



Ministry
of Defence

An Introduction to **System Safety Management in the MOD**



PART I

System Safety
Concepts and
Principles

ISSUE 4 – 2018

© 2018, 2020 MOD all rights reserved

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. The safety of MOD employees and others affected by its activities can only be achieved through a clear understanding of the risks involved, continuous vigilance and effective management of risks throughout the system lifetime.

MOD is building on a history of generally good safety management and is learning lessons from other sectors to ensure that safety is managed successfully and continuously improved in all areas of its responsibility.

DE&S has to provide a safe working environment for its own people and also safe equipment, systems and services that it acquires and supports for the Armed Forces. 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 (SofS) for Defence issues MOD's Health, Safety and Environmental Protection Policy stating (*inter alia*) that he requires that:

We minimise work-related fatalities, injuries, ill-health and adverse effects on the environment, and we reduce health and safety risks so that they are as low as reasonably practicable (ALARP) and tolerable. (April 2020)

Purpose

This document 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 document are intended for information and must therefore not be used as the basis for any contract or instruction to contractors. It can provide a reminder of training course material but cannot replace formal training.

The terminology used in this document is aligned with the Acquisition Safety and Environmental Management System (ASEMS) and with Def Stan 00-056.

The document does not attempt to cover safety tools and techniques in detail, as is done in MOD's System Safety Practitioner (SSP) courses and in the MOD ASEMS Toolkit (see reference documents at the end).

Main changes for Issue 4

Issue 4 of MOD's Safety "White Book" has been produced eight years after issue 3 and it includes new content to reflect some significant changes in the way in which MOD manages system safety. The Defence Safety Authority (DSA) has been established as an independent authority, empowered under charter from the SofS to undertake the roles of safety regulator across defence, investigator of defence accidents and Defence Authority for safety, health and environmental protection. MOD has also introduced the Duty Holder concept for those individuals with particular responsibility for safe operation of systems, facilities and activities which might pose a significant risk to life.

Issue 4 has been structured into two parts, with Part I covering general concepts and principles and Part II describing how system safety is managed in the MOD acquisition process.

The document includes some examples of good practice and also provides warnings against areas of common poor practice. These are highlighted in text boxes that are coloured green and red respectively. New material has been added to cover safety for service provision acquisition projects.

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 team**

e-mail: DESEngSftyQSEPSEP-App@mod.gov.uk

Issue 4 (2018, reissued with minor amendments May 2020)

Part I – Introduction to System Safety Concepts and Principles

Many of MOD's activities have the potential to cause significant harm, including the risk of fatality to MOD personnel (both in DE&S and Front Line Commands), contractors or members of the public. Particular responsibilities lie with the individuals who manage and control those activities that are judged to pose a Risk to Life.

Part I introduces the most important concepts and principles for effective System Safety Management. These apply in any sector, but this booklet highlights their relevance in the Defence environment.

Part I covers topics that are in MOD's System Safety In Action (SSIA) training course.

DE&S has to provide a safe working environment for its own people and also safe equipment, systems and services that it acquires and supports for the Armed Forces.

Part II is a separate document that builds on the content of Part I and describes how system safety is managed in the MOD acquisition process throughout the lifecycle.

Contents

1 INTRODUCTION	6	6 SAFETY RISK MANAGEMENT	38
1.1 Safety Matters.....	6	6.1 Introduction.....	39
1.2 Why Manage Safety?.....	7	6.2 The Hazard Log.....	39
1.3 Judgement and Evidence	8	6.3 Risk Management and Assessment.....	40
1.4 How MOD Manages System Safety	8	6.4 Making Risks ALARP	41
2 WHAT IS SAFETY?	10	6.5 Risk Ownership, Management and Referral.....	42
2.1 General.....	10	6.6 Safety Risk Management in Service.....	43
2.2 Safety.....	10	7 SAFETY ASSESSMENT TECHNIQUES.....	44
2.3 What a System Includes.....	11	7.1 Introduction.....	44
2.4 Physical and Functional Safety.....	12	7.2 Hazard Identification Techniques.....	46
2.5 Hazards.....	12	7.3 Causal Techniques.....	46
2.6 Accidents and Incidents	13	7.4 Consequence Techniques.....	47
2.7 “How Safe is Safe?”	13	Final thoughts.....	48
2.8 Risk, Tolerability and ALARP.....	14	Further sources of information	48
2.9 Risk during times of Conflict and Training.15		Standards and MOD Publications.....	48
3 SAFETY RESPONSIBILITIES AND THE LAW 18		Textbooks and Guides.....	48
3.1 Why is Safety Important to the MOD ?.....	18	Websites.....	49
3.2 Legal Duties of Care.....	19		
3.3 Legal Responsibilities.....	19		
3.4 Regulations, Guidance and EC / EU Directives.....	20		
3.5 Supply Law, User Law and CE Marking.....	21		
3.6 MOD Policy.....	22		
3.7 Health and Safety Regulation of MOD.....	22		
3.8 MOD Duty Holder Approach.....	24		
3.9 Delegation of Safety Tasks within MOD.....	25		
4 SAFETY COMPETENCE AND CULTURE	26		
4.1 Safety Competence	26		
4.2 The Culture of Safety.....	28		
4.3 A Just Culture.....	29		
4.4 Incident and Accident Reporting and Investigation	30		
4.5 Continuous Improvement.....	31		
5 THE MANAGEMENT OF SAFETY	32		
5.1 Who Manages Safety?.....	32		
5.2 Pre-requisites to Successful Safety Management	32		
5.3 Setting Safety Requirements.....	32		
5.4 Safety Management Planning.....	36		
5.5 Safety Committees.....	37		

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 some 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 or people they care about. 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 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 usually indications of a failure on the part of management. The official inquiry report on

the capsizing 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 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.

1 Introduction (continued)

Figure 1: Key Elements of Successful Safety Management (adapted from 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.

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 something 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 the Defence Safety Authority (DSA) DSA01 suite of documents, particularly DSA01.1 which amplifies the Secretary of State for Defence’s (SofS) policy statement for Health, Safety and Environmental Protection (HS&EP).

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 “insurance”) function is responsible for meeting the defined standards.

The SofS’s policy statement also identifies each Top Level Budget (TLB) holder and each Chief Executive

of Trading Fund Agencies, Bespoke Trading Entities and the Defence Infrastructure Organisation (DIO) as Senior Duty Holder (SDH) for safety of defence activities in their own area of responsibility. They have systems for explicitly delegating down the management chain, the authority for implementing safety policy and also 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 Part II, the companion publication to this booklet). 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 00-056 is the contractual document normally used to define the 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.



2 What is Safety?

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. 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 Part II, the companion publication to this booklet).

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

2.3 What a System Includes

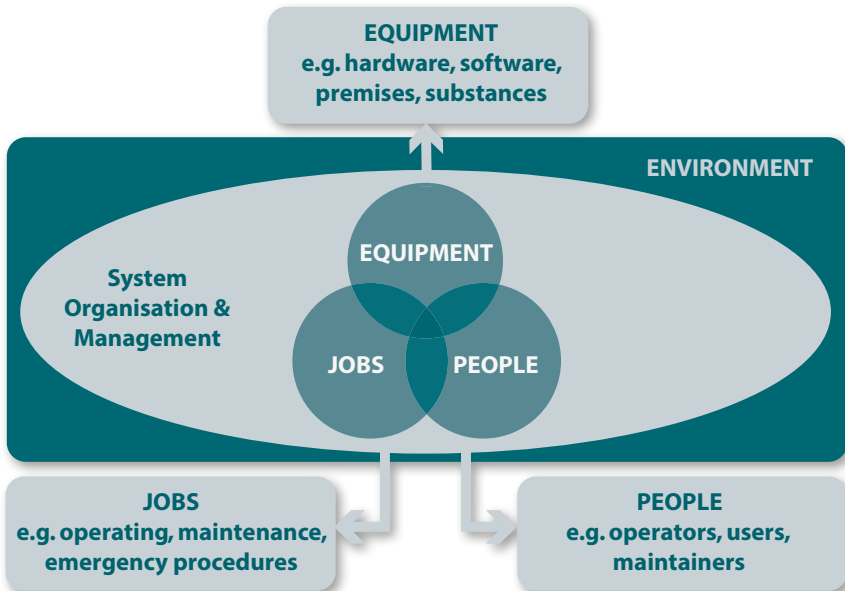
When considering safety, it is essential to recognise that a system includes more than just the equipment hardware. Safety management must cover the software, human, procedural and organisational aspects as well as the system hardware.

A **system** is defined in Def Stan 00-056 as “a combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate.”

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 operating 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.

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



2 What is Safety? (continued)

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, be that controlling equipment or providing people with important information.

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 to cause adverse impact on people, including fatality, physical or psychological injury or damage to health.*” [based on Def Stan 00-056].

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 an 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.

Figure 3: An Accident Sequence



2.6 Accidents and Incidents

An **accident** is defined in Def Stan 00-056 as “an event, or sequence of events, that causes unintended harm.” The accident is the undesired outcome, rather than the initiating event or any intermediate state.

Figure 3 above 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 in Def Stan 00-056 as “the occurrence of a hazard that might have progressed to an accident but did not.” “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, right) and for various industry sectors (Table 2, page 14) (the figures are historical averages based on data from the HSE publication *Reducing Risks, Protecting People*).

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.

Table 1: Annual Risk of Death for Various Causes

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

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

2 What is Safety? (continued)

working year, and so individual systems should present only a fraction of the **total** risk that is considered “tolerable”.

Table 2: Annual Risk of Death from Industrial Accidents

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

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 of something valuable. 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 possibility of 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, thereby allowing corrective action to be taken where it will have most benefit.

Although an individual who is killed is probably not concerned whether they die 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. This is important because the public response to a catastrophic event with many deaths is greater than multiple smaller occurrences with the same total number of fatalities.

Assessment of risk should cover both individual and societal risks. (see Section 7 on analysis techniques)



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, Table 3, 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.

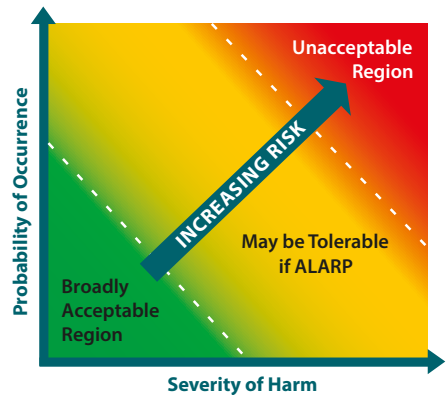
Table 3: Average Risk of Death for Various Activities

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

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”.

Figure 4: Risk as a Combination of Severity and Probability



2 What is Safety? (continued)

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 needed in the “Tolerable if 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

Combat Immunity is a legal concept which establishes that there is no common law liability for negligence for acts or omissions on the part of those who are actually engaged in armed combat. It is very much circumstance-dependent and will usually only be identified after the incident when MOD is facing an allegation that the duty of care has been breached and legal action is being taken. It is not a concept that can be invoked ahead of a situation to suspend the duty of care but rather it may be argued, after the incident, that the circumstances at the time constituted those that warrant Combat Immunity.

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 systems 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.



MOD takes system safety very seriously for sound reasons, including to:

- Avoid harm to people and also the environment
- Comply with the law
- Comply with safety regulations and policy
- Maintain defence capability, both equipment and morale
- Maintain MOD's reputation
- Avoid diversion of resources after accidents

And also for moral reasons: **good safety management is the right thing for MOD to do.**

3.2 Legal Duties of Care

A **duty of care** is a formalisation of the “social contract”, meaning the implicit responsibilities held towards other people in society. There is a legal obligation on everyone to take reasonable care to avoid acts or omissions which they can reasonably foresee would be likely to harm someone else, whether that harm is physical, mental or economic.

The legal obligations are from three sources:

- Specific duties defined by statute law
- Accepted general duties of care, such as those owed by motorists to other road users
- Duties developed through common law rulings

Where a duty of care exists, the law requires people to achieve a **standard of care** “*that would be exercised by the reasonably prudent professional in that line of work.*”

Some duties of care can be on organisations and others rest with individuals, as we will see from the following overview of legal responsibilities for safety.

3.3 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 legislation, including the Health and Safety at Work etc. Act (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.

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)

3 Safety Responsibilities and the Law (continued)

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.

3.4 Regulations, Guidance and EC / EU 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. Many of 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 and issued by the HSE 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 produced by standards making bodies (e.g. ISO, BS, IEC) can have a similar status 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 / EU Directives are binding on member states (rather than directly on individuals or organisations) but they are implemented in UK law through regulation if necessary.

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

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

3.5 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 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). 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 Safety Responsibilities and the Law (continued)

3.6 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, safety and environmental protection (HS&EP) throughout the MOD and produces a statement of safety and environmental policy. In summary, the policy is that SofS requires that:

- ▶ *We minimise work-related fatalities, injuries, ill-health and adverse effects on the environment, and we reduce health and safety risks so that they are as low as reasonably practicable (ALARP).*
- ▶ *Within the UK we comply with all applicable HS&EP legislation.*
- ▶ *Overseas we apply our UK arrangements where reasonably practicable and, in addition, respond to host nations' relevant HS&EP expectations.*
- ▶ *Where Defence has exemptions, derogations or dis-applications from HS&EP legislation, we maintain Departmental arrangements that produce outcomes that are, so far as reasonably practicable, at least as good as those required by UK legislation.*
- ▶ *Those of us in positions of management or command, from the Defence Board downwards, lead by example on HS&EP as part of normal business and maintain a part culture where everyone is empowered to contribute to HS&EP objectives.*
- ▶ *We take reasonable care of the health and safety of ourselves and others who may be affected by our acts or omissions at work, we protect the environment and we co-operate with arrangements that are in place to enable us to discharge the duties placed on us.*

The SofS' Policy Statement also defines the governance arrangements for HS&EP and refers out to the detailed organisation and arrangements that are now contained in DSA01.1.



3.7 Health and Safety Regulation of MOD

Most defence activities are fully subject to health and safety legislation and are regulated by Statutory Regulators such as the Health and Safety Executive (HSE), the Maritime and Coastguard Agency (MCA), the Office for Nuclear Regulation (ONR), Local Authorities etc. The regulatory regimes vary according to the legislation empowering each regulator and many of these Statutory Regulators have a Memorandum of Understanding (MoU) with MOD that defines areas of responsibility, rights of access, powers of enforcement etc.

Certain legislation does not apply to Defence on the grounds of national security. Some legislation includes a specific **Disapplication** for Defence. Other legislation allows for Defence to apply for **Exemptions**, usually on a case-by-case basis. MOD may also have a **Derogation** or partial suppression / delay in implementation of other legal requirements.

Defence Safety Regulators in the DSA, empowered by SofS through a specific Charter, operate regulatory regimes which are aligned, where possible, with the civil equivalents. The Defence Safety Regulators and their areas of interest consist of:

- **Defence Fire Safety Regulator (DFSR)** (fire safety)
- **Defence Land Safety Regulator (DLSR)** (land systems; movements and transport; fuel and gas)
- **Defence Maritime Regulator (DMR)** (maritime including diving)
- **Defence Nuclear Safety Regulator (DNSR)** (nuclear and radiological)
- **Defence Ordnance, Munitions and Explosives Safety Regulator (DOSR)** (OME; Major Accident Control Regulations (MACR); range safety; laser safety)
- **Military Aviation Authority (MAA)** (military air safety)



3 Safety Responsibilities and the Law (continued)

Each Defence Safety Regulator has produced a set of Regulations (see reference documents) and they set, enforce and assure the mandatory requirements for their own area, using an organisation that has authority and independence from financial, political and operational pressures.

3.8 MOD Duty Holder Approach

We saw in Sections 3.2 and 3.3 that some legal duties apply to organisations and others to individuals. The term “**duty holder**” is sometimes used to identify the person or organisation holding a specific legal duty, particularly those placed by the Health and Safety at Work Act, the Management of Health and Safety at Work Regulations (MHSWR) and the Control of Major Accident Hazard (COMAH) Regulations. The use of the term legal duty holder can provide clarity about who is legally responsible for what, and so avoid safety issues “falling through the cracks” or being lost within the hierarchy of large and complex organisations.

The **legal duty holder** would be **legally** accountable according to the legal duty's scope and whether it is an absolute duty or qualified, for example “so far as is reasonably practicable”.

MOD has introduced a system of appointing individuals as “Duty Holder” where a defence activity is judged as involving very significant

hazards. This approach seeks to provide clarity about who is responsible for the safety of specified activities. The MOD Duty Holder regime currently has three tiers, from Delivery Duty Holder, through Operating Duty Holder and up to Senior Duty Holder. Information on significant safety risks would be escalated through the organisation's Duty Holder chain for consideration and action, ultimately to SofS.

The MOD Duty Holder approach does not alter or remove any **legal** duties on MOD, DE&S, other organisations or individuals. The **MOD Duty Holder** has no different or additional legal responsibilities, due to their identification as “MOD Duty Holder”, but they can be held to account for their actions (MOD accountability rather than legal accountability).

As a Crown Body the MOD cannot be prosecuted by the Crown for failings against duties from Criminal Law such as HSWA, but MOD may be censured in respect of offences which would have led to prosecution of private sector organisations. Individuals would not be prosecuted in substitution for MOD or if there were defects in the management organisation.

MOD Duty Holder

- Always an individual employee of MOD
- Formal appointment through Letter of Delegation as part of Duty Holder chain
- Duty Holder approach provides clarity of individual responsibility for **safe operation** of high hazard systems, facilities and activities that they manage or direct
- **No additional legal** duties due to appointment
- Can be held accountable in MOD

Legal duty holder

- Sometimes an organisation, sometimes a person
- Clear and explicit legal duties from statute or common law
- Duties from legislation may relate to operation, design, manufacture, maintenance etc.
- Can be held accountable in law

3.9 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 Delivery 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



4 Safety Competence and Culture

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

Competence is defined by the Engineering Council as *“the ability to carry out a task to an effective standard. Its achievement requires the right level of knowledge, understanding and skill, as well as a professional attitude.”* It is important that an individual’s safety competence should be matched to their role and accountability.



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 00-056 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 components including:

- Skills
- Knowledge
- Understanding
- Attitudes and personal qualities

Figure 4: Elements of Individual Competence and Their Development



An individual's safety competence should be developed through a combination of education, training and practical experience. A person's level of ability in each component part (or "competency") may be indicated by qualifications or tests, but other abilities must be assessed from evidence of relevant experience and previous achievement.

Even where a person has the intrinsic ability needed to do a job, their actual effectiveness may be reduced, for example by:

- Poor fitness (physical, medical or mental)
- Lack of appreciation of their own limitations
- Working in difficult situations (e.g. in an emergency or with degraded equipment)
- Poor organisation, inadequate resources, poor work processes

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.

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 Safety Competence and Culture (continued)

4.2 The Culture of Safety

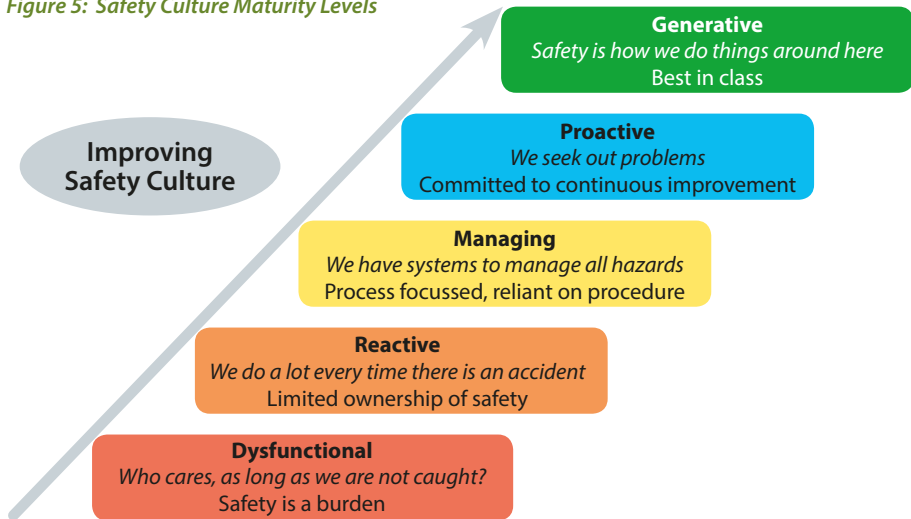
Safety culture is defined as “the product of individual and group values, attitudes, perceptions, competences, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation’s health and safety management.” (UK Health and Safety Commission).

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. The “safety culture” of

an organisation can be considered under the following three headings, and the maturity of that culture is sometimes measured on a scale with several levels:

- **Psychological aspects:** how people feel (the ‘safety climate’)
- **Behavioural aspects:** what people do (safety-related behaviours & actions)
- **Situational aspects:** what the organisation has (policies, procedures, systems)

Figure 5: Safety Culture Maturity Levels



Signs of a poor Safety Culture

- **Profit/performance before safety:** safety viewed as a cost, focus on short term
- **Fear:** problems hidden by those trying to avoid sanction
- **Ineffective leadership:** blinkered leaders and poor decision making
- **Miscommunication:** (undiluted) critical information not reaching decision makers
- **Competency failures:** inadequate staff competence and organisation’s capability
- **Ignoring problems:** warning signs not recognised, shared or acted on

4.3 A Just Culture

Safety culture requires an atmosphere in which individuals are not unduly blamed or punished 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 reckless or 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.

Figure 6: Components of Safety Culture (based on James Reason's model)



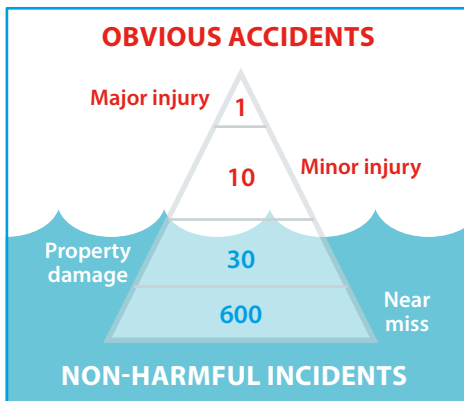
4.4 Incident and Accident Reporting and Investigation

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 or contribute to a hazard. Each incident provides potential for learning and it is important that events are not dismissed quickly as one-offs.

Figure 7: The "Iceberg" of Accident and Incident Statistics



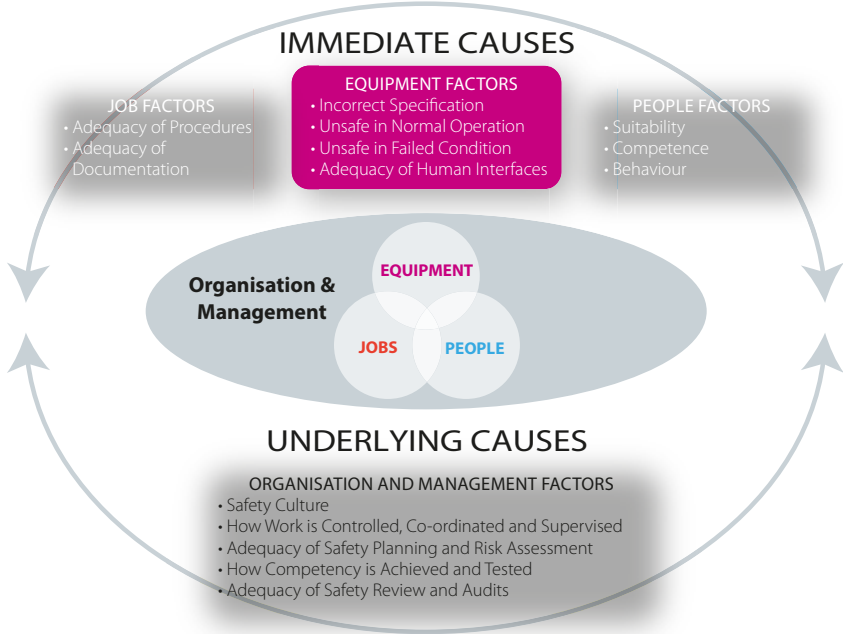
Studies from a range of industries have shown that there is consistently a much greater number of less serious incidents than those which led to an injury. Often it was only a matter of chance that these near misses or non-injury accidents didn't harm people. Figure 7 illustrates the "iceberg" of accident 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.)
- Experienced and knowledgeable people should investigate the incident (how and why did it happen?) and determine the causes, both immediate and underlying
- 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 8.

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 Delivery Team and designers.

Figure 8: Immediate and Underlying Causes of Accidents



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
- Learning From Experience (LFE) events and publications - active
- 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.

5 The Management of Safety

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 strong 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 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 driving down 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 bound 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 domain, function, or role, but will include one or more of the following:

Legal and Regulatory Requirements which 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 Regulatory Requirements which are published by the Defence Safety Regulators for each area of responsibility. For example, regulations for MOD shipping in DSA02-DMR and Land Systems Safety and Environmental Protection in DSA02.DLSR.LSSR.

MOD Certification Requirements which 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.

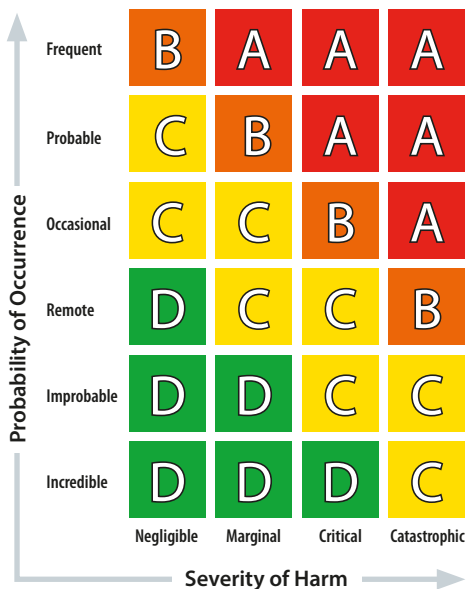
Safety Related Standards which will include MOD, British, international or other applicable

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.

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.

Figure 9: A Risk Classification Matrix



5 The Management of Safety (continued)

The Risk Classification Matrix in Figure 9 is a version of the risk diagram illustrated in Figure 4, but where the continuum has been divided 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 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 risk 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

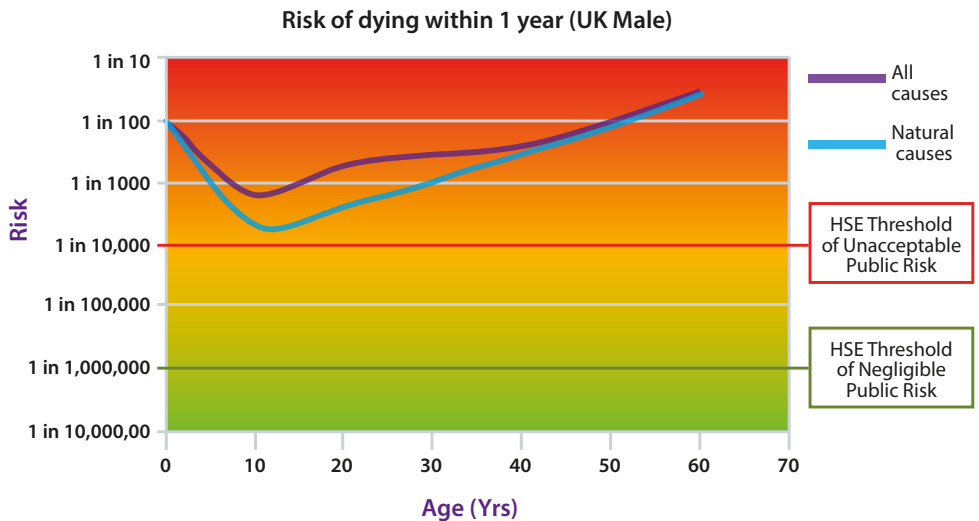
probability bands for the particular system, together with the choice of relevant units for frequency.

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 10 has a graph showing the average annual risk of dying for males in the UK, and how this varies with age. HSE statistics 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 close to the lowest level of risk that people face from natural causes at any point in their lifetime 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".

Quantitative risk targets should be chosen

Figure 10: Risk Thresholds Compared with Average Fatality Rates (n.b. logarithmic scale for Risk)



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 tailored 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 Report 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 reviewed and 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 which 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 an 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 sector or technology Safety Standards which use **Safety Integrity Levels (SILs)** or similar concepts (e.g. Safety Assurance Levels). 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 apply to “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

5 The Management of Safety (continued)

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 can be used by the customer or Delivery 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) (including ease of use, protection against human error, ability to recover from errors)
- 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.

For an acquisition project both the MOD and the supplier 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, dependencies, 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 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 testing that safety features operate as they should and reviewing all safety incidents which occur.



6 Safety Risk Management

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 the principal means of tracking the status of all identified hazards, decisions made and actions taken to reduce risks, and should be used to facilitate oversight by the Project Safety Committee (PSC) and other stakeholders.

The hazards, accident sequences and accidents recorded are those which could conceivably occur, as well as those which have already been experienced. The term hazard log is slightly misleading as the information stored relates to the entire safety programme and covers accidents, controls, risk evaluation and ALARP justification, as well as data on hazards.

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.

Records can be tracked by the use of a status field, which for example, identifies whether the record has just been opened, or is awaiting confirmation of mitigation actions, or is ALARP.

Hazards should not be deleted from the hazard log, but closed and marked as “out of scope” or “not considered credible”, together with appropriate justification. Where such hazards are no longer considered relevant to the system, the hazard log entry should be updated to reflect this.

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



The hazard log contains the traceable record of the hazard management process for the project and therefore:

- Ensures that the project safety programme uses a consistent set of safety information
- Facilitates oversight by the Project Safety Committee and other stakeholders of the current status of the Safety activities
- Supports the effective management of possible hazards and accidents so that the associated risks are brought up to and maintained at a tolerable level
- Provides traceability of safety decisions made

eCASSANDRA (a web-enabled version) are the MOD-preferred tools for constructing hazard logs and eCASSANDRA has been mandated for all new DE&S projects. Commercially available tools include HARMS, SMART and SMARTER.

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.

6 Safety Risk Management (continued)

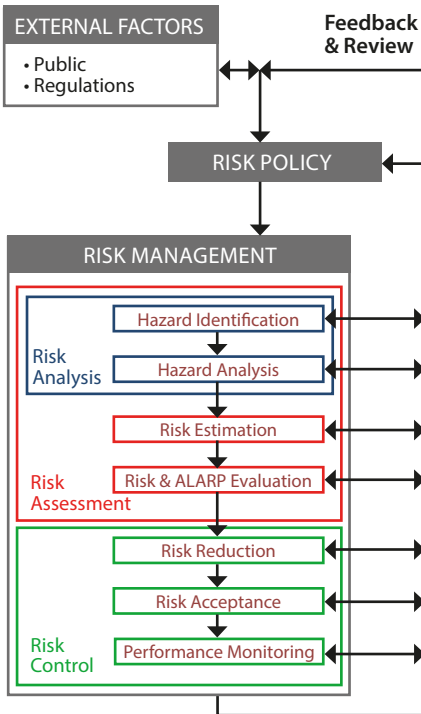
6.3 Risk Management and Assessment

Risk management is defined as “*The systematic identification, evaluation and reduction of risk.*” (Def Stan 00-056).

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. Risk decisions should be supported by qualitative assessment methods, complemented where necessary by quantitative methods. Quantitative methods are particularly appropriate where the

Figure 11: The Risk Management Process (after Def Stan 00-056)



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”.

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; Figure 11 shows the Def Stan 00-056 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 revision 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:

1. Elimination of the hazard
2. Substitution of the hazard (e.g. by use of alternative substances or procedures)
3. Hazard control by engineered means (e.g. physical protective measures such as interlocks or guards)
4. Hazard control by administrative means (e.g. procedural or training)
5. Protect against hazard effects (e.g. with Personal Protective Equipment)

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 of ensuring, “So Far As is Reasonably Practicable”, that people are not exposed to risks. 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 that would be suffered by injured parties,



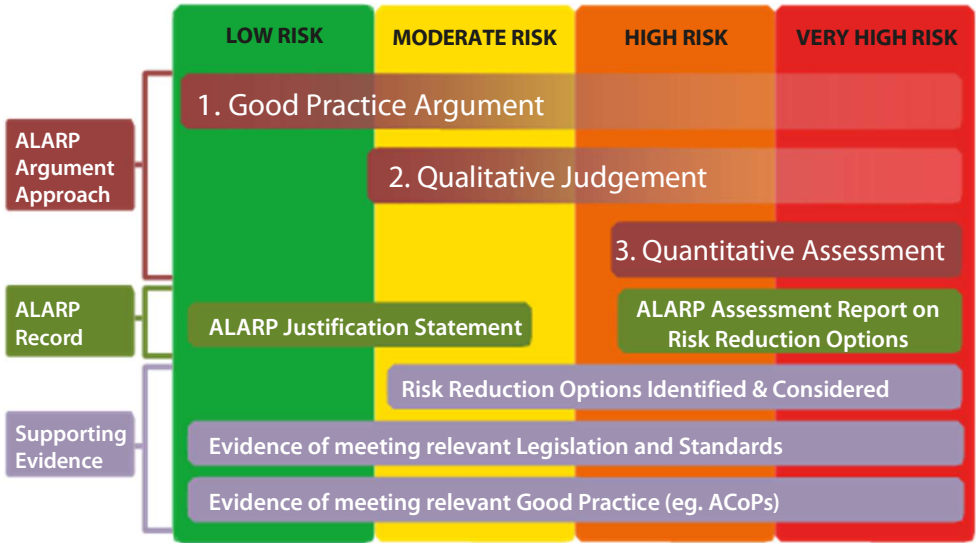
then using value this to decide whether the costs associated with possible further risk reduction measures can be justified. Great care is therefore required to ensure that disproportion factors are correctly considered and that the conclusion is explored for its sensitivity to assumptions.

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 hazards 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 Safety Risk Management (continued)

Figure 12: How to Show ALARP



6.5 Risk Ownership, Management 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 agreeing who will lead on management actions where appropriate.

Risk classification and prioritisation (eg. 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.

6.6 Safety Risk Management in Service

Safety risk management during development is mainly proactive and consists of trying to understand, forecast and control possible safety risks before there is any real risk exposure for people. Once a system comes into service, there can be real exposure to the risk of harming people and this means that risk management changes in emphasis: there must be:

- (Proactive) Attention to detail when controlling those risks already identified (see below)
- (Reactive) Vigilance to detect any signs that unexpected hazards might affect the system:
 - Incident and accident reporting, investigation and resolution
- (Proactive) risk management for any changes, for example changes to:
 - System operation / context / modification / aging / manning / organisation



Throughout the in service period, the agreed safety risk control measures must be correctly implemented or the expected level of residual safety risk will be exceeded:

- Compliance with the intended controls to the intended standards, e.g.
 - System operation within defined “safety envelope”
 - Material state of system safety features (e.g. indicators, alarms, shutdowns, barriers)
 - Competence and manning levels for Operators & Maintainers
 - Working to procedures (no short cuts or work arounds)
 - Emergency preparedness (e.g. evacuation plans, emergency equipment)
- Assurance that this is being achieved for safety critical elements, e.g.
 - Inspections, audits, exercises, incident reviews, contractual metrics
 - Corrective action and/or enforcement if shortfalls are detected.



7 Safety Assessment Techniques

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.

7.1 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.

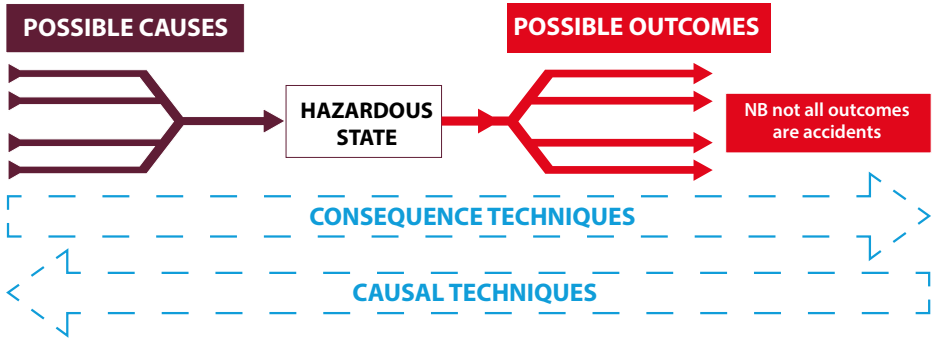
Designers concentrate on normal operation rather than abnormal. A safety assessment should ask how a system could fail, not only how it will work. It requires the use of imagination to determine possible sequences of events leading to accidents.

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 ASG.



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 best 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.

A safety Risk Classification Matrix (RCM) can provide a framework for ranking or classifying safety issues according to their significance. Such RCMs provide a broad brush **Risk Evaluation** technique, to highlight and prioritise the value an organisation places on exposure to possible future losses.

Objective information on accident likelihood and severity is taken from safety analyses (see below) and then evaluated using **subjective** value criteria.

7 Safety Assessment Techniques (continued)

7.2 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.

7.3 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.

7.4 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.

Bow-tie diagrams cover the full accident scenario from causes to consequences. Their graphical representation can enable clear communication with non safety specialists about the current status of Risk Control Measures, risk exposure and critical areas.

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.



Final thoughts

The MOD operates in what is the most challenging and varied environment for safety and this 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 incidents and accidents both in defence and in other sectors.

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

Further sources of information

Standards and MOD Publications

BS OHSAS 18001:2007.....	Occupational Health and Safety Management Systems Requirements Standard
Def Stan 00-056.....	Safety Management Requirements for Defence Systems
Def Stan 00-055.....	Requirements for Safety of Programmable Elements (PE) in Defence Systems
DSA01.1	Defence Policy for Health, Safety and Environmental Protection
DSA02-DMR.....	MOD Shipping Regulations for Safety and Environmental Protection
DSA02.DLSR.LSSR.....	Land Systems Safety and Environmental Protection
JSP 518	Regulation of the Naval Nuclear Propulsion Programme
JSP 520	Safety and Environmental Management of Ordnance, Munitions and Explosives over the Equipment Acquisition Cycle
JSP 538	Regulation of the Nuclear Weapons Programme
MRP.....	Military Aviation Authority Regulatory Publications
POSMS.....	DE&S's Project-Oriented Safety Management System
Mil Std 882 E.....	US Department of Defense Standard Practice for System Safety
BS EN 61508.....	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

Textbooks and Guides

The Health and Safety Executive **"Managing for Health and Safety"** HSG65 3rd Edn. 2013

The Health and Safety Executive **"Reducing Risks, Protecting People"** (R2P2) ISBN 0-7176-2151-0 2001

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 **"Code of Practice: Competence for Safety-related System Practitioners"** 2016

RSSB **"Taking Safe Decisions – How Britain's railways take decisions that affect safety"** Version 2.1 2014

Safety Critical Systems Club **"Data Safety Guidance"** Version 3 SCSC-127C ISBN-10: 1981662464 2018

Websites

Defence Safety Authority (DSA)	www.gov.uk/government/organisations/defence-safety-authority
Health and Safety Executive (HSE)	www.hse.gov.uk
Royal Society for the Prevention of Accidents (ROSPA)	www.rospa.com
Safety and Reliability Society.....	www.sars.org.uk
The International System Safety Society.....	www.system-safety.org
The Hazards Forum.....	www.hazardsforum.org.uk
The Safety-Critical Systems Club.....	https://scsc.uk/
Institution of Engineering and Technology (IET) – Systems Safety Engineering Technical and Professional Network.....	https://theiet.org/safety
MOD Acquisition Systems Guidance – Safety and Environmental Protection.....	www.aof.mod.uk/aofcontent/tactical/safety/content/introduction.htm
<i>Log in to ASG required for access to these pages</i>	
Acquisition Safety and Environmental Management System – Online.....	https://www.asems.mod.uk/
MOD Safety Manager’s Toolkit.....	www.asems.mod.uk/toolkit
US Forces Safety (Navy, Army and Air Force).....	http://www.public.navy.mil/NAVSAFECEN/Pages/index.aspx http://safety.army.mil/ https://safety.af.mil/
The Aviation Safety Network.....	www.aviation-safety.net
Forum on Risks to the Public in Computers and Related Systems	http://catless.ncl.ac.uk/Risks



Ministry
of Defence