in the "ALARP" region. This can include balancing the costs of reduction measures against expected risk reduction, benefit in money terms, to correctly target risk reduction resources. This involves placing a financial value on human lives, injuries or environmental damage, and so can be an emotive matter.

For each identified hazard, measures must be taken to reduce the risk, either by cutting the chances of accidents happening or by decreasing the severity of the consequences. Control measures further back in the accident sequence are preferable: it is better to eliminate a hazardous substance or process than to find ways of controlling them. Risk reduction measures should therefore be applied in order of precedence and this is discussed further in Section 6.3.

2.9 Risk During Times of Conflict and Training

During recent conflicts a significant proportion of the casualties have been caused by accidents, in addition to those due to enemy action. Safe equipment, working practices and a safe environment are key force protection measures which must be provided to maintain operational capability. The Secretary of State for Defence's policy statement on safety and environmental management states:

> *"… in the acquisition of materiel and equipment of all kinds, safety and environmental management begins at the requirement definition stage and is carried forward through life to disposal. This includes all aspects of maintenance and operation."*

The aim for safety management applied to military operations should be to assess the likely hazards in advance and to have appropriate control measures and risk management integrated into military planning. Safety continues to be important during times of conflict. Safety assessment should provide commanders with systems which are safe for their military role, and with information to enable them to make good decisions when on operations.

For military equipment, performance and reliability become part of the safety characteristics when used operationally. Although equipment will be used in peaceful ways for most or all of its service life, it must be made safe enough to provide the capability required when it is needed.

The user must be involved in safety throughout the lifecycle, from setting appropriate safety requirements through to managing residual risk and feeding back information on changes of capability requirement, desired changes of use or problems in service. As it is the service personnel who will be exposed to most safety risks in service, they must have a major role in saying what level of risk they will be prepared to tolerate for the benefits which the new equipment will provide.

Risk assessment applied to military operations is particularly difficult: even if the consequence severity can be estimated, the frequency aspects of risk depend significantly on the action and capabilities of opposing forces. The assessment may ignore frequency, but should aim to show that *"all that is reasonably practicable"* has been done to reduce the harmful consequences.

Safety cases for military systems may be more challenging than those for civilian facilities. Even complex industrial systems are usually designed to achieve a simple aim (e.g. generate electricity) and operate in well defined ways. Military equipment must often be flexible; equipment may be organised and re-organised into complex "systems of systems" to achieve different goals, or capability

People should only be exposed to safety risks if a benefit is expected to result and the risks are adequately controlled. In military operations, there can be severe penalties attached to a reluctance to carry out an operation just because it is "unsafe". Thus the peacetime concept of balancing risk against benefit, may be transformed in operational missions to encompass risk against counter-risk. The benefits may not be visible where the risk exposure occurs and the command structure must ensure that competent, experienced and well-informed people are in the decision-making role. Such decisions are taken by operational commands and are not within the scope of the Acquisition Safety Management System, although they may be influenced by information from that SMS.

Equipment procured as an Urgent Operational Requirement (UOR) is needed to satisfy an operational imperative. Safety management activities are still necessary and may have to be done in compressed timescales.

Often the UOR Capability is needed to drive down the risks faced by military personnel on operations. Having that capability available is therefore part of making their risk exposure ALARP.

In wartime the risk of damage to equipment or injury to personnel is increased by the actions of the enemy (military risk). This additional risk must be factored into the risk analysis by the military commander in determining whether it is sensible to take additional safety risk to achieve the military objective and mission.

Realistic training is itself a risk reduction measure, designed to maximise fighting capability in military operations. Legislation recognises that safety risks may be tolerated, provided that they are reduced "so far as is reasonably practicable". The standard of what is considered "reasonably practicable" can be justified as being different from normal civilian activities, when applied to operational training and particularly to military operations.

Safety management is the MOD's principal risk reduction process to protect personnel. To achieve this, safety management must be a routine part of planning and executing operational missions.

3. Safety Responsibilities and the Law

Key Messages
There are moral, legal and financial reasons why MOD has to strive to make its equipment safe throughout the lifecycle
MOD and other UK employers have a legal duty to provide a safe place of work, safe equipment and safe ways of working
All employees have legal duties to take care of their own health and safety and others they might affect
Manufacturers and others have legal duties to ensure that the articles they supply for use at work are designed and constructed to be safe
Many of the legal duties for health and safety recognise that the risk of harm must be balanced against the cost (in money, time and trouble) of taking measures to reduce risk
MOD has a written policy for health and safety and a formal system of delegating authority for safety management tasks to those best placed to do them

3.1 Why is Safety Important to the MOD?

People in the armed forces know that they may have to face grave danger, so why is safety so important to MOD?

As an employer MOD has moral and legal responsibilities to its employees and to other people who could be affected by its activities. Although MOD is not a manufacturer of equipment, it is closely involved in the process of design, development, manufacture and maintenance.

The safer the equipment which MOD procures for use by the armed forces, the more readily can the MOD comply with its legal responsibilities as an employer.

Accidents can damage organisations as well as people, by affecting morale, costing money and harming their reputation. For MOD, accidents may also affect capability and force protection. Effective safety management safeguards military capability and so has benefits for the general population, as well as people most directly affected by accidents.

There are therefore very sound moral, legal and financial reasons why the MOD should make every attempt to ensure that the equipment which it procures, operates and maintains, is safe throughout all the stages of its life cycle.

3.2 Legal Responsibilities

There are two types of legal duty relating to safety at work: the statutory duties as set out in the Health and Safety at Work etc. Act 1974 (HSWA) and common law duties. Common law has developed over time as a result of decisions made by judges in court.

The HSWA 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 following paragraphs summarise the duties under the HSWA but should not be taken as providing definitive legal guidance or interpretation. Further advice is available from MOD's Safety Management Offices (SMOs); contact details are given at the end of this booklet.

Employers' duties. Under the HSWA, employers have to provide the people working for them with a safe place to work, safe equipment to work with and safe ways of doing work.

Employers also have to ensure, so far as is reasonably practicable, that persons other than their employees (including members of the general public) are not adversely affected by their activities (Section 3 HSWA).

Employees' duties. Employees have a duty to:

- Take reasonable care of the health and safety of themselves and others who may be affected by their work activities
- Co-operate with their employers and others to enable them to comply with any duties laid upon them by statutory provisions (Section 7 HSWA)

There is also a duty laid upon everyone (employees, visitors and even trespassers) not to intentionally or recklessly interfere with or misuse anything provided in the interests of health, safety or welfare in compliance with health and safety statutory provisions (Section 8 HSWA).

Manufacturers' and others' duties.
Manufacturers, suppliers, importers and designers of articles (which includes equipment) for use at work must, 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 (Section 6 HSWA)

The Standard "So Far as is Reasonably Practicable". Many of the duties listed above are qualified by the statement "so far as is reasonably practicable". In case law (i.e. founded on previous legal rulings) this has come to mean that the degree of risk of injury or adverse effect must be balanced against the cost in terms of money, time and physical difficulty of taking measures to reduce the risk. If the risk of injury is insignificant compared to measures needed to attenuate the risk, then no action need be taken to satisfy the law. However, the greater the risk, the more likely it is that one will be required to use substantial resources to do something about it, because courts will consider such measures to be "reasonably practicable".

In the HSWA and in some regulations, stricter standards may apply, setting out what **must** be done and what **cannot** be done. For example, some regulations use the phrase **"all practicable means"** and this signifies that everything possible must be done, regardless of the costs of doing so.

3.3 Regulations, Guidance and EC Directives

The HSWA sets out the general duties which employers have towards employees and members of the public, and employees have to themselves and to each other. These duties are qualified in the Act by the principle of *'so far as is reasonably practicable'.* In other words, an employer does not have to take measures to avoid or reduce the risk if they are technically impossible or if the time, trouble or cost of the measures would be grossly disproportionate to the risk. What the law requires here is what good management and common sense would lead employers to do anyway: that is, to look at what the risks are and take sensible measures to tackle them.

The HSWA is also an enabling Act, allowing for the making of health and safety regulations (Section 15 HSWA). Regulations are law issued under the HSWA where the Health and Safety Executive (HSE) consider that the risks are so great, or proper measures so costly, that employers should not be allowed discretion. For example there are regulations for controlling noise at work, controlling exposure to radiation and exposure to substances harmful to health.

Regulations are supported by Guidance and sometimes by an Approved Code of Practice (ACoP). Both are prepared by the HSE and issued by the Health and Safety Commission (HSC) and both provide practical guidance on HSWA or its Regulations. However they differ in legal status as follows:

- **Guidance** has no legal status and is therefore not compulsory although compliance with guidance is normally sufficient to comply with the law.
- **Approved Codes of Practice** give advice on how to comply with the law; they represent good practice and have a special legal status. If duty-holders are prosecuted for a breach of health and safety law and it is proved that they have not followed the relevant provisions of the ACoP, a court will find them at fault unless they can show that they have complied with the law in some other way. Following the advice in an ACoP, on the specific matters on which it gives advice, is enough to comply with the law. Safety standards have a similar effect in law to ACoPs.

The Highway Code is an example of an ACoP: it is not part of the law, but you should have a very good reason for not following its direction if you want to avoid prosecution.

EC Directives are binding on each member state but they are implemented in UK law through regulation if necessary.

Other Legislation Account must also be taken of the requirements of system-specific legislation such as:

- The Merchant Shipping Act
- The Civil Aviation Act
- The Road Traffic Act

3.4 Supply Law, User Law and CE Marking

The law on buying new machinery (normally regarded as being a piece of equipment which has moving parts and, usually, some kind of drive unit such as fork-lift trucks, metal working drills and escalators) is broadly split into **supply** law and **user** law. Supply law deals with what manufacturers and suppliers of new machinery have to do. The most frequently encountered supply law is the Supply of Machinery (Safety) Regulations 2008 which require manufacturers and suppliers to ensure that machinery is safe when supplied and to fix CE marking to it. Manufacturers have to:

- Ensure that machines they make are safe, through hazard identification, risk assessment, removal of hazards, controls on remaining hazards and warning signs
- Keep a **technical file** of information explaining what they have done and why
- Fix **CE marking** to the machine where necessary, to show that they have complied with all the relevant supply laws
- Issue a **Declaration of Conformity** (covering name and address of manufacturer; make, type and serial number of the machine; signature of an authorised person and information on which standards (if any) have been used in the design and manufacture, what EU laws the machine complies with and what the machine is intended for)
- Provide the buyer with **instructions** explaining safe installation, use and maintenance

Supply law does not apply to certain special categories of machinery such as firearms, pressure vessels, Military and Police equipment and nuclear equipment. Many of these categories will have specific legislation and standards that apply to them.

User law deals with what the users of machinery and other equipment have to do. The most frequently encountered is the Provision and Use of Work Equipment Regulations (PUWER) 1998. These require employers to:

- Provide the right kind of safe equipment for use at work
- Ensure that it can be used correctly
- Keep it maintained in a safe condition

HSE stress that CE marking is only a **claim** by the manufacturer that the machinery is safe and that they have met the relevant supply law. The user also has a legal duty under PUWER to check that it is, in fact, safe and complies with all the supply law that is relevant.

3.5 MOD Policy

The HSWA requires employers to produce a written statement of their policy for the health and safety of their employees at work.

The Secretary of State for Defence has overall responsibility for health and safety throughout the MOD and produces a statement of safety and environmental policy which is published in JSP 815. In summary, the policy is that:

- Within the UK we comply with all legislation which extends to the UK (including legislation giving effect to the UK's international obligations)
- Overseas we apply UK standards where reasonably practicable, and in addition, comply with relevant host nations' standards

The policy states that where Defence can rely on exemptions or derogations from either domestic or international law, we introduce standards and management arrangements that are, so far as reasonably practicable, at least as good as those required by legislation.

Additionally, the statement notes that we seek to disapply legislation on the grounds of national security as far as possible only when such action is absolutely essential to maintain operational capability, or in accordance with applicable laws. Where there is no relevant legislation, our internal standards aim to optimise the balance between risks and benefits. The statement notes that this does not mean avoiding risks but managing them responsibly, on the basis of impact and likelihood.

The policy statement contains a list of strategic principles, in which the Secretary of State requires MOD to:

- Avoid work-related fatalities and minimise work-related injuries and ill-health
- Maintain effective emergency arrangements
- Protect the environment
- Deliver against the government's sustainable development commitments

3.6 Delegation of Safety Tasks Within MOD

MOD has a system of "Letters of Delegation" which serve to delegate down the management chain the authority for carrying out safety and other management tasks and to define their scope. At the highest level, the delegation starts from the Secretary of State and it will normally be passed down to individual project team leaders, project managers (PMs) or commanders. Below that level, the process can be continued, where necessary, through an individual's job description, terms of reference or further letters of delegation.

A letter of delegation is not a legal document and cannot **transfer** legal responsibility for safety. In health and safety law, the employer cannot transfer the legal responsibility for carrying out duties which the HSWA says are the employer's: the letter of delegation transfers **authority** rather than **responsibility.**

As for any delegation of work, the person delegating the authority must:

- Ensure that the person tasked is competent (see Section 4.1) to undertake the task
- Provide the necessary resources
- Continue to monitor the progress of the task

The person thus tasked must:

- Report back on progress
- Identify shortfalls in achievement or necessary resource

Key Messages
Organisations and individuals responsible for safety activities must be "competent" for those tasks. Competence includes skills, experience, qualifications and also fitness at the time
Competence management schemes allow organisations to define requirements for different roles and to assess and improve the competence of people assigned to those roles
A strong "safety culture" encourages safety through values, attitudes and behaviour shared throughout an organisation
A key part of an effective safety culture is a just culture in which individuals are not unduly blamed for their mistakes
Information from real accidents and incidents gives a chance to learn about problems and to improve safety
There are more near-misses and minor accidents than major ones. They all give opportunities to learn about problems, and so they should be investigated to learn about their immediate and underlying causes
Safety can degrade over time as people become complacent and less vigilant. The management system must be stimulated through audits, reviews, working groups etc to ensure that safety performance will continuously improve

4.1 Safety Competence

Many UK safety regulations require use of a "competent person", which is a person who has "sufficient training and experience or knowledge and other qualities to enable him properly to assist in undertaking the measures referred to." Standards such as Def Stan 00-56 and BS EN 61508 require that tasks which influence safety must be carried out by individuals and organisations that are demonstrably competent to do them. Other legislation and standards require the use of Suitably Qualified and Experienced Persons (SQEP).

Competence to undertake safety-related work has several aspects including:

- Skills and knowledge
- Experience of applying those skills and knowledge
- Experience of the relevant domain or sector and technology
- Relevant qualifications
- Attitudes and behaviours (e.g. team working and integrity)
- Fitness (physical, medical and mental)
- Appreciation of one's own limitations

A person who is "competent" in one role may not be competent in a different role, for example if the technology is different or if the system has a safety function. Also, an individual may not be competent, even if they have the necessary qualifications and experience, for example if they are exhausted.

There are safety competence schemes for managers and engineers involved with safety-related systems. These allow organisations to define the requirements for different roles and to assess and improve the competence of people assigned to those roles. Competence can be improved by training and by practical application under supervision. Evidence that people and organisations are competent provides some assurance that their work and decisions relating to safety are good and so forms part of the safety case.

4.2 The Culture of Safety

Safety culture is defined as "the product of individual and group values, attitudes, perceptions, competences, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management." (UK Health and Safety Commission).

Safety should be the concern of the MOD organisation and the individuals within it. A "safety culture" is the attitude that exists when everyone recognises and accepts their responsibilities for safety, and the organisation "thinks safety" as a matter of course.

4.3 A Just Culture

Safety culture requires an atmosphere in which individuals are not unduly punished or blamed for their mistakes. This is an ideal which is difficult to achieve in practice; when things really do go wrong, people's reaction is often to protect themselves by pointing the finger of blame at others.

An organisation that strives to achieve a just culture is still subject to rules and legal regulation. A "just" culture is one in which individuals are not free of blame if they are culpably negligent and where the organisation seeks to balance accountability with learning from mistakes. Such an attitude works well in industries like air transportation where it has helped to encourage a free flow of safety information. Errors and mistakes are inevitable, and safety can only be improved if the organisation can learn from its mistakes.

4.4 Incident and Accident Reporting and Investigation

A key part of safety management is measuring performance to know how safe the organisation's equipment and operations are, and to identify problem areas for improvement. Information on real accidents and incidents, whether or not they actually caused damage, gives a chance to learn about actual problems and to improve safety.

Information from accidents and incidents provides a direct measure of the safety performance in real usage and is vital for understanding the actual risk exposure and updating forecasts of risk. Although incident data provides a "lagging indicator" for safety, it provides the most relevant information to refine the "leading indicators" from audits, inspections etc. Incidents may highlight hazards that weren't recognised before or they may show that the previous understanding was incomplete.

People should be encouraged, without threat of disciplinary action, to report equipment failures, design faults or procedures which might cause a hazard. Each incident provides potential for learning and it is important that events are not dismissed quickly as one-offs.

Studies from a range of industries have shown that there is consistently a much greater number of less serious incidents than those which led to an injury. Often it was only a matter of chance that these near misses or non-injury accidents didn't harm people. Figure 5 illustrates the "iceberg" of accident and incident statistics, where the large bulk of learning opportunities lie below the surface of obvious accidents.

For accidents and incidents to be used to improve safety and to measure safety performance, they must be recorded, investigated and the lessons learned. An effective system of incident investigation requires the following:

- The incident must be recognised as being relevant to safety
- It must be easy for people to report and record the necessary information (what, where, when, who etc.)
- Knowledgeable people should investigate the incident (how and why did it happen?) and determine the causes, both immediate and underlying

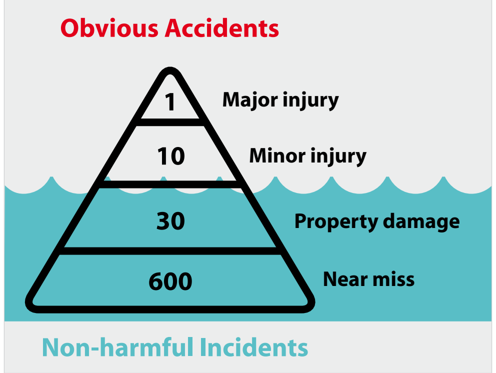


Figure 5: The "Iceberg" of Accident and Incident Statistics

- Where necessary, recommendations must be made to improve safety (e.g. change the design, procedures, training, contingency arrangements)
- There should be follow-up to see whether the improvements have worked or similar incidents have happened again

The investigation should try to find all the causes of an incident as illustrated in Figure 6.

Incident data can be used to monitor in a qualitative or quantitative way the safety performance of equipment and systems. To do this, the recording systems must be specific about which equipment was involved in each safety incident, and data must be available on how much the equipment has been used.

There are reporting and investigation procedures within MOD for material defects, incidents and accidents. It is important that these are used and the information is fed back to the project team and design authority, where they exist.

4.5 Continuous Improvement

The safety achievement of a system is not static and it will usually tend to degrade over time as people become complacent and less vigilant. Monitoring and feedback are therefore required to maintain or improve the safety performance.

There are several ways of achieving the safety management goal of continuous improvement. These include both active and reactive methods such as the following:

- Incident reporting, investigation and feedback (see above) - reactive
- Safety reviews and audits - active
- Safety working groups and safety committees - active and reactive
- Suggestion schemes which cover safety - active

Safety management must not be viewed as a one-off exercise: people should be continuously trying to make things safer. A strong safety culture, with the necessary stimulation from reviews, audits, incidents and suggestions, will ensure that safety improves.

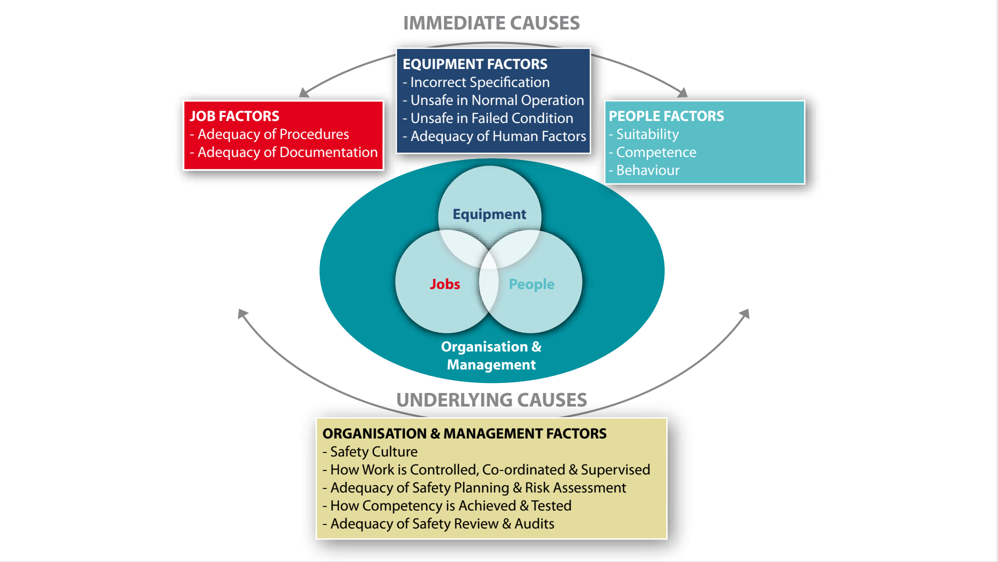

IMMEDIATE CAUSES
EQUIPMENT FACTORS
- Incorrect Specification
- Unsafe in Normal Operation
- Unsafe in Failed Condition
- Adequacy of Human Factors
JOB FACTORS
- Adequacy of Procedures
- Adequacy of Documentation
PEOPLE FACTORS
- Suitability
- Competence
- Behaviour
Equipment
Jobs
People
Organisation & Management
UNDERLYING CAUSES
ORGANISATION & MANAGEMENT FACTORS
- Safety Culture
- How Work is Controlled, Co-ordinated & Supervised
- Adequacy of Safety Planning & Risk Assessment
- How Competency is Achieved & Tested
- Adequacy of Safety Review & Audits

Figure 6: Immediate and Underlying Causes of Accidents

Key Messages
System-specific safety requirements set early in a project lifecycle should drive the development to satisfy the needs of stakeholders
Safety management is most successful when there is good engagement with stakeholders from an early stage of the lifecycle
The project safety committee provides the forum for decision-takers to hold safety discussion with stakeholders, with support, where necessary, from subject matter experts
Safety monitoring and audits are used to ensure that the "safety system" does not decay, but is stimulated

5.1 Who Manages Safety?

"The results of successful health and safety management are often expressed as a series of negative outcomes, such as absence of injuries, ill health, incidents or losses" (HSE).

To contribute to "negative safety outcomes" a healthy and active Safety Management System (SMS) is essential. This will ensure that safety aims, objectives, managerial responsibilities and technical tasks are clearly understood and that the organisations responsible for their implementation are defined.

Even where organisations have a nominated safety manager, the "safety culture" means that all staff will still think about safety issues and contribute towards achieving safety, rather than treating it as that manager's exclusive responsibility.

5.2 Pre-requisites to Successful Safety Management

Successful safety management requires that organisations and project teams must follow good practices in areas such as:

- Quality
- Configuration management
- Use of Suitably Qualified and Experienced Personnel (SQEP)
- Management of corporate and project risk
- Design reviews
- Independent review
- Closed-loop problem reporting and resolution
- Focus on safety culture

5.3 Setting Safety Requirements

One of the most difficult elements of the safety process is setting the level of required safety risk for the system in both peacetime and wartime. This should be based on the ***ALARP*** principle for tolerating risks to service, contractor or third party personnel and to the environment.

The application of the ALARP principle to MOD systems is not straightforward. Individual projects will be guided by departmental safety policy but must develop and record their own justification for the targets and criteria which they use.

The safety requirements should also consider the influence of the operating context (or environment) on the consequences of Hazards for the system. For example, this system may be part of a wider "system of systems" whose performance and ability to mitigate or prevent consequences, must be taken into account.

The requirements for safety will vary according to the system size, function, or role, but will include one or more of the following:

- Legal and regulatory requirements
- MOD certification requirements
- Safety related standards
- MOD policy or procedural requirements
- Risk targets (quantitative and qualitative)
- Safety integrity requirements
- Design safety criteria

Legal and Regulatory Requirements

Legal requirements and regulatory safety requirements are based upon UK statutory and regulatory safety requirements. These may or may not be applicable for a military system, as, some regulations explicitly exclude the military and some others allow the Secretary of State for Defence to disapply legislation on the grounds of national security. This type of requirement may include absolute requirements defining the features which a system **must include** and **must exclude** for safety purposes. Examples of this are:

> *"The system shall incorporate residual current circuit breakers for all external power supplies."*
>
> *"The system shall not contain any components or devices incorporating a radioactive source."*

MOD Certification Requirements

MOD certification requirements are historical and are invoked to control the risks from particular hazardous aspects of defence equipment (e.g. explosive hazards). The requirements codify experience of how these particular hazards are best controlled.

Safety Related Standards

Safety related standards will include MOD, British, international or other applicable foreign standards. UK Armed Forces operate in different countries where statutory and regulatory requirements may not be the same as in the UK. The User Requirements Document (URD) and System Requirements Document (SRD) must cover the requirements of all proposed operational environments.

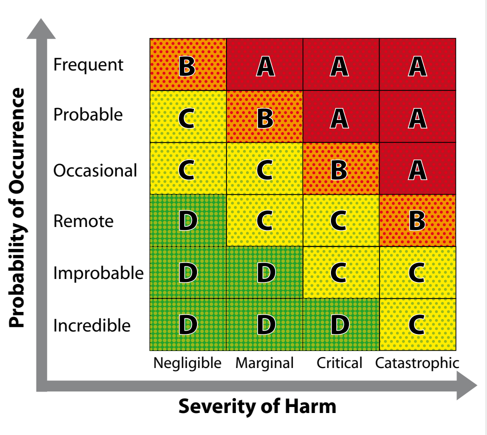
Existing equipment may have been originally assessed using a civilian or non-UK military safety standard such as US Mil Std 882. The acquisition strategy should define how any existing safety information can be used efficiently or developed to satisfy UK MOD's requirements for evidence such as the safety case or specific safety certification.

MOD Policy or Procedural Requirements

MOD policy or procedural requirements are published in relevant Joint Services Publications (JSPs). For example, there may be a requirement to comply with JSP 553 Regulations for Airworthiness, or to follow departmental safety procedures for nuclear weapons.

Risk Targets

In MOD ***qualitative risk targets*** are often based upon a Risk Classification Matrix (RCM) that has been tailored to the system. This matrix defines the framework for classifying ***accident risk*** according to its ***significance,*** which is typically defined by four qualitative levels.



Probability of Occurrence	Negligible	Marginal	Critical	Catastrophic
Frequent	B	A	A	A
Probable	C	B	A	A
Occasional	C	C	B	A
Remote	D	C	C	B
Improbable	D	D	C	C
Incredible	D	D	D	C

Probability of Occurrence
Severity of Harm

Figure 7: A Risk Classification Matrix

The Risk Classification Matrix in Figure 7 is a version of the risk diagram illustrated in Figure 4, but where the continuum has been broken down into chunks. Use of a matrix such as this, reflects the fact that you don't have to know exactly where on the diagram a risk lies: even an approximate position shows how important it is and this can be used to prioritise issues for action and for more detailed assessment where necessary. A matrix is intended to give a broad indication of significance: the most important risks should be analysed in detail (see Section 8 on techniques) and this would typically include possible accidents with very severe consequences (e.g. multiple fatalities). A matrix will help to identify the most significant risks on which the safety case should concentrate, but it will not usually be the only form of assessment for those risks.

The letter in each area defines a risk class (A, B, C or D), each of which has a particular level of authority for acceptance. Class A risks represent a very high level of risk, which can only be tolerated under truly exceptional circumstances.

The tailoring process for safety requirements includes the definition of the severity and probability bands for the particular system, together with the choice of relevant units for frequency.

Quantitative risk targets address the likelihood of occurrence of specific identified accidents during the lifetime of a system or the total risk to which individuals or groups may be exposed.

Figure 8 has a graph showing the average annual risk of dying for males in the UK, and how this varies with age. HSE figures show that the fatality rate is at its lowest, approximately 1 in 5,000 per year, for boys aged between 5 and 14. It is in this context that we can appreciate HSE's tolerability limits for the public who have a risk imposed on them. The upper limit of 1 in 10,000 per year (or 1 E-04) is some half of the total average risk that people face and any **additional** risk of this scale will be considered unacceptable. Conversely, additional risk which is less than 1/100 of this level is so small in comparison with the background risk, that it is considered to be "broadly acceptable".

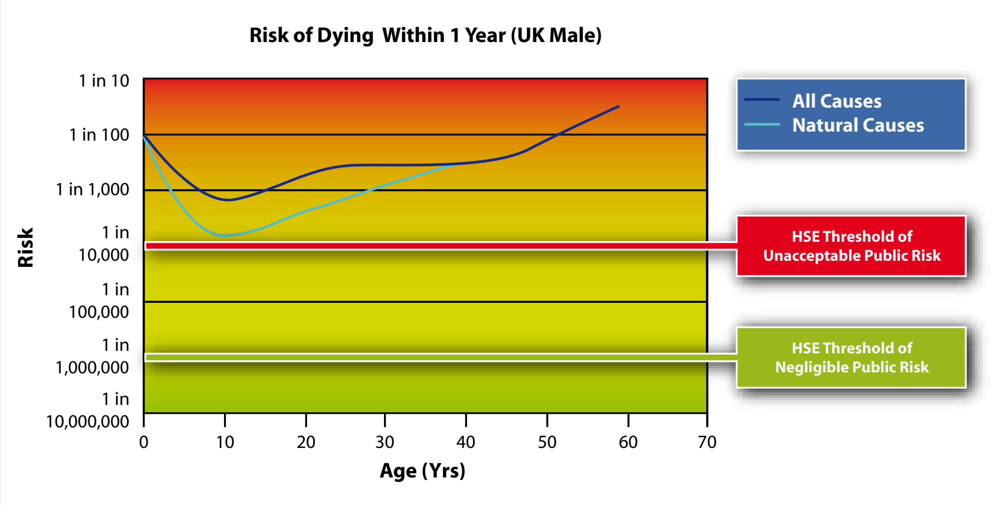


Figure 8: Risk Thresholds Compared with Average Fatality Rates

Quantitative risk targets should be chosen to provide a measurable approach to the achievement of safety. Unrealistic or unmeasurable safety targets do not contribute to the safety process and can lead to unnecessary project expense or an inability to verify that the requirements have been met.

Quantitative safety targets should be uniquely set for a specific system according to its function and nature and should be recorded in the Safety Management Plan (SMP). They may be based upon historical knowledge of similar systems, or based on the results of a ***Preliminary Hazard Analysis,*** or based upon engineering judgement, or a combination of all three.

During a project lifecycle, several iterations of the safety case will be required for the system to pass major project milestones such as Initial Gate, Main Gate, System Acceptance and introduction of a mid-life update. These milestones will provide the measurement points at which the achievement of safety requirements by the system can be confirmed.

As the work in the safety programme proceeds, there is a natural increase in knowledge which offers the opportunity to refine the safety targets.

Safety Integrity Requirements

Safety integrity requirements are about protection of the system against dangerous failures. Safety integrity includes aspects like reliability, availability, robustness, and timeliness, as well as a measure of confidence in these properties. An example safety integrity requirement is:

> *"The shutdown function shall have a probability of failure on demand of less than 1 in 1,000, at 90% confidence."*

Integrity covers both random and **systematic** failures, which are those which occur repeatably, given a particular combination of inputs or under specific environmental conditions. A system event that is not caused by a random event is, by definition, a systematic event, so all software failures are systematic events.

Safety integrity requirements are generally most relevant for **"complex electronic elements"** (software or hardware electronics) which are **"safety related"** (i.e. having any effect on the safety of the overall system). For such complex elements, failures due to specification or design faults are the main concern.

There are various standards which use **Safety Integrity Levels (SILs)** or similar concepts (e.g. Safety Assurance Levels) for a specific industry sector. For each SIL, the standards define good practice both for engineering development methods (e.g. design rules and tools) and assurance activities (e.g. type and extent of testing). The standards may also define "claim limits" for each SIL thus identifying the lowest rate of systematic failure that can be claimed for a function or component developed to that level.

Each function or component may be assigned a SIL, for example in the range S1 to S4, with the most stringent safety requirement placed at level S4 for "Safety Critical" functions (levels S3, S2, and S1 concern "Safety Related" functions.) Sometimes a fifth level, S0, is declared and assigned to software and functions that are neither Safety Critical nor Safety Related, although this is not covered in standards.

An example Safety integrity requirement using the SIL approach is:

> *"The shutdown function shall satisfy the requirements of SIL1 of BS EN 61508, using the failure on demand mode."*

Safety integrity requirements should be used by the system designers to develop a suitable architecture of sub-systems and to select appropriate technologies. Techniques such as redundancy and error tolerance may be necessary to achieve the required safety integrity. System models are typically used to help the designers to apportion the safety integrity requirements to the components implementing the function, taking account of any dependencies between the components (e.g. common mode failures). Designers should ensure that lower integrity functions cannot affect functions of higher integrity, for example by partitioning.

Use of SILs is not the only method for safety integrity assurance, and there have been moves towards an "evidence-based approach". Under such an approach, there may be less prescription of engineering development and testing methods, and greater flexibility of the types and amounts of evidence acceptable in showing achievement of safety integrity requirements.

It is vital that any quantified safety targets are stated in units which are appropriate for the system. For example, fatalities per year, accidents per flight or tonnes discharged per year. A target such as *"better than one in a million"* has no meaning until the units are defined.

Design Safety Criteria

Design safety criteria can be used by the customer or project team to indicate to the designers some principles for achieving a satisfactory design solution. Whilst these criteria should not be too constricting, they should influence the consideration of options. Some examples of design criteria include:

- Design for good Human Factors (HF)
- Design for integrity of safety functions (such as specified safety factors or safety margins, one fault safe criteria, redundancy)
- Passive control – process inherently cannot run-away
- Friendly design such as smooth control system response, tolerance of mal-operation (design for recovery), design for disposal/dismantling, clear status visible on system components (e.g. valves)

5.4 Safety Management Planning

If the safety requirements define where we want to reach, the Safety Management Plan (SMP) sets out how to reach the destination.

Both the MOD and the prime contractor will have a Safety Management Plan. Each one will deal with how their safety goals are to be reached and their resources deployed. These two plans will obviously be strongly related in terms of complementary and co-ordinated programmes of activities.

An effective planning process comprises three elements:

- Accurate information on the current status
- Suitable benchmarks against which to make comparisons
- Competent people to carry out the activities and make judgements

The Safety Management Plan will typically:

- Describe the system and any variants
- Define the system context, functionality and interfaces
- Identify safety stakeholders and subject matter experts and their roles on the project
- Describe the safety management system
- Detail the safety requirements
- Detail the programme of work, deliverables and milestones
- Identify any procedures or tools to be used
- Identify supporting resources such as safety engineers and facilities
- Describe how the SMP is to be developed as the system matures

The SMP should reflect the current stage in the system life but also include planning for the future phases.

The SMP may be integrated with other project plans to enable a coherent and co-ordinated system development, and it will form a key part of the Through Life Management Plan (TLMP).

As well as design issues, the initial SMP will address the requirements for disposal, which may happen many years in the future. In addition to system disposal at the end of its life, the SMP must cover how items will be disposed of earlier on (through life disposal), including test articles, consumables and unintended disposal (e.g. systems which are scrapped after a crash). As the end of the in-service system life approaches, the requirements within the SMP for the final safe disposal of the system will become more detailed.

5.5 Safety Committees

Safety management is most successful when the decision-takers have good engagement with stakeholders from an early stage of a project. Firstly, the stakeholders must be identified and then there should be consultation to understand their requirements. The Project Safety Committee (PSC) provides the forum for decision-takers to consult stakeholders, with support where necessary from Subject Matter Experts (SMEs).

An MOD PSC provides the safety management focus a system, equipment or group of equipments within MOD. Committee membership should include representatives from all authorities that have safety responsibilities for the system/equipment(s), typically consisting of:

- Project team personnel (e.g. project safety manager and other technical, finance and contracts officers as required)
- Head of Capability SMEs
- Front Line Command (User) SMEs
- Trials team
- Maintenance specialists
- Prime contractor and/or design authority
- Specialist advisors (e.g. from industry, MOD or independent safety specialists)
- Independent Safety Auditor (ISA) (where one is appointed)

The Front Line Command has a key role in the PSC since they have the detailed knowledge of the usage environment and their personnel will usually be the people who are most exposed to the risk of harm. It is important that the Front Line Command are represented at an appropriate level to bring relevant operational experience and to have the necessary authority for any decisions that have to be taken.

Early in a project lifecycle there is most scope to influence the development/acquisition for safety, taking account of stakeholder requirements and experience to set a good safety management strategy. The PSC should therefore be convened at project initiation, to ensure that safety aspects are correctly considered and integrated into project activities as necessary.

The PSC should co-ordinate the Safety Management Plan, develop safety requirements, and progress the production of the safety case. The composition of the PSC for system may change through the project lifecycle according to the work required at that stage.

A PSC should cover each system or equipment throughout its lifecycle, although this is often achieved through grouping together similar equipments under one committee. For smaller projects, the PSC may be integrated with other meetings but safety issues should be a separate, and permanent, agenda item at these meetings.

5.6 Safety Monitoring and Audits

There is never certainty that the risks of accident occurrence have been fully controlled or that a positive safety culture is prevalent within an organisation. The non-occurrence of system accidents or incidents is no guarantee of a safe system. Safety monitoring and safety audit are the methods used to ensure that the "safety system" does not decay but is continually stimulated to improve the methods of risk control and safety management.

In this context, both monitoring and audit apply to the total Safety Management System. Examinations of equipment and plant to identify health and safety problems are sometimes referred to as safety audits but are really inspections. They are also part of the wider process of reviewing and improving safety.

Safety monitoring of an organisation provides feedback on its safety. It should include monitoring of:

- The achievement of specific objectives
- The operation of the Safety Management System
- The compliance with Safety Requirements as defined in the Safety Management Plan

Active monitoring aims to prevent accidents, or incidents, and should be proportional to the system complexity and risk. **Reactive monitoring** responds to the occurrence of accidents and incidents. The overriding objective is to learn from mistakes and to prevent similar occurrences in the future.

Safety auditing can be defined as "the structured process of collecting independent information on the efficiency, effectiveness and reliability of the total health and safety management system and drawing up plans for continued improvement of that system".

The aims of an audit programme are to establish:

- That appropriate management arrangements are in place
- That adequate risk management systems exist, are implemented and are consistent with the accident/hazard profile of the system
- That appropriate workplace precautions are in place
- The effectiveness of policies, strategies and Safety Management Systems

Safety auditing is similar to quality auditing: both check working practices against procedures and examine records and traceability. The emphasis in quality has changed from **control** by checking the product against specification, to **assurance** through confirmation that procedures are being used throughout the process of interest. For effective safety management, it is not appropriate simply to check that no accidents are happening; progressive assurance is required.

Safety audits are not only aimed at finding weaknesses: they should also build on strengths to develop and spread the good practices already in place.

The Independent Safety Auditor. To maintain safety integrity across large and/or high risk projects, it is advisable that an Independent Safety Auditor (ISA) be appointed to ensure that MOD contracted safety requirements are being met by the contractor. The ISA should be acceptable to both contractor and the MOD, be independent of both organisations and have a good understanding of safety issues for systems of that type. The ISA must have a well defined role that is clearly understood by all parties. This role might include providing assurance by auditing Safety process being followed, or by doing some safety assessment independently to check the primary assessment. The role may change at different points through the life cycle, but the ISA's independence must not be compromised by involving them in activities such as setting safety requirements, tender assessment or providing specific advice on engineering changes.

5.7 Safety Compliance Assessment and Verification

Safety compliance assessment is concerned with checking whether the system achieves, or is likely to achieve, the safety requirements. It uses both design analysis and auditing techniques. If the requirements are not achieved, then corrective action has to be taken and the safety must be re-assessed.

Safety verification aims to provide assurance that the claimed theoretical safety characteristics of the system are achieved in practice. This will involve reviewing all safety incidents which occur and testing that safety features operate as they should.

Key Messages
It isn't possible to know when or how the next accident will happen: instead it is important to try to recognise where there are dangers, understand them and control them
Measures of safety risk should be treated as forecasts with a degree of uncertainty. Using input from people who know the system and its operation will give improved forecasts of risk
Risk forecasts should be used to focus effort and resources on the most significant risks, to have the greatest influence on safety
Risk management is required throughout the lifecycle of a project. At the early stages the management activities are mainly pro-active. When the system is in operation there is significant emphasis on re-active management as well, so that the current significant risks are recognised and managed
The hazard log is a key tool for managing safety risks: it provides traceability of how safety issues are being dealt with and resolved
Risk assessment provides information, but safety will only improve when risk reduction measures are taken
Risks must be driven down to a level that is "As Low As is Reasonably Practicable" (ALARP). There are three main approaches by which Duty Holders can argue ALARP, but the validity of this argument can only be decided definitively by the courts, should an accident happen

6.1 Introduction

It isn't possible to know when or how the next accident will happen: instead it is important to try to recognise where there are dangers, understand them and control them. Risk management needs vigilance to keep looking for new threats and an open-minded attitude to accept that our current understanding can be improved.

Risk is concerned with exposure to possible loss and because it depends on unpredictable events, measures of risk should only be treated as forecasts with a degree of uncertainty. Using the expertise and understanding of people who know the system and its operation will give improved forecasts of risk. These risk forecasts should be used to focus management effort and resources on the most significant risks to have the greatest influence on safety.

Safety risks associated with a system and its operation have to be recognised, understood and managed throughout the system's lifecycle.

During the early stages of a project lifecycle, the risk management activities are mainly pro-active; they are concerned with identifying hazards, determining how the hazards may arise, assessing the consequences and establishing how often they are likely to be realised, then deciding on how best to control their risks.

During the later stages of a project, when the system is in operational use, there is a significant emphasis on re-active management of risk as well as continuing pro-active effort. During the in-service stage there will be real operational evidence in the form of incidents, surveillance records and anecdotal experience from users and maintainers. All of this valuable information should be used to identify the current most significant risks that require attention. The "theoretical" forecasts of risk from early stages of the lifecycle should be updated with real information so that they support the ongoing risk management process.

Throughout the safety risk management process it is important that there is traceable information on how hazards and risks have been managed and why they are considered to be currently tolerable.

6.2 The Hazard Log

The hazard log is one of the most important tools for managing safety, especially in a development programme.

It is a database which contains information to show how safety issues are being dealt with and resolved. Despite the name, it deals with more than just hazards: the commonly used versions have the following 5 parts:

- Part 1: **System data** (information on build standard, usage, environment etc.) and **Safety Requirements** (legal, certification, Safety elements of the URD and SRD and tailored risk matrix - see Section 5.3above)
- Part 2: **Hazard data** (a record of every identified hazard with its description, associated causes, controls and possible accidents, how it is analysed etc)
- Part 3: **Accident data** (a record of possible accidents for the system, associated hazards and controls, target risk class, how it is analysed, assessed risk class)
- Part 4: **Statement of system safety** (the assessed risk of the system)
- Part 5: **Journal** (the running log or diary of significant events in the safety programme)

The hazard log provides traceability of how safety issues have been dealt with during a project. Outstanding issues should be regularly reviewed by the PSC to make sure that safety-related actions are completed and risks are driven down to a level which can be agreed as "tolerable and ALARP". The hazard log should help stakeholders by identifying the most important issues and tracking their resolution.

The hazard log should contain all identified hazards and accidents for the system, not only those that have happened or are considered likely. This includes those which are signed off as Closed, and those considered as not credible, such as an accident caused by a major earthquake. The hazard log will show that they have been considered and provide the audit trail of reasons why they are closed. Should the circumstances change, for example if the system is to be used in an earthquake zone, then the safety argument can be re-examined.

Figure 9 shows how the hazard log takes information from each activity in a safety programme and also provides the data input for the safety case. In fact, the hazard log can be thought of as an index to the mass of information held in the safety case regarding identified hazards and accidents.

The hazard log will normally be implemented as some kind of computer database. For low complexity systems with few risks it may be appropriate to maintain the database using Word or Excel, however for most systems a dedicated tool would be preferred. CASSANDRA and eCASSANDRA (a web-enabled version) are the MOD-preferred tools for constructing hazard logs. Commercially available tools include HARMS, SMART and SMARTER. Details of CASSANDRA and other hazard log tools can be obtained from the Safety Management Offices listed at the back of this booklet.

Word processing tools make producing a document easier but don't always result in one that is well-written; this depends on the skill of the author. In the same way, hazard log tools provide very useful functionality for recording and connecting information on possible hazards and accidents, but must be applied intelligently. If hazards, accidents and controls are chosen and described at a useful level, then the hazard log will be most effective in supporting the safety risk management process.

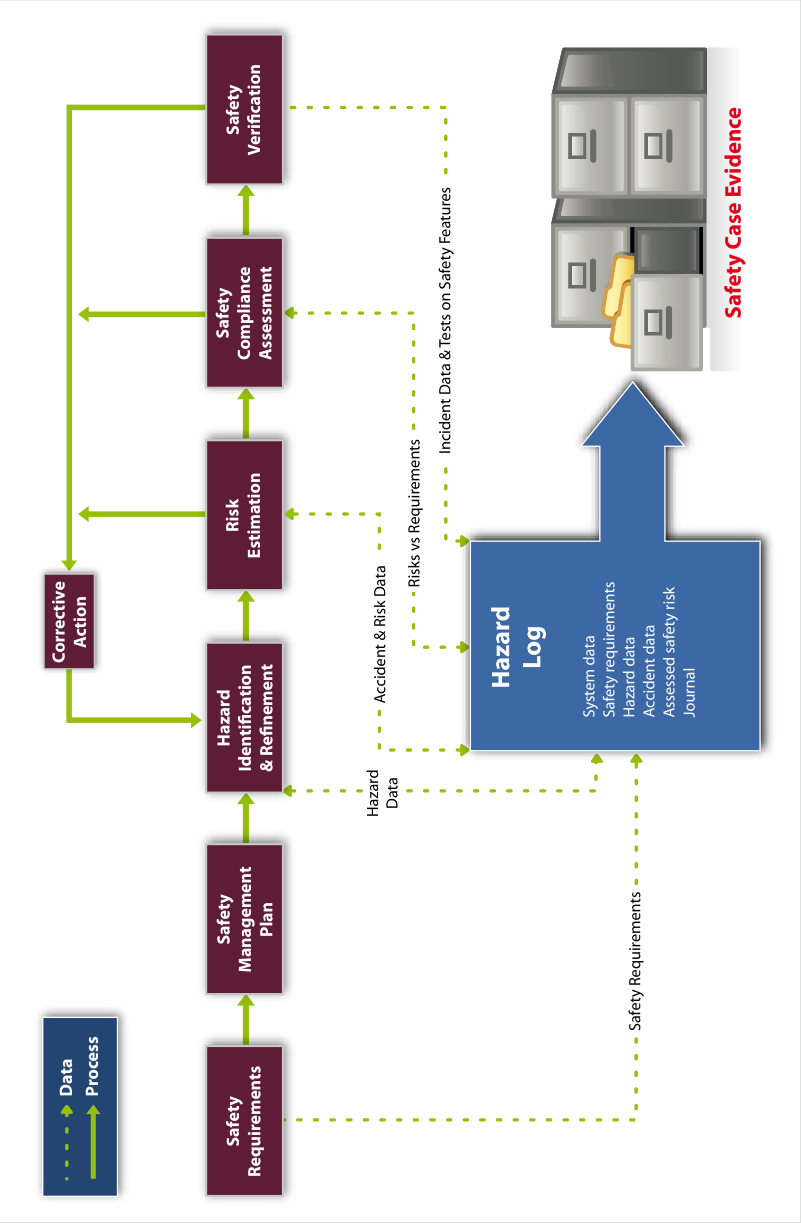


Figure 9: How the Hazard Log Supports the Safety Activities

6.3 Risk Management and Assessment

Risk management is defined as "The systematic application of management policies, procedures and practices to the tasks of Hazard Identification, Hazard Analysis, Risk Estimation, Risk and ALARP Evaluation, Risk Reduction and Risk Acceptance." (Def Stan 00-56).

Management of risk for a system is not simply about reducing risk: it relates to striking a balance between the benefits from reduced risk and the expense of that reduction. However, some risks may be completely unacceptable and not a subject for balancing against expense.

Risk management relies on judgment. The decisions should be supported by qualitative assessment methods, complemented where necessary by quantitative methods. Quantitative methods are particularly appropriate where the severities and extent of harm are high. The effort for risk assessment should be proportionate to the risks involved, with particular care needed in dealing with novel technologies and unusual applications. Risk assessments are required by law to be "suitable and sufficient to identify the safety measures needed".

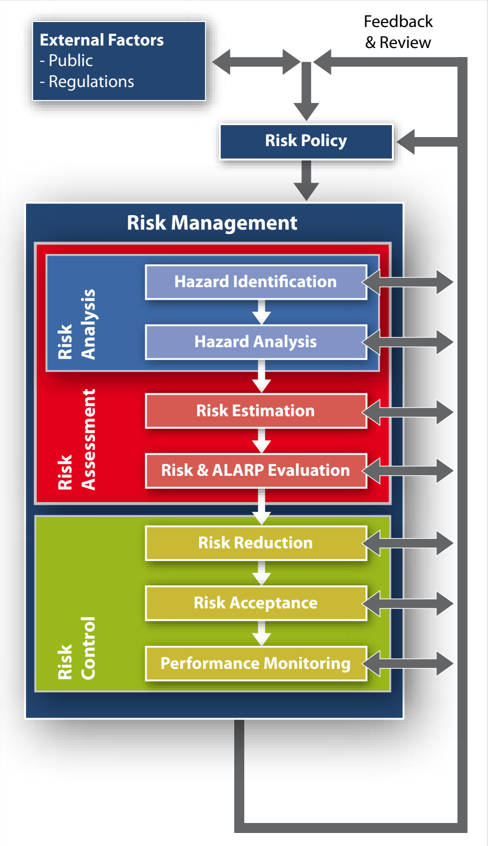


Figure 10: The Risk Management Process (after Def Stan 00-56)

There are various models of the activities involved in risk management and the terms "analysis", "assessment" and "control" are used in a variety of ways; Fig 10 shows the Def Stan 00-56 interpretation. Regardless of the model and the terminology, risk management is an iterative process, where the results of activities feed back and are considered in the repetition and refinement of previous activities.

Risk assessment is the bridge between identifying the hazards and the decisions that must be made about controlling them.

Risk management is part of safety management. Risk management activities have no effect on risk until the process of risk reduction is actually implemented, be it a design change, additional safety protective features or revised working practices.

Risks should be controlled in the following order of priority:

- Elimination of the hazard
- Substitution of the hazard (e.g. by use of alternative substances or procedures)
- Hazard control (e.g. physical protective measures such as interlocks or guards)
- Provision of safety procedures, additional training, personal protective equipment etc

Design changes are necessary to eliminate or substitute hazards. This shows the importance of beginning risk management early in a project lifecycle, when it is easier (and cheaper) to use these preferred risk control strategies.

6.4 Making Risks ALARP

Risks should be reduced to a level which is "As Low As is Reasonably Practicable" (ALARP). This is the HSE's approach to meeting the legal concept "So Far As is Reasonably Practicable". The "risk creator" has a legal duty for many types of risk to judge when risk exposure should be tolerated, and to record their justification for this.

An ALARP argument should balance the "sacrifice" (in money, time or trouble) of possible further risk reduction measures with their expected safety benefit (incremental reduction in residual risk exposure). The balance should be weighted in favour of safety, with a greater "disproportion factor" for higher levels of risk exposure.

The HSE recognises three approaches to making a claim that risk is ALARP:

- **Good practice arguments** which demonstrate that risk control measures comply with relevant good practice as defined in ACoPs, HSE guidance, standards etc
- **Qualitative first principles arguments** based on common sense or professional judgement to weigh possible risk reduction against the necessary "sacrifice"
- **Quantitative first principles arguments** based on numerical techniques such as Cost Benefit Analysis (CBA) to weigh possible risk reduction against the necessary "sacrifice"

In making a claim that risk has been reduced ALARP, the duty holder should consider the person at greatest exposure (sometimes called the "hypothetical worst case individual").

Although quantitative ALARP arguments are rarely required, they can be emotive and challenging. They rely on placing monetary values on the level of harm suffered by injured parties, then using this value to decide whether the costs associated with possible further risk reduction measures can be justified. Great care is therefore required to ensure that disproportion factors are correctly considered and that the conclusion is explored for its sensitivity to assumptions.

A duty holder makes an argument that risks have been made ALARP; however, the validity of this argument can only be decided definitively by the courts, should an accident happen. Duty holders may therefore decide to seek an independent opinion on the strength of their ALARP arguments for risks of a high level.

In most sectors, activity with safety implications would not be allowed until risks have been shown to be ALARP and it can be shown that all risk mitigation measures have been fully implemented. In a military environment, many systems are intended to reduce risk for friendly forces. It may therefore be necessary to take a wider view of risk exposure, given that certain military operations must be undertaken within time constraints. ALARP arguments would therefore consider the wider risk reduction measures which are available for "reasonably practicable" adoption, both short term and long term.

6.5 Risk Ownership, Transfer and Referral

Where an organisation is responsible for many activities or systems, it is important that there is clearly defined responsibility for safety risk management. Often each "single risk" or each risk control measure will be assigned to an owner, or there may be a single owner who is responsible for all "single risks" associated with an activity or system.

For a particular system one "single risk" may be controlled by several separate risk control measures, for example design change, a user procedure and a training element. For a MOD acquisition project, the project manager would typically be responsible for deciding on the necessary risk control measures and for co-ordinating the authorities responsible for implementing them, although those authorities retain responsibility for the implementation. The project manager will use the project safety committee as the forum for discussions with the various authorities involved and use the hazard log for tracking the risk management process.

During safety analysis for a particular system, information may be revealed about hazards or accidents that are the responsibility of others. For example, if a system is part of a wider "system of systems", it may only be at the higher level that there is enough understanding of the full accident sequence and all control measures to complete the risk assessment. There should therefore be methods of communicating information on these safety issues to other parties and of making a formal transfer of risk ownership where appropriate.

The common system of risk classification (e.g. by risk matrix) is intended to ensure that the issues with the greatest significance receive the greatest level of scrutiny. Risk issues are typically referred to higher management levels for oversight of the risk management process, since senior management can decide on whether additional resources should be made available to reduce risk.

Key Messages
The safety case approach to safety regulation makes the organisation wanting to do an activity responsible for demonstrating that their operations are going to be safe
MOD use safety cases to provide the argument and evidence that their systems are safe for their purpose
Safety cases are live, working documentation that are developed and reviewed through the lifecycle
Safety cases are required for MOD legacy systems and for OTS (Off the Shelf) equipment
Configuration management is vital to good safety management

7.1 Approaches to Regulation

Where activities are considered to be particularly hazardous, a safety regulator may be appointed to give society added assurance that organisations creating risks are managing them effectively. For major hazards industries such as chemical processing, oil and gas and rail transport, the approach taken is called "permissioning" and this explicitly makes the **creator** of risks responsible for demonstrating that their activities are going to be safe. The demonstration is by means of a safety case, which is a body of evidence presented as a reasoned argument.

The operator's safety management system is an important part of the safety case evidence, as it shows that they will carry on thinking about safety and striving for continuous improvement throughout the life of the system. The safety case will then be examined by the regulator, who can provide approval to operate, or written acceptance of the case made, when they are satisfied with the evidence of safety. This does not remove any of the responsibility for safety from the creator of the risks.

In this context, MOD is the "creator of the risks" but it is also the "regulator". The regulator or assurance function must be organisationally distinct within MOD, so that one area is not responsible both for preparing the safety argument, and declaring it adequate.

MOD has developed its regulatory and assurance functions to be proportionate to the nature and scale of hazards. In some areas of its business, such as ship "key hazards" and nuclear propulsion, MOD has a safety regulatory organisation. In other areas MOD has its own assurance function but it does not operate a "permissioning regime". It is important for project staff to identify and engage with the regulatory and/or assurance authorities for their project.

The MOD may contract out the production of the safety case but it is still owned by MOD.

7.2 The Safety Case

A **safety case** is defined as "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment" (Def Stan 00-56). A simple way of understanding the safety case is to consider five basic questions:

- **What are we looking at?** - (System description)
- **What could go wrong?** - (Hazard identification and analysis)
- **How bad could it be and what are the major threats?** – (Risk estimation)
- **What has been or can be done about it?** – (Risk and ALARP evaluation, risk reduction and acceptance)
- **What if it happens?** - (Emergency and contingency arrangements)

The safety case should answer these questions for the whole system under consideration and for the uses defined. A key aspect of the safety case is that it should highlight the major hazards and concentrate on these: often safety cases can be swamped by a mass of detail on all the hazards from the trivial to the most significant.

Safety cases should be proportionate to the risks which the system poses. Understanding the major hazards will help to determine the scale and complexity of the required safety case. Therefore preliminary hazard identification and analysis should be done early in the project lifecycle to scope the activities and resources needed to build the safety case.

In MOD terminology the **"safety case"** is the body of evidence: a comprehensive and structured document or set of documents. It usually includes evidence in test results, detailed safety analysis reports and so on.

The MOD safety case is often summarised at key decision points in a project in a series of **"safety case reports".** These reports enable management to understand the safety issues, as one of the contributing factors, informing the decision whether to proceed from one phase of the project cycle to the next. The purpose of these safety case reports changes at different stages of the lifecycle. Early in the lifecycle, a safety case report will aim to show that the safety requirements and characteristics of the solution are properly understood and that a strategy is in place to manage safety through the rest of the project. Later on, a safety case report will be used to show that planned trials can be conducted safely and then that the system can be introduced safely into service use or mid-life updates can occur. If an incident or accident happens in service, a safety case report may be needed to show that adequate safety can still be achieved, through design, upkeep or usage changes if necessary. Finally, a safety case report may be used to show that safe disposal can be made at the end of a system's life.

The safety case provides an audit trail of safety considerations from requirements through to evidence of compliance and risk control. It gives the traceability of why decisions have been made and how they have been validated. The safety case develops during a project lifecycle and will typically be summarised in safety case reports at the end of each phase or prior to each major decision point.

The main elements of a safety case report include:

- Executive summary
- Summary of system definition and description
- Assumptions
- Progress against the safety programme
- Meeting safety requirements
    - Safety requirements, targets and objectives
    - Summary of argument and evidence showing how requirements have been / will be met
    - Any requirements that are unlikely to be met, with remedial actions
    - Outstanding risk management actions
    - Residual risk
    - Regulatory approvals and associated restrictions
    - Feedback arrangements for defects and shortfalls
    - Interface issues with other systems
- Emergency and contingency arrangements
- Operational information
    - Operational envelopes
    - Limitations on operational capability
    - Main areas of risk (e.g. A or B Class)
- ISA report (if appointed)
- Conclusions and recommendations
- References

The safety case is live, working documentation and shouldn't just gather dust in a cupboard. Its relevance and accuracy must continue to be reviewed in the light of information from incidents, overhauls, in-service surveillance which can validate assumptions or provide counter evidence. The safety case should be updated if:

- The equipment/system is modified
- There are changes in how or where it is used
- There are changes in legislation or the safety requirements
- There is a deviation between actual performance and design intention
- Incidents in service highlight previously unrecognised hazards or show that current risk estimates are wrong

Not all safety cases are good. The HSE has reviewed many real safety cases in its role as regulator, and some of the problems it has found with poor examples include:

- They contain assertions rather than reasoned argument
- There are unjustified and implicit assumptions
- Some major hazards have not been identified and are therefore never studied
- There is a poor treatment of data with uncertain pedigree, and the effects this uncertainty has on subsequent assessments
- They don't deal well with human factors
- They don't deal well with software
- There is inadequate involvement of senior management
- Ownership of the safety case is not always clear

Safety cases can be considered the tangible products of an effective safety management system. The intangible product is a safer system. Having a safety case does not in itself reduce risk: it is only when the findings are acted upon and the outputs implemented that safety will improve and people will be safer.

7.3 Safety Cases and Users' Safety Management

The user need not be given the full system safety case, since they do not need to know all the information contained in it. However, the information that deals with emergency arrangements and with limitations for safe use (the "safe envelope") must be available to them, usually through standard user documentation. Other safety information should be provided in formats that are tailored to the end-user's needs, for example as command safety summaries or operator's aide memoires.

The user organisation also requires Operator and Maintainer (O&M) procedures that are safe and information on training to ensure that the human part of the system will be trained safely and able to keep the system safe through life.

The safety case must highlight key safety items to the user, such as critical equipment and procedures. It should also provide necessary information, for example on safety margins, so that the responsible user authority can take these into account in their own operational risk assessments.

The user must be satisfied that the safety case, or its outputs, addresses the User Requirements set for the asset, was produced with the involvement of relevant stakeholders, has been independently reviewed to validate and verify its content and assumptions, and provides suitable and sufficient information and procedures.

The user organisation must provide feedback on any incidents and accidents that occur and there must be assurance that any assumptions in the safety case are valid in actual usage. These assumptions might cover aspects such as manning levels, how the system is being used, any interfaces with other systems etc.

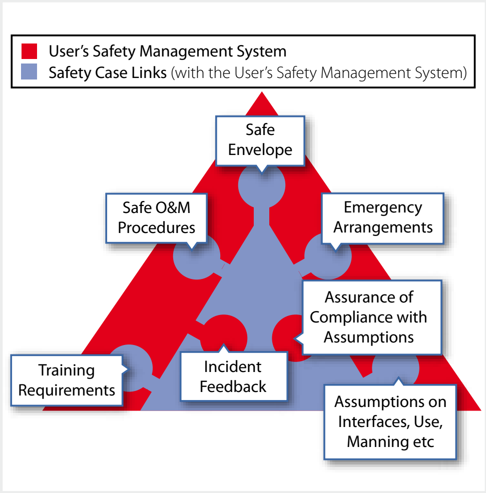

🟥 User's Safety Management System
🟦 Safety Case Links (with the User's Safety Management System)
Safe Envelope
Safe O&M Procedures
Emergency Arrangements
Assurance of Compliance with Assumptions
Training Requirements
Incident Feedback
Assumptions on Interfaces, Use, Manning etc

Figure 11: How the Safety Case (shown in Blue) Links with the User's Safety Management System (shown in Red)

Users and maintainers of systems covered by safety cases will often have a requirement to conduct safety risk assessments for particular operations or sites. It is important that all safety stakeholders discuss and agree the scope of the system safety case, and responsibilities for providing information for related risk assessments. These might cover situations such as:

- Workplace (e.g. workshop) risk assessments
- Control Of Substances Hazardous to Health (COSHH) risk assessments
- Training area risk assessments
- Lifting operation risk assessments

7.4 Safety Evidence and Assumptions

Many people imagine that safety cases are made up from extensive theoretical analyses which "prove" numerically that a system is safe. In fact, the safety case should bring together **all forms** of evidence of safety and make an explicit argument showing why the system should be considered safe.

MOD is building on existing good practice of procuring and operating safe systems; it is not only interested in numerical analyses. The safety case should embody all forms of evidence such as:

- Performance in previous use (accident/ incident/failure rate record)
- Compliance with standards, regulations and guidelines
- Calculations (e.g. Finite Element Analyses for stress and fatigue life)
- Testing (e.g. performance, fatigue life, software)
- Simulation
- Analytical (e.g. HAZOPS, FMECA, FTA etc.)
- Expert review / best practice / certification

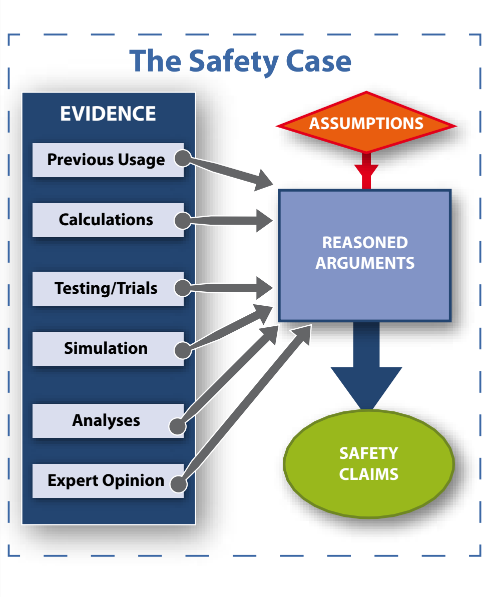


Figure 12: How the Safety Case Draws on Evidence and Assumptions

Figure 12 shows that the reasoned arguments combine various types of evidence and also build on assumptions. It is important that these assumptions are declared openly. During the safety programme, the key assumptions should be validated wherever possible, thus effectively replacing each assumption with evidence.

It is not always easy to follow the reasoned arguments in safety cases. Information is sometimes amassed and the readers are encouraged to draw a general conclusion that the system must be safe. Techniques such as Goal Structuring Notation (GSN) and Claims, Argument, Evidence (CAE) have been developed to provide rigour and clarity in the presentation of safety cases and similar types of reasoned argument. Computer tools exist to implement these techniques, and they can be very helpful in the management of information as well as its comprehension; details of available tools can be obtained from the Safety Management Offices listed at the back of this booklet.

The next chapter gives an overview of the analytical techniques which are used to provide some of the inputs to safety cases.

7.5 Safety Cases for Legacy Systems

The safety case should be developed alongside the system design through its life cycle to provide progressive assurance of its eventual safety in operation and disposal. But what about safety cases for **existing** systems and operations?

MOD has a policy of requiring a retrospective assessment of safety for existing systems. This assessment should be documented in a format which is essentially the same as for a safety case.

The evidence contained in a legacy system safety case would be expected to contain a higher proportion of real operational experience than for a developmental system, which would initially rely on analytical and testing evidence. This operational evidence might be quantitative (e.g. maintenance and breakdown history and accident rates experienced in service) or qualitative (e.g. anecdotal feedback on incidents experienced by the user community). Such operational experience can provide some of the strongest evidence to support the safety case, because it reflects how the system actually behaves under real conditions, rather than depending on simulated conditions or paper-based analyses.

It is important that the safety case for a legacy system reflects the actual material condition and build state. It may be necessary to survey the in-service systems to establish their state and to identify any variations from the design records.

Existing or "legacy" systems are different from those in development and the safety case must be tailored to reflect the differences. Some of the important characteristics of legacy systems include the following:

- Development activity is complete - there is very limited opportunity to influence the system design to make it safer
- There should be actual field data on safety and incident/accident records (although this might show that the level of achieved safety is not good)
- Often there were no or poor safety requirements in the original specification
- Sometimes the original design information is hard to find
- The justifications for decisions in development may no longer be known
- Configuration control is especially important - what has been changed since original design and are all items of the same build standard?
- The way in which the system is used may have changed since the original design
- There may have been a significant change in legislation since the system was introduced.

Although there is limited opportunity to influence system design, improvements to reduce risk are still to be expected. These could include:

- Design changes (e.g. new safeguards)
- Restrictions on use
- Procedure and documentation changes (operator and maintainer)
- Training changes
- New technology

7.6 Safety Cases for Off The Shelf Equipment

MOD procures a wide variety of Off The Shelf (OTS) equipment. By definition, the equipment should not require development to meet MOD's requirement. However, many projects do involve modification of an existing commercial product to meet MOD-specific requirements. Some OTS equipment is procured allowing contractors "fit, form and function" changes on delivery, modification or repair. This may require specific risk assessment.

In the simplest case, an equipment may be "CE" marked. CE marking is only a claim by the manufacturer that the item is safe and that they have met the relevant supply law. The user still has a legal duty to check that it is, in fact, safe and complies with all the supply law that is relevant. In order to assign CE marking, the manufacturer will have carried out a safety analysis to demonstrate the safety of the product. This analysis must be checked to verify that it is relevant for the environment and the way in which MOD would operate and eventually dispose of the equipment.

- If there are significant differences between the civilian and military environments, the manufacturer's analysis will have to be revisited. The output will then form the safety case for that OTS equipment in its military use
- If there are no significant differences between the basis of design and the military usage, the manufacturer's analysis will form the basis of the safety case

At the other extreme, OTS acquisition can involve extensive development of a commercial design to meet MOD requirements. In these cases, the safety management tasks described for the full lifecycle should be applied.

7.7 Configuration Management

Configuration management is vital to good safety management. The safety evidence embodied in the safety case will apply to a particular defined build standard and usage of a system. If the actual build standard is different from this there may be different hazards or increased risks associated with the known hazards. Def Stan 05-57 provides requirements and procedures for the configuration management of defence materiel in support of MOD projects.

The build standard and modification status of the systems in the field must be known to the person with safety responsibility. Unapproved modifications or changes in the usage of the system will not have been covered by safety assessment and are strongly discouraged (see note above on OTS).

Key Messages
Safety assessment is an iterative process within the overall development of the system
Safety assessment draws on a range of available techniques to identify and understand possible hazards and accident sequences
Safety assessment must be applied to all parts of the system, including hardware, software and human factors
Possible hazards must be identified and understood so that they can be eliminated or controlled
Hazard identification is most effective when done systematically by a team of people with knowledge about the system, its design, usage and environment

8.1 Introduction

There is no standard, correct and formal way to analyse system safety: there is always the need for human judgement. What is required is an ordered approach to consider and document safety as the system design and its operation and support arrangements are developed. The assessment should be systematic and auditable, but there is no guarantee that the analysis will be 100% effective and complete. For that reason safety management for in-service systems must be vigilant for hazards that have not yet been considered.

Safety assessment is an iterative process within the overall development of the system. The techniques mentioned in this section can be used to different depth at different stages in the development process.

Designers concentrate on normal operation rather than abnormal. A safety assessment should ask how a system could fail, not only how it will work. It requires the use of imagination to determine possible sequences of events leading to accidents.

It is important that the analysis covers all parts of the system, including hardware, software and the human factors. The human being and the jobs they do are just as much part of a system as the equipment. They must also be covered in the safety analysis. Human factors issues are not just about human errors; they also cover failures in the interaction between people and machines, people and the environment and between individuals.

This chapter introduces some of the analytical techniques which are used for safety assessments. Each technique has strengths and weaknesses which must be considered when deciding the best set of tools for any safety assessment. More detail can be found in the references at the end of the booklet, including MOD's Safety Manager's Toolkit, which is available from the AOF.

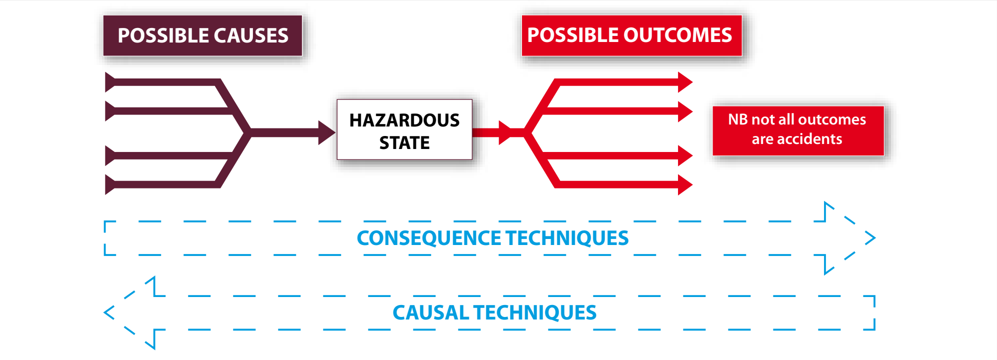


Figure 13: Forward and Backward-looking Analysis Techniques

The simple diagram (Figure 3) of one accident sequence shows an initiating event leading to a hazard and on to an accident. In fact, a particular hazard may have several possible causes, either acting alone or together. The same hazard may lead on to a variety of different outcomes, some of which will be accidents and some relatively unimportant. It is vital to link the hazards to the accidents (see Figure 13) they could cause, because the risk assessment is applied to the accident outcome.

Where accident sequences are complex it is important that they are analysed so that the risk estimation is valid. If there are many interacting factors involved, then the safety case must demonstrate that they were explored and understood in detail. Forecasts of likelihood based on opinion or historical records alone are not appropriate for complex or very rare but catastrophic events.

The analytical techniques must provide the required information on every credible hazard and accident sequence for the system. The techniques fall into three broad categories:

- Hazard identification techniques
- Causal techniques (looking back to see how hazards and accidents might possibly be caused)
- Consequence techniques (looking forward to identify possible outcomes from a given event or situation)

Some of the techniques available serve more than one purpose: they not only identify hazards but examine consequences too. Nevertheless it is vital to choose the correct combination of techniques and to tailor them to the particular system being assessed.

The techniques mentioned below are the individual tools used for assessing system safety and concentrate on what the system is (physical safety) and what it does (functional safety). Terms such as Probabilistic Safety Assessment (PSA) and Quantified Risk Assessment (QRA) describe a whole process which would use several of the individual techniques.

8.2 Hazard Identification Techniques

If possible safety problems are not recognised, there is no chance of controlling them or assessing their risks. Hazard identification serves several purposes including:

- Setting safety requirements
- Eliminating or controlling the hazard
- A necessary precursor to hazard analysis and risk assessment
- Planning emergency and contingency arrangements

MOD's Safety Manager's Toolkit includes information on several Hazard Identification techniques such as:

- Hazard checklist
- HAZard and OPerability Studies (HAZOPS)
- Structured What-If Technique (SWIFT)
- Failure Mode and Effects Analysis (FMEA)

It is important to use a modern, open method to identify possible hazards, but a safety study should consider hazards identified by any means: previous incidents, checklists, design reviews etc. Whatever techniques are used, good hazard identification depends on experience and imagination. It is very important that hazard identification should draw on the knowledge and understanding of those who know about systems or equipment of this type, including designers, operators, maintainers and other subject matter experts.

8.3 Causal Techniques

The most common technique for looking at how a known hazard (top event) could be caused is Fault Tree Analysis (FTA).

FTA is particularly useful for systems with redundancy (two or more ways of achieving a function) and looking at the number of separate events required to cause the undesired top event. It can also identify potential problems with "dependent failures" which might affect several apparently separate redundant equipments (e.g. both the duty and standby power supplies).

FTA provides valuable information through qualitative analysis, but can also be quantified with event probabilities or rates, to give an estimate of how often the top event will occur.

The backward looking part of HAZOPS, SWIFT and FMEA are also causal analyses. Other techniques, such as Reliability Block Diagram (RBD) and Cause Consequence Diagram (CCD) modelling, can be used to represent the causes of a defined event. The representation is different but the analysis process is very similar to that for FTA.

8.4 Consequence Techniques

Consequence techniques are used to assess how a situation or event could develop. They explore the possible consequences, not all of which will result in harm.

There are several consequence techniques including:

- Event Tree Analysis (ETA)
- Failure Mode and Effects Analysis (FMEA)

The forward looking part of HAZOPS, SWIFT and FMEA are also Consequence Analyses.

Other techniques, such as Cause Consequence Diagram (CCD) modelling and Bow-tie diagrams can be used to represent complete accident sequences from initiating event to outcome. The representation is different, but the analysis process is very similar to those for both FTA and ETA.

Consequence Models and Simulations In many situations it is difficult to be certain about the scale of the consequences. There may be little quantitative data available on rare events such as major explosions and releases of toxic gas clouds. Models which are frequently computer-based, are then used to study the possible outcomes.

The results from such models form a part of the safety evidence, and so the assumptions must be traceable. The model should be validated against experimental results where possible, and the results compared with information from other sources.

8.5 Analysis Techniques for Software

The safety of the software parts of systems can cause significant problems, possibly because the system faults which software can cause, appear unfamiliar and unpredictable.

Software problems arise from a number of causes:

- Mistakes in specification
- Mistakes in design
- Mistakes in implementation
- Mistakes in testing
- Mistakes in maintenance
- Mistakes in configuration management
- Mistakes in change control (new problems introduced in curing known problems)

Faults from causes like these will sit in the software waiting for a "revealing mechanism", such as an unexpected input or a change of operating conditions. The fault then becomes a software error, which is a "discrepancy from its required state". A software failure is the effect of the error on the intended function, and may cause minor irritation through to catastrophe, depending on the software function affected.

The first stage, required both for safety assessment but also for choosing how to design the software, is to look at the functions it will perform in the system. Any of the techniques described above can be used to identify the system hazards which could be caused by the software. If the software doesn't do its job, for whatever reason, then these are the undesired conditions which could result.

The analysis of the hazards will identify the possible consequences and the other features which control the risks. The severity of the consequences will determine how much effort should be invested in making the software right and in providing the assurance evidence.

8.6 Developing Safe Software

There are several approaches for developing software that reliably does the job required. Factors which are considered include the choice of language, depth and type of testing, formality and rigour of the specification and verification.

There are many methods for the assessment of software but they fall into the two main classes of **process-based** and **product-based** techniques.

- **Process-based techniques** look at the design and development methodologies used to produce the software, and so provide an indirect indication of the software's actual quality
- **Product-based techniques** look at the actual software produced, and so provide a direct indication of the software's quality. Methods such as dynamic testing and static analysis fall in this category

Whichever class of technique is used, one cannot be certain that the last latent problem has been identified and removed. There remains residual risk that the software could fail. Various methods can be used to estimate failure probability for the software, but none of these is universally accepted. Estimated probabilities of a software failure should then be included in the overall Quantitative Risk Assessment (QRA) of the system.

Quantitative measures of software reliability can be produced by modelling failure rates to show how they have decreased (preferably!) during previous usage. Rules-of-thumb have been proposed for estimating the number of faults in software, depending on the number of lines and development methodology. Again, these are not universally accepted.

The methods described above will provide the parts of the safety evidence relating to a system's software. It should be an integral part of the system safety case.

8.7 Safety Assessments for Existing Software

System developers are increasingly reluctant to develop bespoke systems, and wish to use off-the-shelf software (including firmware) or re-use existing software in new applications. Such software is, to a greater or lesser extent, of unknown pedigree, and the catch-all term Software of Unknown Pedigree (SOUP) has been adopted.

When these systems are safety-related, assurance is required that they work reliably and correctly. It can often be difficult to justify the use of OTS/reused software using the same techniques as for bespoke software. For example design and specification information may be unavailable or incomplete.

Many standards pertaining to safety-related software are targeted at bespoke software, where control over design and implementation issues is possible. However, these approaches are unsuited to assurance of OTS/reused software. Therefore, the MOD has concluded that an "evidential" approach is better suited to the safety justification of SOUP.

The main element of the SOUP justification approach is one of basing safety arguments on the evidence available. Software components can be thought of as belonging to three categories, and the evidence-based approach has to be tailored to take account of each circumstance:

1. Black-box, where little or no information about the internal workings of the software is available
2. White-box, where internal workings, such as the original source is available
3. Open-box, where not only the source driving the software is known, but it is also adaptable depending on circumstances of its use

An evidential approach is then based on the following process to establish pedigree:

- An identification of the evidence required to establish the safety arguments in context. This should include any Black-box and White-box analysis
- A preliminary assessment of the viability of this analysis, based on the requirements already established at this stage
- Gathering and presentation of the initial evidence required by this stage
- An assessment of the evidence gathered and mitigation of any gaps
- A decision on whether the safety case has been established or not, and if not, whether to return to the testing phase, or abandon the process entirely

It might seem that re-using existing software will always be easier, faster and cheaper than a bespoke software development, However, there can be substantial work required to establish pedigree and provide the necessary assurance information for SOUP. This must be considered early in a project lifecycle, or there will be significant risks that using OTS software for safety-related purposes will delay or prevent safety approval of the system.

Key Messages
MOD applies the Acquisition Safety and Environmental Management System (ASEMS) to all its acquisition projects
ASEMS is a flexible system, covering all acquisition strategies and technologies, across all domains, to meet the requirements of domain-specific JSPs
ASEMS consists of POSMS for Safety Management and POEMS for Environmental Management
Compliance with the POSMS and POEMS will ensure that any project's safety and environmental management system is robust, proportionate to the project's levels of risk and is compatible with the DE&S corporate reporting requirements
The right safety management activities must be done at the right time, otherwise there may be excessive safety risks in service or excessive project risks (e.g. project delay, cancellation, cost overrun)
Before the system comes into service, safety is mainly an engineering discipline, influencing the design process. Safety management will also be concerned with keeping personnel safe when they come in contact with the system, for example during trials and commissioning
From the in-service date onwards, safety management is concerned with keeping people free from harm, by using safe systems of work, by responding to incidents that occur and by considering the effects of changes
Project Teams can influence safety for their systems by: - Consulting widely - Setting good safety requirements - Maintaining a good safety culture - Selecting and working closely with competent contractors

9.1 General

Different safety activities happen through the stages in a system's lifecycle, and their successful implementation requires a variety of approaches and skills. This section looks at these activities and indicates what should should be done and when.

The safety programme requires a close working relationship between the sponsor, the project management team, the users, equipment developers and any safety regulation or approval authorities.

The approaches required at various stages draw on different mental attitudes:

- **Inception** (earliest stages) - **imaginative** and **decision-making**
- **Execution** (development, introduction) - **meticulous** and **understanding**
- **Use - competent** and **disciplined**

Most of the following discussion is based around the CADMID acquisition cycle (Concept, Assessment, Demonstration, Manufacture, In-service, Disposal), which is one example of a project lifecycle model. Not all projects follow this model, but the basic stages from conception, through examining design options to construction, installation, usage and disposal, are widely applicable. Although the CADMID cycle is usually represented as a sequence of discrete stages, elements of the cycle frequently take place in parallel rather than series. For instance, disposal activities cover more than merely system disposal at the end of its life: items may be disposed of from the Assessment or Demonstration phase onwards, including test articles, consumables and unintended disposal (e.g. systems which are scrapped after a crash).

9.2 MOD's Acquisition Safety and Environmental Management System

DE&S applies the Acquisition Safety and Environmental Management System (ASEMS) to all their acquisition projects. It is a flexible system which can be applied by project teams for projects of all acquisition strategies and technologies, across all domains to meet the requirements of domain-specific safety Joint Services Publications (JSPs).

At the core of the ASEMS there are two systems manuals: the Project Oriented Safety Management System (POSMS), and the Project Oriented Environmental Management System (POEMS). Each manual contains a number of procedures designed to assist project teams to manage safety risks and environmental impacts and to apply the appropriate mitigation measures. The manuals may also be used by contractors, suppliers, and advisors where appropriate. Compliance with the POSMS and POEMS will ensure that any project's safety and environmental management system is robust, proportionate to the project's levels of risk and is compatible with the DE&S corporate reporting requirements.

Access to the POSMS and POEMS procedures can be either through the manuals, or by accessing business process maps. These maps define the safety and environmental activities that should at happen at different stages in the project lifecycle, and give users access to tools and forms that will help them produce the necessary outputs in a consistent way. ASEMS is available throughout the acquisition community and, as part of the Acquisition Operating Framework (AOF), can be accessed through the internet.

9.3 What is Done and When

Safety activities are undertaken throughout the life of a system but it is vital that the right ones are done at the right time. If they're not, then there are two possible undesirable outcomes:

- Introducing an unsafe system into service (excessive **safety risk**)
- Major delays, cancellation or cost overruns if safety problems are discovered late (excessive **project risk**)

Safety analyses should determine the safety requirements and influence the design process. The safety programme is therefore integrated with the overall project programme. In an ideal world, the analyses would result in a system that was free from hazards. In practice, a new system should contain no surprises and strategies should be in place to control hazards that remain. The safety programme should also be closely tied to project risk management activities so that potential project risks due to safety can be understood and managed with appropriate visibility.

The nature of safety management for a project is different before and after the system comes into service. Until that point, the emphasis of safety is on managing the development process and safety is therefore mainly an engineering discipline. Once a system comes into service, the safety management system is principally concerned with keeping people free from harm. Of course, activities such as development trials can cause harm, and system modifications when in service require the same engineering emphasis as during the original development.

As illustrated in Fig 14, a separate safety case report is produced at each key stage of the lifecycle, or decision point. This should be seen as gradual refinement and extension of the same documentation. A safety case report is a summary of work up to a given point, or for a defined purpose (see Table 4). From the earliest stages it should be known what type of evidence will be required to demonstrate that safety will be achieved. The safety programme aims to fill in the known evidence gaps.

The following sub-sections and Table 4 identify the key activities at each of the lifecycle phases. They do not include the activities which run throughout the lifecycle, including:

- Operating the project safety management system (including auditing and monitoring incidents and accidents)
- Convening meetings of the project safety committee
- Producing and maintaining the safety management plan
- Conducting project risk management activities, including those for project risks resulting from the safety programme

9.4 How Project Teams can Influence Safety

The major ways in which a project team can influence safety for their system include:

- **Consulting widely with stakeholders and subject matter experts -** to ensure that the capability, environment, interfaces, safety approval requirements etc, are well understood
- **Setting good safety requirements –** by taking account of stakeholder needs and through timely application of risk management
- **Maintaining a good safety culture –** adopting a Just Culture, speaking up when they have safety concerns and maintaining competency levels through training, review and audit
- **Selecting and working closely with competent contractors –** the competence must cover the relevant technologies, domains and safety management

9.5 Concept

At the earliest stage of a project the emphasis is on deciding whether the capability requirement can, in principle, be met sufficiently safely.

Initial activities should include identifying stakeholders and consulting with them. This will help gain an understanding of the capability required, interfaces with other systems and any constraints on the solution. The stakeholders will also help to identify the safety regulatory or approval regime that will apply to the system when it comes into service, and any specific requirements for safety information which must be provided. Consultation with stakeholders and subject matter experts will continue throughout the life of the project.

At this stage, the design solution may be unknown, or understood only as a conceptual outline. Hazard identification is therefore principally through functional analysis (e.g. a Functional FMEA). Information on incidents and accidents from forerunner systems and comparable commercial systems may also be useful.

Nearly all accidents that occur can be traced back to events or phenomena that were predictable at the design concept stage. The hazards and accidents identified at this time can be studied and dealt with far more effectively than those coming to light later in the lifecycle.

The hazard log should be started and populated with the known information on the system and its possible hazards and accidents.

Some consequence analysis is necessary to determine the possible accidents for the system. Once the range of possible accidents is known, the Risk Classification Matrix can be produced and tailored for the particular system. This matrix provides the framework against which risks will be judged at later stages of the lifecycle and forms part of the safety requirements which should also include:

- Legal requirements
- MOD certification requirements
- Safety related standards
- MOD policy or procedural requirements

The safety programme aims to determine whether the capability requirements can be met without causing unacceptable risks to service personnel, members of the public and the environment. Where unacceptable risks are identified, the project safety committee must consider whether they can be eliminated or reduced during the development process and make recommendations in the Initial Gate submission.

The main safety outputs at the Concept stage are:

- Safety case report including a conclusion on whether the capability requirement can be achieved sufficiently safely
- The safety sections of the User Requirement Document (URD)
- A Safety Management Plan (SMP) for subsequent phases of the project

9.6 Assessment

At the Assessment stage of a project the emphasis is on deciding how the URD safety objectives can be achieved and, where relevant, on determining which design option provides the safer solution.

The expected safety performance of different design options should inform the choice of which solution should be selected. If any option has a fundamental shortcoming that will prevent it meeting legal or policy requirements or being made tolerably safe, then this should be identified early and will prevent that solution being adopted.

Separate safety programmes are conducted for each of the options, although there will be common material because the functions and environment will be very similar. A separate hazard log should be maintained for each option. The output of the safety work will be a separate safety case and safety case report for each option.

The hazard identification and consequence analysis should be extended and refined now that there is some information on how the conceptual design will be realised.

During Assessment, or earlier, the project manager must judge whether the risks for the system warrant the appointment of an Independent Safety Auditor (see Section 5.6.).

Emphasis should be on refining the safety requirements and developing the safety analyses to a greater level of detail. As information becomes available, hazard identification and hazard analysis should be extended to sub-system levels. Where necessary, the safety requirements should be apportioned down to sub-system level.

The main safety outputs at the Assessment stage are:

- A separate safety case report for each design option and a ranking of options from the safety perspective, together with identification of any fundamental safety shortcomings of any option
- Refinement of the safety targets for inclusion in the System Requirement Document (SRD)
- A Safety Management Plan (SMP) for subsequent phases of the project

9.7 Demonstration

The bulk of detailed safety evidence is produced at the Demonstration stage of a project, when the safety assessment is used to guide the design process to produce a safer system. The aim should be to eliminate hazards through design changes, since this can be achieved cost-effectively at this stage. The safety activities will also influence the development of the in-service safety management system and the supporting arrangements for the equipment.

These will include factors such as:

- Training
- Personnel
- Infrastructure and facilities

- Resources, spares and support
- Interoperability issues

The safety case should contain all the safety evidence and show how the safety targets are being and will be met.

Safety case reports may have to be produced to show that any trials can be conducted safely and there may have to be demonstration trials of any safety aspects.

The safety assessment should also consider the effects of the production process and how the system can be safely introduced into service.

The main safety outputs at the Demonstration stage are:

- Input to the design process to produce a safer system
- A Demonstration stage safety case report
- Evidence that the safety targets are being/ will be met
- A Through-Life Safety Management Plan

9.8 Manufacture

At the Manufacture stage of a project the emphasis is on ensuring that neither the production process nor any design changes compromise safety. Once the complete system exists, trials are conducted to verify "testable" aspects of the design. At this stage the necessary supporting arrangements must be put in place and be shown to be adequate to keep the system safe before it is allowed into service.

The safety analyses should be revisited to examine the effects of modifications. The safety information will also provide a major input to the development of documentation (e.g. user and maintainer manuals), training material and schemes.

The main safety outputs at the Manufacture stage are:

- A Full System/ Manufacture stage safety case report
- Results of verification tests
- Further evidence that the safety targets are being met
- Verification of user and maintainer documentation and training
- A Through-Life Safety Management Plan

9.9 In-Service

The emphasis of the safety management system changes when an equipment or capability comes into service. Up until that point, safety activities are principally concerned with influencing the design solution for better safety, and with preparing the necessary arrangements to keep safety performance high when in-service. Once the capability is in service, the management system should concentrate on avoiding harm through implementing the control measures already decided on (e.g. training, safe systems of work, contingency arrangements), and learning the lessons from any incidents or accidents that do happen.

Reporting of incidents and accidents should be strongly encouraged and they should be investigated to find out the direct and underlying causes. It is important that incidents are not dismissed as isolated occurrences or one-offs without careful consideration. Where incident investigation identifies systemic issues or implications for other systems, then these must be communicated to the appropriate authorities.

The safety analyses should be revisited to examine the effects on safety of changes to the design, how it is used or the operating environment.

Changes in legislation and technology should be monitored to identify their effect on the system and its safety.

The effects on safety of planned organisational changes should also be considered particularly carefully during the in-service period. Manning levels, competence and organisational factors can affect the safety performance and so changes could either reduce or increase the risk exposure.

The safety case should be reviewed on a planned basis at intervals appropriate to the estimated risk level for that system. The authorities involved and the depth, coverage and rigour of the periodic review must be considered carefully so that it is more than just a quick confirmation that "nothing has changed". The safety case should also be reviewed, and updated if necessary, when there are:

- Accidents or incidents relevant to safety
- Significant changes to the design or material state (e.g. mid-life update)
- Significant changes in usage
- Deviations between actual performance and design intention
- Plans to extend the in-service life

The main safety outputs at the In-Service stage are:

- Continuous safety improvement though incident investigation and safety audits
- In-service safety case reports when the system is modified or there are changes in how it is used
- Ability to influence the design process for improved safety if there are modifications or updates
- A Safety Management Plan for changes, and system disposal

9.10 Disposal

Planning for disposal should begin at an early stage of a project so that the design can be influenced for safe disposal, for example by eliminating materials that are hazardous to dispose of and making dismantling simple. The plan for end of life disposal should be refined and updated as the equipment is modified and as legislation or policy requirements change. The applicable legislation, such as the Waste Electrical and Electronic Equipment (WEEE) Regulations, should be recognised and understood so that the project can plan for the necessary activities and the costs involved.

At the Disposal stage of a project, the activities depend on the complexity and risks of disposal. For systems with significant disposal hazards, the disposal programme may become a project in its own right. For simpler systems, the planned safe disposal process should be confirmed and then implemented by the disposal authority.

If equipment is sold or given to another owner rather than being scrapped, then MOD is taking the role of supplier. As a supplier, MOD has legal duties to ensure that the equipment complies with legislation, is designed and constructed to be safe and is supported by suitable information on its safe use and upkeep. The costs of achieving this position, and any residual liability, must be considered when MOD is deciding whether to scrap or sell equipment at the end of its life.

The main safety outputs at the Disposal stage are:

- A safety case report for the disposal programme
- A plan for safe disposal

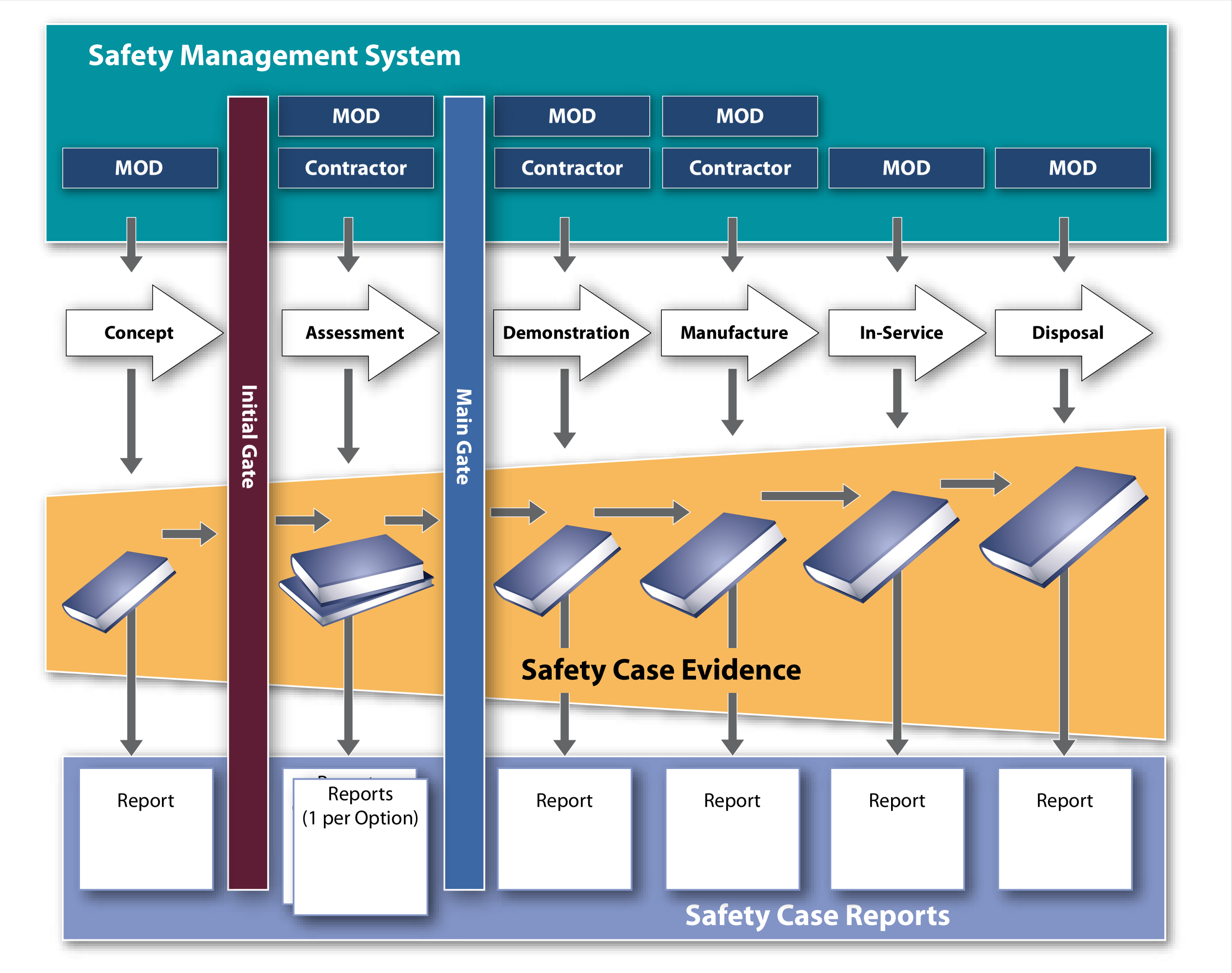


Figure 14: Example of Safety Case and Safety Case Report Development Through-Life

	ACQUISITION LIFE CYCLE MODEL							
	Concept		Assessment		Demonstration	Manufacture	In-Service	Disposal
Safety Activities	• Identify and consult with stakeholders • Identify safety regulatory or approvals regime • Identify and agree stakeholder responsibilities and information requirements • Derive safety requirements for URD • Identify constraints & assumptions	Initial Gate	• Examine feasibility of achieving URD safety objectives • Refine safety requirements for SRD • Apportion safety requirements where necessary • Define safety assurance evidence and acceptance criteria • Compare safety potential of options	Main Gate	• Influence design to produce a safer system • Develop safety assurance evidence through analysis, modelling, simulation, testing etc. • Conduct trials safely and test safety features • Develop support arrangements to keep the system safe in service	• Assess safety impact of change proposals • Verify safety features through tests • Update safety assessment when system built and documentation available • Verify user and maintainer documentation and training schemes • Verify support arrangements	• Transfer safety responsibility to in-service authority (when applicable) • Continuously improve safety though incident investigation, feedback on performance and safety audits • Assess safety impact of changes of, design, use, organisation, legislation etc.	• Review and update plans for safe disposal • Make system safe and provide necessary information if equipment is being sold • Ensure safe disposal
Safety Deliverables	• Concept safety case report, for Initial Gate • Safety sections of URD • Record of key safety stakeholders and their information requirements • SMS and safety committee established • Initial safety management plan • Hazard log established		• Assessment safety cases reports with record of any fundamental safety shortcomings (for each option), for Main Gate • Record of safety stakeholders and their information requirements • Safety sections of SRD • Updated safety management plan • Updated hazard log		• Design safety case report • Input to design to produce a safer system • Input to training and support arrangements to keep system safe • Evidence that the safety targets will be met • Verification tests • Updated safety management plan • Updated hazard log	• System safety case report • Verification tests of safety features • Updated safety management plan • Demonstration that training and support arrangements are in place and adequate to keep system safe • Safety information provided to stakeholders • Updated hazard log	• In-service safety case report (up-dated as necessary during life) • Investigation reports on safety incidents and accidents • Input to design modifications to produce a safer system • Input to training and support arrangements to maintain / improve safety • Updated hazard log	• Disposal safety case report • Disposal safety management plan • Safe disposal procedures • Updated hazard log • Archived safety documentation

Table 4: Example of Key Activities and Deliverables through the Acquisition Cycle

9.11 Final Thoughts

The MOD operates in what is the most challenging and varied environment for safety which requires the use of rigorous and robust safety management. There is commitment from the highest levels to recognise and discharge the MOD's responsibilities for safety and the environment. The organisation is determined to develop its safety culture and to learn lessons from accidents such as the loss of Nimrod XV230.

This booklet forms part of the process of informing those involved in MOD about the topic of system safety.

Standards and MOD Publications	
BS OHSAS 18001:2007	Occupational Health and Safety Management Systems Requirements Standard
Def Stan 00-56	Safety Management Requirements for Defence Systems
JSP 815	Defence Environment and Safety Management
JSP 430	Ship Safety Management Policy
JSP 454	Procedures for Land Systems Safety and Environmental Protection Group
JSP 518	Regulation of the Naval Nuclear Propulsion Programme
JSP 520	Ordnance, Munitions and Explosives Safety Management System
JSP 538	Regulation of the Naval Nuclear Weapons Programme
JSP 553	Military Airworthiness Regulations
POSMS	DE&S's Project-Oriented Safety Management System
Mil Std 882 D	Standard Practice for System Safety
BS EN 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
BS EN 1050	Safety of Machinery – Principles for Risk Assessment

Textbooks and Guides
The Health and Safety Executive **"Successful Health and Safety Management"** HSG65
The Health and Safety Executive **"Reducing Risks, Protecting People"** (R2P2) ISBN 0-7176-2151-0 2001
The Engineering Council **"Guidelines on Risk Issues"** ISBN 0-9516611-7-5 Feb 1993
The Health and Safety Executive **"Programmable Electronic Systems in Safety-related Applications. An Introductory Guide"** ISBN 0118839136
The Health and Safety Executive **"Managing Competence for Safety-related Systems"** (Red Book) Part 1 Key Guidance and Part 2 Supplementary Material 2007
The IET **"Competence Criteria for Safety-related System Practitioners"** (Blue Book) 2007
The Hazards Forum **"Safety-related Systems – Guidance for Engineers"** ISBN 0-952510308
SJ Cox and NR Tait **"Reliability, Safety and Risk Management – An Integrated Approach"** ISBN 0-7506-1073-5

Websites	
Health and Safety Executive (HSE)	http://www.hse.gov.uk/
OHSAS Occupational Health and Safety Zone	http://www.ohsas-18001-occupational-health-and-safety.com/
Royal Society for the Prevention of Accidents (ROSPA)	http://www.rospa.com/
Safety and Reliability Society	http://www.sars.org.uk/
The System Safety Society	http://www.system-safety.org/
The Hazards Forum	http://www.hazardsforum.org.uk/
Institution of Engineering and Technology (IET) – Functional Safety Network	http://kn.theiet.org/communities/functionalsafety/index.cfm
MOD AOF Safety and Environmental Protection Introduction Page **Acquisition Safety and Environmental Management System**	http://www.aof.mod.uk/aofcontent/tactical/safety/content/introduction.htm http://www.asems.dii.r.mil.uk/
MOD Safety Manager's Toolkit	http://www.aof.mod.uk/aofcontent/tactical/safety/content/techniques.htm
The Nimrod Review by Charles Haddon-Cave QC	http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf
US Forces Safety (Navy, Army and Air Force)	http://www.safetycenter.navy.mil/index.asp https://safety.army.mil/ http://afsc.af.mil/
Engineering Safety Management for Railways (the Yellow Book)	http://www.yellowbook-rail.org.uk/
The Aviation Safety Network	http://aviation-safety.net/index.php
The Centre for Software Reliability (incl. Safety Critical Systems Club)	http://www.csr.ncl.ac.uk/
Forum on Risks to the Public in Computers and Related Systems	http://catless.ncl.ac.uk/Risks
Defence Standards	http://www.dstan.mod.uk/home.html

MOD Safety Management Offices

Further guidance and information on Safety Management can be obtained from the relevant MOD Safety Management Office.

DE&S Safety and Environmental Protection Group
DESSESEP-Acq-Safety@mod.uk

Ship Safety Management Office (SSMO)
DESSESea-SSMO@mod.uk

Land Systems Safety Office (LSSO)
DESSELand-LSSO@mod.uk

MOD Airworthiness Regulator (MAA)
MAA-Tech-Reg-1@mod.uk

Defence Ordnance Safety Group – Safety Management Office (DOSG SMO)

Printed on paper made from a minimum of 75% de-inked post-consumer waste using a chlorine-free process.

MINISTRY OF DEFENCE