Ministry of Defence

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

PART II

System Safety in MOD Acquisition

ISSUE 4 – 2018

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). (August 2014)*

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 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 Safety Managers Toolkit (see reference documents at the end).

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

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: **DESTECH-SEPApplications@mod.uk**

Issue 4

Part II – System Safety Management in the MOD Acquisition Process

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 the Front Line Commands), contractors or members of the public. Particular responsibilities lie with the individuals who manage and control such activities that are judged to pose a Risk to Life.

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 I is a separate document that introduces the most important concepts and principles for effective System Safety Management. It forms the foundation for Part II and so should be read first.

Part II concentrates on how system safety is managed in the MOD acquisition process throughout the lifecycle. It is relevant whether the acquisition activities are done by DE&S, by contractors and suppliers working for DE&S or by other members of the "acquisition community".

System safety in acquisition is a wider matter than "product safety" or "equipment safety", since it can apply to service provision as well as to tangible items and also deals with all Defence Lines of Development, not just the equipment DLOD.

Part II covers topics that are in MOD's System Safety Process Management (SSPM) course.

Contents

1 DE&S Governance of System Safety in Acquisition

Key Messages

Governance is the system by which the most senior managers lead, direct and control their organisation.

Safety governance involves setting safety values, standards and objectives for the whole organisation to follow. It also includes clear definition of safety responsibility and accountability through an organisation and holding management to account.

DE&S has an explicit policy for both workplace safety and the safety of its work outputs ("acquisition safety").

Each Operating Centre in DE&S has governance arrangements for acquisition safety.

Other stakeholders involved in acquisition, including through the supply chain, must also have their own governance arrangements, appropriate to their role and activities.

1.1 Introduction

Governance is the system for direction and control of organisations by the most senior managers (usually the board of directors for businesses). It includes strategic direction, defining responsibilities, internal controls and assurance. It is distinct from **management** – which can be thought of as the regular day-to-day decisions and actions required to run the organisation.

The key elements of governance, for which boards of directors are responsible are:

- Leading the organisation and establishing the overall strategic direction
- Setting values and standards for the organisation and clear objectives for management – and delineating the limits of their responsibility
- Holding management to account for their performance in running the organisation
- Upholding obligations to the owners (e.g. shareholders, the government) and other interested parties
- Overseeing internal controls

In setting the strategic aims for the organisation, the board will benefit from a fundamental understanding of the role safety plays in the overall performance of the organisation. Furthermore, their leadership role and influence in setting clear values and standards to work by, is key to establishing the culture of the organisation, including the Safety Culture.

Investigations into the causes of many major accidents has identified failures of safety governance as a significant contributory factor. For example the Inspector charged with the investigation into the King's Cross Underground Fire in 1987 blamed the board for having loose supervision on the safety management of a subsidiary company:

> *"In my view it is imperative that a holding company charged with ensuring safety of operation should discharge its duty fully. It is not acceptable that it should try to discharge that duty by delegating it to its subsidiary, coupled with maintaining a loose supervision by having on the board of the main company a director of the subsidiary company."*

Part I, the separate introduction to concepts and principles, has outlined the governance arrangements that MOD applies to system safety, including the Regulatory arrangements, the SofS Policy and the system of Letters of Delegation for authority for discharging safety responsibilities. This section describes the arrangements for system safety governance in DE&S, particularly as those apply to DE&S' acquisition activities. Other organisations involved in defence, such as FLCs, suppliers and contractors, will also have their own governance arrangements for system safety.

1.2 DE&S's Role in Achieving Safety

Much of DE&S's work activity is low risk in nature and carried out in well-controlled office environments. But some of what DE&S does involves significant hazards, for example maritime salvage and trials activities and also the operation of Defence Munitions establishments. DE&S also has to provide safe equipment, systems and services that it acquires and supports for the Armed Forces (sometimes called "acquisition safety").

Activities undertaken and controlled by FLCs

Even though DE&S does not provide the "controlling mind" for these activities, it has an important part to play, because it usually provided equipment and/or services to be used by the FLC. DE&S would therefore be responsible to for:

- Supplying products, systems and services that are adequately safe to use
- Providing suitable and sufficient information to enable the risks associated with the use of products, systems and services to be appropriately managed

DE&S personnel are also often responsible for managing safety-related certification and release-to-service activities. DE&S personnel who discharge such duties do so under bespoke (to their role) safety LoDs, e.g. Letters of Airworthiness Authority; people performing these roles are not routinely identified as MOD Duty Holders, as they are not in control of activities involving risks.

Activities undertaken and controlled by DE&S

Where DE&S controls activities involving significant hazards it has particular responsibilities to people who might be harmed, and so it has systems in place to ensure that:

- DE&S clearly identifies the person who has the authority for discharging safety responsibilities
- Their scope of responsibility is clearly defined and understood
- They have the necessary competence, resources and support
- There are suitable assurance arrangements, which are commensurate with the risk of the activity

1.3 DE&S Arrangements and Policy for Acquisition Safety

The SofS for Defence is ultimately responsible for all health, safety and environmental matters within Defence. Authority for discharging these responsibilities within DE&S has been delegated to the Chief Executive Officer (CEO) of DE&S, via the Permanent Under Secretary (PUS). The CEO is accountable to SofS for matters of health, safety and environment within DE&S, covering both the working environment (Occupational Health and Safety) and the work outputs of DE&S (acquisition safety).

The CEO of DE&S is personally responsible to PUS for implementing MOD policy for safety and environmental protection. CEO delegates authority to specific individuals to carry out parts of this responsibility. The policy set out in the CEO's Health & Safety Policy Statement must be followed by all DE&S staff involved in the procurement and support of equipment and services. Policy requirements apply to all equipment and services acquired for Government use, supported and managed through DE&S either directly or by agencies operating on its behalf. Specific delegations of authority are covered in separate letters, if required. Holders of safety delegations may, at their discretion and with some exceptions, sub-delegate elements of their tasks. Any sub-delegations must be to specified individuals and in writing.

DE&S Mandated Requirements (Policy):

Those holding safety and environmental delegations are to ensure that in the procuring or supporting equipment and services, they conform to the Secretary of State's Health Safety and Environmental Protection Policy and MOD

standards and regulations set by the safety regulators.

CEO has issued Organisation and Arrangements (O&A) for Health, Safety, and Environment for DE&S covering:

- Policy
- Objectives
- Roles & Responsibilities, including Duty Holder identification and responsibilities
- Management System
- Competent Health, Safety and Environmental Resources
- Safety Committee
- Safety and Environmental Protection (S&EP) Targets, Risk Management and Reporting
- S&EP Culture

1.4 DE&S High-Level Organisational Structure for Acquisition Safety

The **DE&S Board** provides the strategic leadership of DE&S, helping to ensure that DE&S deliver its strategic objectives. This Board is chaired by a Non-Executive Chairperson and has a number of committees underneath it to provide oversight of the delivery of DE&S business.

Under the lead of the CEO, the **DE&S Executive Committee** is responsible for the day-to-day running of the business. It also has a number of sub-committees, including the **DE&S Safety Health and Environment Committee** (SHEC) which provides oversight and assurance of S&EP performance and also advises the CEO on action to take as Senior Duty Holder.

1.5 DE&S Safety Governance for Operating Centres and Delivery Teams

Delivery Teams that conduct DE&S's acquisition activities are grouped into Operating Centres (OC), each led by a Director to whom authority for Safety has been delegated by their Chief of Materiel (CoM). Each CoM holds authority for Safety in their area of responsibility, via their own LoD from the CEO.

Although governance arrangements in the OCs differ in some detailed respects, they comply with common principles that flow from DE&S' Organisation and Arrangements (O&A).

- **OC Directors** are responsible for ensuring that the equipment, systems and services procured, delivered and supported by their OC are fit for purpose and comply with appropriate legislation and regulations. Directors are responsible for ensuring that the resource is available to allow Team Leaders to use their delegated authority and meet the required S&EP performance levels
- Authority for carrying out S&EP responsibilities is delegated by the OC Director to **DE&S Team Leaders**, who are responsible for the management of S&EP activities
- Delivery Teams typically have one or more **Technical Authority** or **Chief Engineer** who is responsible for providing technical support to the TL in relation to system safety. In the air domain, the Type Airworthiness Authority (TAA) would hold a Letter of Airworthiness Authority (LoAA), separate from the TL's Letter of Delegation
- A **Safety** or **S&EP Manager,** will act as the focal point for S&E management activities throughout the team and report to the TL on S&EP performance. The Safety Manager typically does not have delegated authority for decision making, but will have appropriate safety competence to understand safety legislation and policy in their area, so that they can establish and operate a Safety and Environmental Management System (SEMS), provide informed advice to senior managers and act as an "intelligent customer" for S&EP work done by the Delivery Team and its suppliers

1.6 Acquisition Safety Governance for Other Stakeholders

DE&S acquisition activities link supplier capability (both from industry and other parts of MOD) to the military who use the systems, equipment and services that DE&S procure and support. DE&S play a crucial role in co-ordinating and cooperating with its suppliers and customers. In many cases, DE&S's suppliers themselves have sub-contractors and/or suppliers, so the supply chain may extend beyond DE&S's direct contractual relationships.

For Acquisition Safety, DE&S must work with stakeholders to set safety requirements that comply with legislation and regulations whilst

giving the users the capability they require. DE&S's relationships with its suppliers and customers should be formalised through contracts or internal business agreements that define each party's safety responsibilities and how the management interface will operate.

Contracts and agreements cannot alter or remove legal duties on any party, so, for example, a company must always comply with Section 6 of HSWA where it is acting as a designer, manufacturer, importer or supplier.

The law also applies to **service provision**, but contracts and service level agreements must recognise whether and how the service provided could cause harm, either directly or indirectly, and they should specify:

- Which party holds what responsibilities (e.g. for equipment ownership, design, condition, operation, upkeep)
- Required performance and integrity levels for the service outputs
- Assurance and enforcement mechanisms

Whilst the law, contracts, standards and agreements will affect how DE&S interacts with other safety stakeholders, each party must have its own governance arrangements for the direction, control and assurance of its own business.

Key Messages

A Safety Management System (SMS) provides the organisation and processes for safety management activities.

A formal and documented SMS is one of the fundamental requirements of good safety management, but success still depends on the attitudes and behaviours of behaviours of people in the organisation.

SMS can be aligned or combined with the management systems for Occupational Health and Environmental Protection.

SMSs should exist at different levels, from corporate to Delivery Team, within the acquisition community.

MOD applies the Acquisition Safety and Environmental Management System (ASEMS) to all its acquisition projects.

ASEMS is a flexible system, covering all acquisition strategies and technologies, across all domains, to meet the requirements of domain-specific regulations.

ASEMS consists of POSMS for Safety Management and POEMS for Environmental Management.

Compliance with the POSMS and POEMS will ensure that any project's safety and environmental management system is robust, proportionate to the project's levels of risk and is compatible with the DE&S corporate reporting requirements.

Auditing the SMS is an important way of ensuring that good safety management does not decay but is continually stimulated and improved.

2.1 Introduction

Def Stan 00-056 defines a **Safety Management System** (SMS) as *"the organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet Safety Requirements and safety policy objectives."* A formal and documented SMS is one of the fundamental requirements of successful safety management by organisations of all sizes and sectors.

Often the SMS may be combined into an Occupational Health and Safety Management System (OH&SMS), aligned with the Environmental Management System (EMS) or combined into a single Safety and Environmental Management System (SEMS). This section concentrates on the SMS and further information on EMS can be found in the MOD's Green Booklet.

An organisation's SMS must be appropriate for the nature of their work and the relevant legal and regulatory requirements. But some fundamental principles apply to all effective SMSs.

SMSs are usually based on the "Plan-Do-Check-Act" (also known as the Deming cycle) iterative management methodology that underpins many management systems in fields such as quality and process improvement. BS OHSAS 18001 specifies the requirements for an occupational health and safety management system and 18002 provides implementation guidance. OHSAS 18001 can be aligned with ISO 9001 (Quality Management) and ISO 14001 (Environmental Management).

Effective Safety Management Systems must be clearly documented and should have:

- Explicit statement of Safety Policy
- Safety governance and leadership arrangements
- Clear Organisation and Arrangements:
  - Separation of delivery decision making ("ensurance") and assurance
  - Clear safety responsibility and accountability
  - Decision taking at appropriate level of seniority
  - Co-operation with internal and external stakeholders
  - Organisational change management
- Resourcing and safety competence
- Effective safety management processes:
  - Legal and regulatory requirements identification, compliance and exemption
  - Timely, proportionate and effective safety risk management through life
  - Formal safety records, including safety case evidence and argument and risk decisions
- Assurance and audit
  - Safety performance measurement and continuous improvement
  - Management review
  - Audit
  - Closed loop incident reporting, investigation and corrective action
  - Learning From Experience

HSE advise that key safety documents should be kept functional and concise, with the emphasis on effectiveness rather than sheer volume of paperwork. They warn that focusing too much on the formal safety documentation of a SMS will distract from addressing the human elements of its implementation – the focus becomes the process of the system itself rather than actually controlling risks.

HSE also stress that just having a SMS is not enough: success still hinges on the attitudes and behaviours of the people in the organisation (sometimes referred to as the **"Safety Culture"** - see Part I).

2.2 Safety Management Systems for Acquisition

Corporate Level: DE&S applies the Acquisition Safety and Environmental Management System (ASEMS) to all their acquisition projects. It is a flexible system which can be applied by Delivery Teams for projects of all acquisition strategies and technologies, across all domains to meet the requirements of domain-specific safety regulations.

ASEMS has three parts:

- Part 1 Policy
- Part 2 Instructions, Guidance and Support
- Part 3 Assurance and Audit

The use of ASEMS is mandated for all DE&S projects. By applying the policy, instructions and guidance described in the three parts of ASEMS, projects are able to demonstrate the implementation of effective and efficient safety and environmental management process which comply with legislation and departmental policy. The aim is to ensure that all appropriate precautions are taken to prevent harm to personnel and protect the environment, consistent with providing the operational capability required by the customers of DE&S.

At the core of the ASEMS there are two systems manuals: the Project Oriented Safety Management System (POSMS), and the Project Oriented

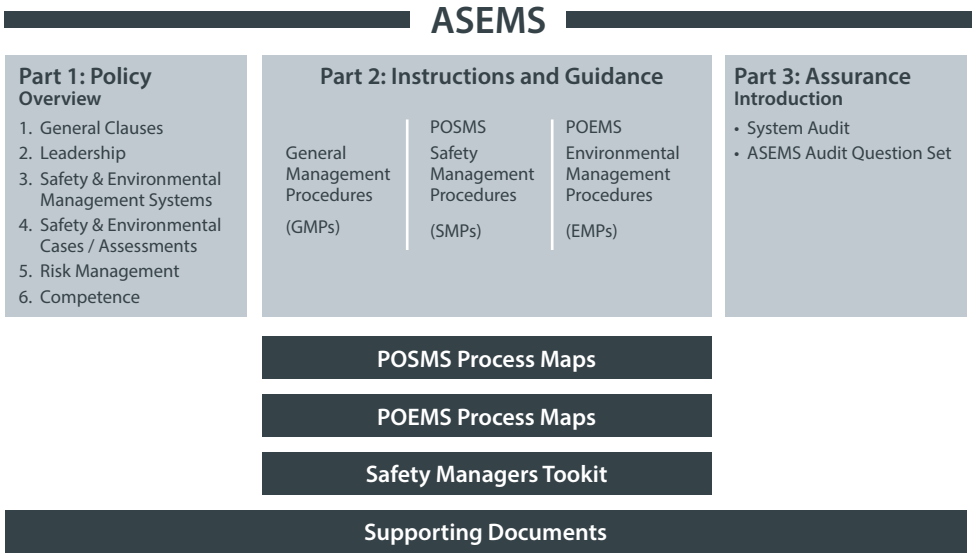
Environmental Management System (POEMS). Each manual contains a number of procedures designed to help Delivery Teams manage safety risks and environmental impacts and apply the appropriate mitigation measures. The manuals may also be used by contractors, suppliers, and advisers where appropriate. Compliance with the POSMS and POEMS will ensure that any project's safety and environmental management system is robust, proportionate to the project's levels of risk and is compatible with the DE&S corporate reporting requirements.

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

Operating Centre Level: DE&S Operating Centres (OCs) have developed and operate their own SMS or combined SEMS, defining their particular Organisation and Arrangements (O&A), tailored to meet their own domain-specific requirements and applicable to all Delivery Teams. The OC management systems define the common ways of working for all projects in that area, including aspects such as safety competence requirements, audit arrangements, delegation of safety authority and Learning From Experience (LFE).

Programme and Delivery Team Level: There may be a SMS or SEMS for a programme, group of projects or single large project. Commonly a single project may work in accordance with the next higher level SMS and would then use a project Safety Management Plan (SMP) to identify the project-specific arrangements, activities, resources, deliverables etc.

Figure 1: Structure of MOD's Acquisition Safety and Environmental Management System



2.3 Safety Committees

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

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

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

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

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

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

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

2.4 Safety Monitoring and Audits

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

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

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

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

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

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

The aims of an audit programme are to establish:

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

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

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

The Independent Safety Auditor. To maintain safety integrity across large and/or high risk projects, it is advisable that an Independent Safety Auditor (ISA) be appointed. The ISA should be acceptable to both the contractor and the MOD, be suitably independent of the DE&S Delivery Team and the Prime Contractor and have a good understanding of safety issues for systems of that technology and domain.

The ISA must have a well defined role that is clearly understood by all parties. This role might include providing assurance by auditing safety process being followed, or by doing some safety assessment independently to check the primary assessment. The role may change at different points through the life cycle, but the ISA's independence must not be compromised by involving them in activities such as setting safety requirements, tender assessment or providing specific advice on engineering changes.

3 System Safety in the Acquisition Lifecycle

Key Messages

The right Safety Management activities must be done at the right time, otherwise there may be excessive safety risks in service or excessive project risks (e.g. project delay, cancellation, cost overrun).

Before the system comes into service, safety is mainly an engineering discipline, influencing the design process. Safety management will also be concerned with keeping personnel safe when they come in contact with the system, for example during trials and commissioning.

From the in-service date onwards, safety management is concerned with keeping people free from harm, by using safe systems of work, by responding to incidents that occur and by considering the effects of changes.

Delivery Teams can influence safety for their systems by:

- Consulting widely
- Setting good safety requirements
- Building a positive safety culture
- Selecting and working closely with competent contractors
- Understanding the "living risk picture" and managing residual risks

3.1 General

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

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

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

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

Safety analyses should shape safety requirements and influence the design and development process. Through-life safety management aims to stop unsafe systems coming into service and prevent late discovery of problems that could cause delay or cost overrun. Attention in service will stop safety degrading.

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

3.2 What is Done and When

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

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

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

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

As illustrated in Figure 2, a separate safety case report is produced at each key stage of the lifecycle, or decision point. This should be seen as gradual refinement and extension of the same documentation. A safety case report is a summary of work up to a given point, or for a defined purpose (see Table 1). From the earliest stages it should be known what type of evidence will be required to demonstrate that safety will be achieved. The safety programme aims to fill in the known evidence gaps.

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

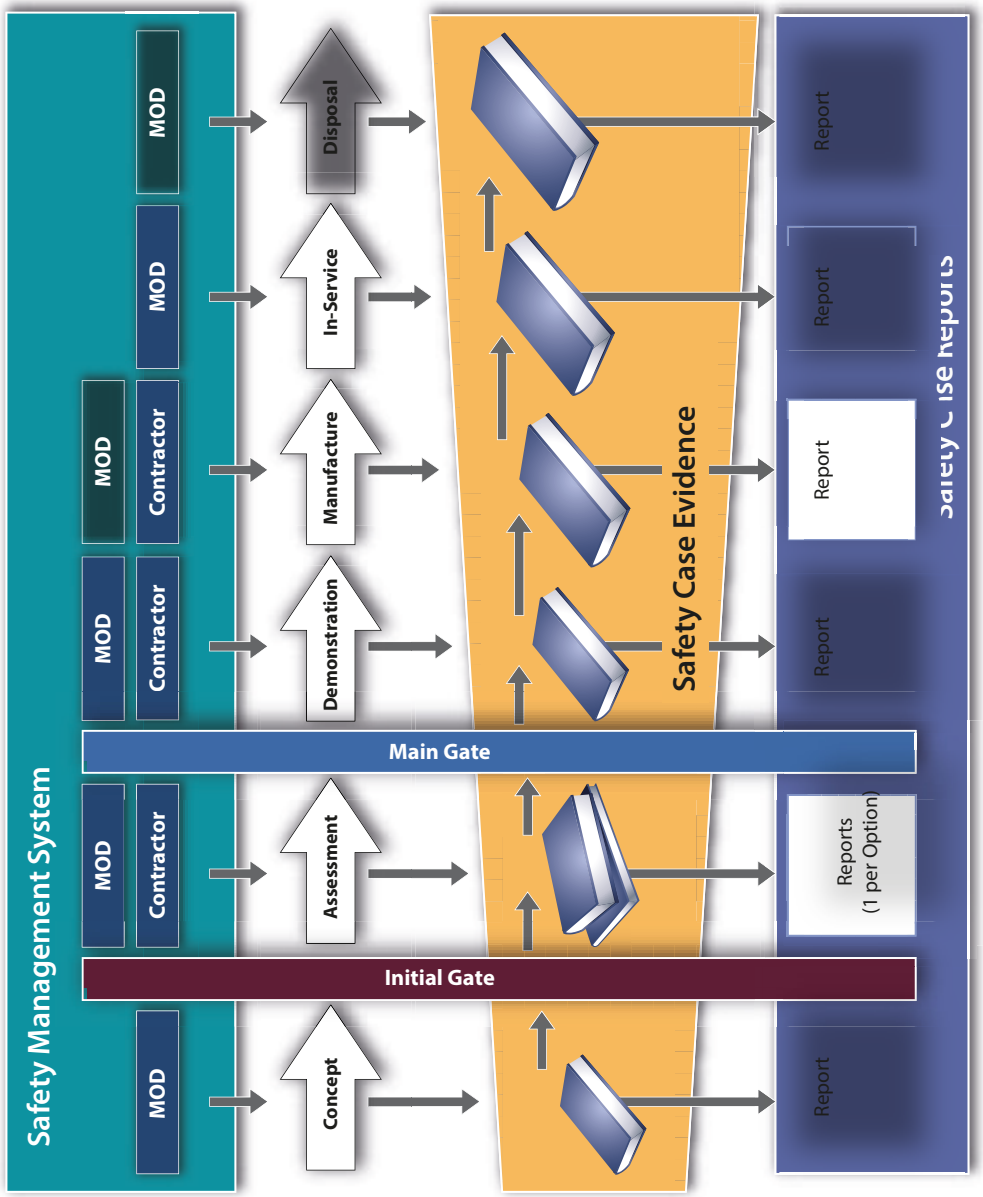
- Operating the project SMS (including auditing and monitoring incidents and accidents)
- Convening meetings of the PSC
- Producing and maintaining the SMP
- Conducting project risk management activities, including those for project risks resulting from the safety programme

3.3 How Delivery Teams can Influence Safety

The major ways in which a Delivery Team can influence safety for their system include:

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

Figure 2: Example of Safety Case and Safety Case Report Development Through-Life



3.4 Concept

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

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

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

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

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

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

- Legal requirements
- MOD policy and regulatory requirements
- MOD certification requirements
- Safety related standards

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

The main safety outputs at the Concept stage are:

- Safety Case Report (SCR) including a conclusion on whether the capability requirement can be achieved sufficiently safely
- The safety sections of the User Requirements Document (URD)
- SMP for subsequent phases of the project

3.5 Assessment

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

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

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

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

During Assessment, or earlier, the project manager must judge whether the risks for the system warrant the appointment of an Independent Safety Auditor (see Section 2.4).

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

The main safety outputs at the Assessment stage are:

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

3.6 Demonstration

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

- Training
- Personnel
- Infrastructure and facilities
- Resources, spares and support
- Interoperability issues

The safety case should contain all the safety evidence and show how the safety targets are being and will be met. Safety case reports may have to be produced to show that any trials can be conducted safely and there may have to be demonstration trials of any safety features.

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

The main safety outputs at the Demonstration stage are:

- Input to the design process to produce a safer system
- A Demonstration stage SCR
- Evidence that the safety targets are being/ will be met
- A Through-Life SMP

3.7 Manufacture

At the Manufacture stage of a project the emphasis is on ensuring that neither the production process nor any design changes compromise safety. Once the complete system exists, trials are conducted to verify "testable" aspects of the design. At this stage

the necessary supporting arrangements must be put in place and be shown to be adequate to keep the system safe before it is allowed into service.

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

The main safety outputs at the Manufacture stage are:

- A Full System Manufacture stage SCR
- Results of verification tests
- Further evidence that the safety targets are being met
- Verification of user and maintainer documentation and training
- A Through-Life SMP

3.8 In-Service

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

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

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

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

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

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. The key requirements are:

- 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.

Safety risk management continues through the in service period, and it includes :

- **Reactive risk management**:
  - Incident & accident reporting, investigation and resolution
- **Pro-active risk management for changes,** e.g.
  - Changes to system operation / context / modification / aging / manning / organisation.

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

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

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

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

3.9 Disposal

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

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

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

Disposal activities include through-life disposal as well as end-of-life disposal. So safe disposal must be considered early for prototypes, test articles, consumables and unintended disposal, which may occur well before the Disposal stage of CADMID.

The main safety outputs at the Disposal stage are:

- A SCR for the disposal programme
- A plan for safe disposal

Table 1: Example of Key Activities and Deliverables through the Acquisition Cycle

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

4 Safety in System Design and Development

Key Messages

During the system development process there are three strands of safety management activities:
- Management
- Ensurance
- Assurance

Safety responsibilities are shared throughout the supply chain, with interconnected responsibilities on the customer and the supplier.

Design for safety must start early in the lifecycle when there is scope for greatest and most cost-effective influence, through developing and selecting inherently safer concepts, processes and configurations.

Safety risk controls should be chosen in an order of precedence that emphasises the most effective strategies, such as hazard elimination, rather than relying on people's behaviour, procedures and warnings.

4.1 Introduction

Engineering can be described as *"the application of scientific and mathematical principles to practical ends, such as the design, manufacture and operation of efficient machines, processes and systems."*

System safety engineering complements safety management and is the technical activity to make and keep systems adequately safe. Starting early in the lifecycle, it includes tasks relating to setting safety requirements, design decision-making and safety assessment. System safety engineering encompasses both making the system adequately safe (ensurance) and showing that this has been achieved (assurance).

We saw in Part I, the separate introduction to concepts and principles, that a system may include hardware, software, human aspects and also interactions with other systems and with the environment. Safety engineering should be a part of a Systems Engineering approach and deal with not just equipment but all Defence Lines of Development (DLODs) and Systems of Systems issues.

Developing and assessing a system according to Def Stan 00-056 requires the interaction of three main strands of activities: Management, Ensurance and Assurance.

- **Management** activities are typically concerned with overseeing safety management, facilitating customer-supplier interaction and formally assessing relevant deliverables for acceptance.
- **Ensurance** activities are typically concerned with the development of the system to the specifications provided.
- **Assurance** activities are typically concerned with the production of a compelling safety argument, supported by strong evidence.

In practice these activities may overlap. For example, performing hazard analysis and deriving safety requirements will require interactions between activities in all three strands. Safety requirements will emerge or be derived as the project proceeds, typically in order to mitigate hazards. The Ensurance and Assurance activities include the establishment of the **derived safety requirements**, as well as the production of a system which can be shown to satisfy all contractual and derived requirements.

The outputs from System Safety Engineering will include

- Systems that are as safe as reasonably practicable
- Evidence that the system meets its safety requirements
- Knowledge and understanding of the identified residual hazards
- The data that is required to enable the operator and support authority to control those hazards effectively

4.2 Safety Responsibilities for Design and Development

It is important to know what responsibilities can be reasonably assigned to the supplier and its engineering team and what are rightly those of the acquisition and operating authority.

Designing and manufacturing equipment that is as safe as reasonably practicable is an engineering task that is defined by the requirements placed upon the supplier by its customer. If the customer is informed that its requirements are likely to result in equipment that is significantly less safe than is reasonably practicable, then the customer and operator must make a decision on the acceptability of the risk of accidents. Of course, if a customer requires equipment that has intolerable risk in normal operation, the supplier is best advised to refuse the contract.

The **supplier** is responsible for:

- Ensuring that their system solutions comply with relevant legislation
- Designing and manufacturing a system solution that meets contract requirements
- Designing and manufacturing a system solution that is as safe as is reasonably practicable
- Informing the customer of requirements in the contract that are unlikely to result in a system solution that is as safe as reasonably practicable
- Informing the customer of any hazards associated with normal and abnormal operation of the system
- Informing the customer of activities required to control hazards in terms of operating limits, operating procedures, safety monitoring activities, maintenance and repair processes and disposal methods
- Informing the customer of any information identified after completion of a contract that may influence that safety of the system supplied

The **customer** is responsible for:

- Specifying requirements that are achievable and are likely to result in a system solution that is as safe as reasonably practicable
- Implementing a Safety Management System that will include hazard management of the known hazards to the safe operation of the system
- Collecting and analysing data on in-service accidents and incidents and using that information to maintain the standards of safe operation

The supplier uses Safety Engineering to deliver equipment that is as safe as reasonably practicable. The users of equipment have a duty to specify and purchase equipment, which is as safe as reasonably practicable, and to use and maintain it so as to manage the hazards to safe operations. Safety Engineering can produce safer equipment but cannot guarantee safety.

The supply chain often has multiple links in each direction. So the primary supplier has sub-contractors and suppliers providing parts of their overall scope of supply. And the immediate customer may act in a supplier role, by providing the equipment or system to a higher-level authority, for example one responsible for a "system of systems".

4.3 Safety in the Engineering Approach

Engineers apply the sciences of physics and mathematics to find suitable solutions to problems or to make improvements to the status quo. If multiple options exist, engineers compare different design choices and choose the solution that best matches the requirements. The crucial task of the engineer is to identify, understand, and interpret the constraints on a design, in order to produce a successful result.

Safety is one of many disciplines that are involved in systems engineering of a project: these disciplines are brought together under the overall project management and must share common data on the current design. Other disciplines with which safety engineering is closely linked include:

- Human Factors
- Integrated Logistics Support
- Dependability (Availability, Reliability and Maintainability)
- Quality

The need for equipment and systems which are 'safe' throughout their lives demands that safety issues are considered and explored from the earliest stages of a project. This will involve:

- **Safety Requirements:** identifying and refining project-specific safety requirements
- **Design for Safety:** creating and refining design solutions so that they can meet the safety requirements
- **Assessment of Safety:** forecasting and evaluating the safety characteristics of proposed design solutions (before the system comes into service, whilst in operation or before changes are made). Such assessments can draw on a range of techniques, including:
  - Analysis
  - Simulation
  - Testing (within and beyond the 'design envelope')
  - In-service data collection

These activities will usually be iterative, so that as the design is altered for improved safety, the analysis and testing will be revisited and updated to reflect the new design. New risk control measures will also usually involved new 'derived safety requirements', specifying how 'good' a safety feature has to be for the system to be considered to be 'safe enough' and meet overall requirements.

4.4 Design for Safety

It is only through the understanding of hazards, that risks can be controlled effectively: once designers understand how a system might be dangerous, they can conceive ways to stop that happening.

The first stage of designing for safety is the identification of hazards and investigation of their characteristics; the causes and severity, immediate consequences and routes to escalation. This knowledge about hazards and their characteristics will grow as the project develops. Understanding of hazards is the trigger for the search for a safer design.That process has a changing emphasis over a project lifecycle, from high-level design to detailed design:

- **During macro (high level) design** aiming to develop and select inherently safer concepts, processes and configurations, thereby eliminating hazards
- **During micro (detailed) design** aiming to optimise the detail, seeking to minimise the hazard likelihood and consequences at source

Good practice in designing for safer systems can be considered under the following elements:

1. **Leadership:** Safety leadership is as important in design as it is in operations, since designers have greatest potential to reduce overall risk. That potential can only be realised through the attitude and personal involvement of the project manager. The right attitude should be evident when discussing design, by those involved asking what are the hazards, and how can they be eliminated or minimised.

2. **Identifying and Understanding Hazards:** Everyone in the design team should take responsibility for identifying and understanding hazards and eliminating or minimising the associated risks in pursuit of a safer design.

3. **Inherently Safer Designs:** Projects should aim to minimise the exposure of personnel to hazards by adopting inherently safer designs.

4. **Concept Selection:** Projects should actively develop inherently safer design concepts, selecting only from those in which the hazards can be managed effectively and risks are reduced to a level that is tolerable and ALARP.

5. **Residual Hazard Management:** Risks from residual hazards on the selected concept should be systematically reduced in design using the formal hierarchy of strategies (see Section 10.5).

6. **Performance Standards of Control Measures:** Measures used to reduce risks of residual hazards should have clearly defined performance standards, which are achievable throughout the life of the system.

7. **Technical Integrity throughout Lifetime:** The design team, in choosing materials and systems, should take full account of the possible loss of technical integrity over the system lifetime and should record decisions affecting operational and maintenance requirements.

8. **Construction, Commissioning and Decommissioning:** Risks associated with construction, commissioning and decommissioning should be fully considered in the design.

9. **Human Factors:** Projects should take responsibility for ensuring good ergonomic design (including interfaces, displays, controls, alarms etc.) to consider human fallibility and reduce human error..

4.5 Safety Risk Reduction Strategies

Once a particular hazard has been recognised, an imaginative exercise is required to devise possible ways to reduce the associated risk. In any given set of circumstances, some risk control measures will be 'better' than others and it is obviously preferable to use the 'best' option.

A number of risk control hierarchies have been developed. Each hierarchy reflects the fact that eliminating and controlling risk by using physical engineering controls and safeguards is more reliable than relying solely on people.

The MOD POSMS procedure on Risk Reduction provides the following hierarchy for strategies to reduce Safety risk:

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)

In some cases the risk reduction strategies will include new safety requirements (for example new protective functions to be incorporated). The design team should identify the safety requirements that realise the selected strategies, and ensure that these are included in the overall safety requirements. Records should be maintained to show traceability between hazards and accidents, and the associated safety requirements

Key Messages

Systems can be affected by failures due to random or pseudo-random causes (such as wear-out or corrosion). Although the time to each such failure is not predictable, failure statistics can be used to predict the rate of occurrence across large populations of similar items.

Systems can also be affected by systematic causes such as errors in specification or design. Such failures depend on input conditions to the system and on transient conditions in the operating domain and would occur whenever the same conditions apply.

Software is not subject to random failure but systematic failures can arise due to mistakes in specification, design implementation, change control etc.

Systematic failures can be prevented by approaches including:
- Fault avoidance
- Fault removal
- Fault detection
- Fault tolerance

Techniques exist to aid development of safe software, but one cannot be certain that the last latent problem has been identified and removed and there remains residual risk that the software could fail.

5.1 Introduction

Systematic failure is important because it can undermine many of the common risk mitigation solutions and invalidate safety assessments that ignore it. Simply providing redundant protection will offer little or no defence against systematic failure, so different strategies are required.

Random failures result from various degradation mechanisms affecting hardware. Variance of properties, within manufacturing tolerances, can cause components to fail after differing times in operation. Failure of equipment comprising many components occurs at broadly predictable rates, because of averaging across multiple component degradation mechanisms.

Random failure includes the failure of limited life items. Such items would normally be replaced before their lifetime expired. For example, a timing belt on a car that needs to be replaced after 40,000 miles. Failure to replace the timing belt after this distance could lead to serious engine damage when the it finally fails.

Design decisions to select cheaper, readily available commercially produced components, as opposed to military-specified components, can lead to increased random failures during the life of the equipment.

With sufficient numbers of systems, or components within a system, system failure rates arising from random hardware failures can be estimated with reasonable accuracy, but the time to individual failures cannot be predicted.

Systematic failure is a failure caused by environmental factors or errors in the specification or design of the system. It is defined in IEC61508 as *"Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or manufacturing process, operational procedures, documentation or other relevant factors."*

Because software behaviour is entirely repeatable (if the conditions that cause that behaviour can be repeated exactly) and has no wear-out mechanism, all software failures are **systematic**.

Systematic failure is also an important failure mechanism in hardware logic and in all types of mechanical systems. Because the failure rate depends on the inputs to the system and transient environmental factors, prediction of the systematic failure rate as a function of **time** is difficult.

5.2 How to Prevent Systematic Failures

There are four groups of techniques that are commonly used to prevent systematic failures:

1. **Fault avoidance**
   - Prevent faults from entering at the design stage
2. **Fault removal**
   - Find faults before it enters service (testing)
3. **Fault detection**
   - During service to detect faults that occur in real time
4. **Fault tolerance**
   - Design the system to allow it to function correctly in presence of faults

None of these techniques is completely effective on its own. In critical applications it is important to use a combination of these techniques to reduce the number of faults to an acceptable level.

5.3 Analysis Techniques for Software

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

Software problems arise from a number of causes:

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

Faults from causes like these will sit in the software waiting for a "revealing mechanism", such as an unexpected input or a change of operating

Words of warning on systematic errors and safety integrity:

- There can be no guarantees that any (affordable) system is completely free from systematic errors, although methods progress towards this goal (e.g. for software, auto-coding and semi-automated formal methods proving)
- Rigorous formal process can avoid errors arising between specification and implementation
- Safety Integrity Levels (SILs) and similar concepts provided by standards can give guidance on the degree of rigour required in design, development and testing – but they are not a "cure-all" for systematic errors
- Errors of requirements and specification are likely to be dominant (assuming current norms of good design and manufacture)
- As complexity of systems increases, we can expect to encounter more systematic errors
- Research has shown that knowledge of architecture, process, software language etc. all have less impact on the quality / integrity of the delivered product than domain knowledge

conditions. The fault then becomes a software error, which is a "discrepancy from its required state". A software failure is the effect of the error on the intended function, and may cause minor irritation through to catastrophe, depending on the software function affected.

The first stage, required both for safety assessment but also for choosing how to design the software, is to look at the functions the software will perform in the system. Hazard identification techniques such as Functional Failure Analysis (FFA) can be used to identify the system hazards which could be caused by the software. If the software doesn't do its job, for whatever reason, then these are the undesired conditions which could result.

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

5.4 Developing Safe Software

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

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

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

Whichever class of technique is used, one cannot

be certain that the last latent problem has been identified and removed. There remains residual risk that the software could fail. Various methods can be used to estimate failure probability for the software, but none of these is universally accepted. Estimated probabilities of a software failure should then be included in the overall Quantitative Risk Assessment (QRA) of the system.

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

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

5.5 Safety Assessments for Existing Software

System developers are increasingly reluctant to produce bespoke systems, and wish to use off-the-shelf software (including firmware) or re-use existing software in new applications. Such software is, to a greater or lesser extent, of unknown pedigree, and the catch-all term Software of Unknown Pedigree (SOUP) has been adopted. When these systems are safety-related, assurance is required that they work correctly and reliably. It can often be difficult to justify the use of OTS/reused software using the same techniques as for bespoke software. For example design and specification information may be unavailable or incomplete.

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

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

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

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

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

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

6 System Safety Assessment and the Safety Case

Key Messages

The safety case approach to safety regulation makes the organisation wanting to do an activity responsible for demonstrating that their operations are going to be safe.

Safety assessment is an iterative process that is part of the overall system development.

Safety assessment draws on a range of techniques to identify and understand possible hazards and accident sequences.

MOD use safety cases to provide the argument and evidence that their systems are safe for their purpose.

Safety cases are live, working documentation that are developed and reviewed through the lifecycle.

Safety cases are required for Service Provision contracts, MOD legacy systems and for OTS equipment.

The safety case must cover all parts of the system including assessment of equipment, people and all other DLODs, including their interaction.

Configuration management is critical to good safety management.

6.1 Approaches to Regulation

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

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

In this context, MOD is the "creator of the risks" but it is also the "regulator" in particular areas (see Part I, the companion publication to this booklet). The regulator or assurance function must be organisationally distinct within MOD, so that one area is not responsible both for preparing the safety argument, and declaring it adequate.

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

6.2 System Safety Assessment

There is no standard, correct and mechanistic 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. Safety assessment techniques can be used to different depths at different stages in the system 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, and so 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.

In the MAA Regulatory Publications the term "Safety Assessment" is applied below the system-level and there may be separate, but related, Safety Assessments for Equipment and each of the other DLODs. These are brought together in the "Air System Safety Case".

Detailed information on safety assessment techniques is contained in the MOD's Safety Managers Toolkit (part of the supporting information of ASEMS) and in the System Safety Practitioner (SSP) training courses, both online and classroom-based.

6.3 The Safety Case

A safety case is defined in Def Stan 00-056 as *"a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment"*. A simple way of understanding the safety case is to consider five basic questions:

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

The safety case should answer these questions for the whole system under consideration and for the uses defined.

The safety case should highlight the major hazards and concentrate on these: often safety cases can be swamped by a mass of detail on all the hazards from the trivial to the most significant.

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

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

The MOD safety case is often summarised at key decision points in a project in a series of **"safety case reports"** as described in Section 3.

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

The Safety Case Report will typically include:

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

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

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

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

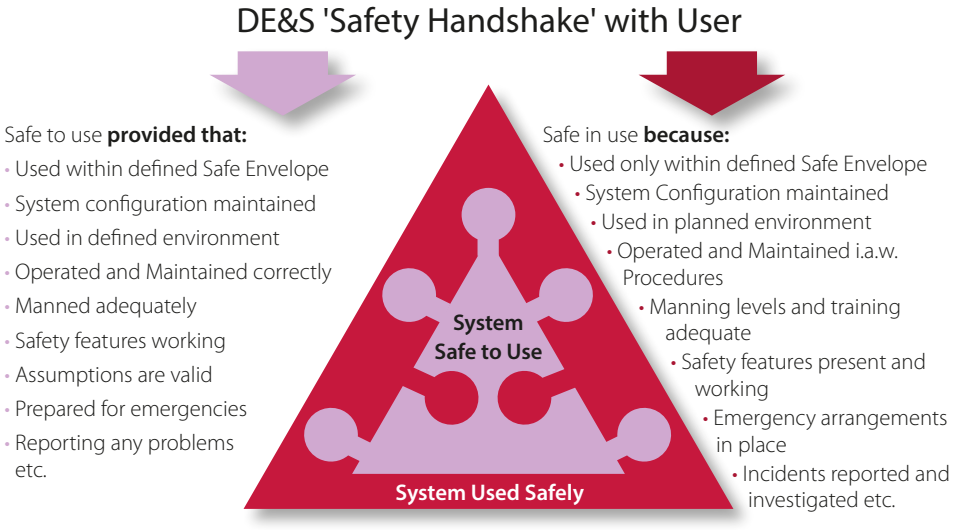
Not all safety cases are good. The HSE has reviewed many real safety cases in its role as regulator and some of the problems it has found with poor examples include:

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

6.4 Safety Cases and Users' Safety Management

The safety case should provide clear argument with evidence to show that the system is, and will remain, adequately safe in its actual usage: it is not sufficient to show that it could be safe or would be safe in a situation that is unrealistic. A supplier may produce a safety case to argue that their supplied product **can be used safely**, but that would be qualified with caveats, assumptions, requirements and dependencies that must all be satisfied for the system to be "safe in use." MOD has legal and regulatory requirements to demonstrate, so far as is reasonably practicable, that its equipment and work activities do not expose people to risk.

Figure 3: How the Safety Case Links with the User's Safety Management



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

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

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

To satisfy itself of the safety case's validity, the user organisation should confirm that the safety case, or its outputs, addresses the User Requirements set for the capability. It must also check that the safety case was produced with the involvement of relevant stakeholders, has been independently reviewed to validate and verify its content and assumptions, and provides suitable and sufficient information and procedures.

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

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

- Local Area (e.g. deployment) risk assessments
- Control Of Substances Hazardous to Health (COSHH) risk assessments
- Training area risk assessments
- Lifting operation risk assessments

6.5 Safety Evidence and Assumptions

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

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

- Performance in previous use (accident/incident/failure rate record)
- Compliance with standards, regulations and guidelines
- Calculations (e.g. Finite Element Analyses for stress and fatigue life)
- Testing (e.g. performance, fatigue life, software)
- Simulation and modelling
- Analytical (e.g. HAZOPS, FMECA, FTA, Bow-Tie Analysis)
- Expert review / best practice / certification
- Process evidence (e.g. existence and use of audited SMS, competent/SQEP staff, assurance of Risk Controls)

Figure 4: How the Safety Case Draws on Evidence and Assumptions

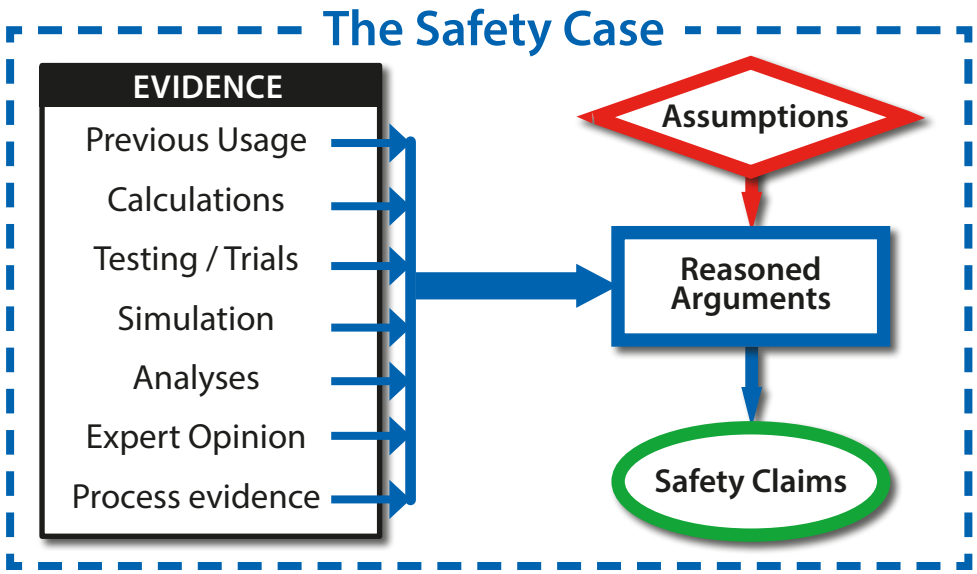


Figure 3 shows that the reasoned arguments combine various types of evidence and also build on assumptions. It is important that these assumptions are declared openly. During the safety programme, the key assumptions should be validated wherever possible, thus effectively replacing each assumption with evidence.

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

6.6 Safety Cases for Service Provision

Acquisition Projects involving provision of a service are becoming increasingly common in Defence and the safety implications vary widely according to the nature of service provided.

Product Safety Legislation relates to tangible products and systems and therefore is not very relevant when considering safety requirements appropriate to service outputs. The contract will therefore be more important than Legislation in these situations and Def Stan 00-056 does cover safety management for service provision. However, the contract cannot be used to transfer away Safety duties that legally rest with a particular organisation or individual. Occupational Health and Safety Legislation will apply to the workplace(s) where the service is provided and all parties should be clear about whose Safety Management processes apply where, and which individuals are in control of staff and work activities.

Early in the lifecycle of a service provision project it is important to define the nature of all the service outputs, and then to explore whether and how these might cause or contribute to harming people. For example:

- **Provision of in-service maintenance support on a defence platform:** maintenance errors might lead to a faulty system that causes the platform to crash in service
- **Training provision:** defective training material, poor delivery or inadequate trainee assessment might result in students having qualified who are not adequately competent. The eventual consequence could be avoidable accidents on the in-service system
- **Provision of data records upkeep:** causes such as human input errors, poor configuration control or a software error could result in incorrect, but credible, data. Depending on the use and safety-significance of the data, this might cause fatalities (e.g. if it relates to navigation information or medical records)

Based on safety assessment of the service outputs, the customer should identify any specific outputs that are considered to be safety-related. Generally the problems identified will not be totally new hazards, but rather additional causes of hazards that are already recognised for the system or operation of interest. Hazard Analysis and Risk Assessment and their organisation's willingness to tolerate of Safety Risk would then be used to define the required performance and integrity of the safety-related outputs. The contract will also typically identify how assurance is to be provided to the customer (e.g. inspection, audit, sample testing, performance metrics) and also the enforcement mechanisms for when shortfalls are detected.

The service provider must understand which outputs are safety-related and explore how these might deviate from the required condition. They must build the necessary rigour and competence into their business processes and also consider their own requirements for assurance which is proportionate to the required integrity.

Safety Cases for service provision are similar to those for tangible equipment and systems in that they must clearly highlight the key hazards and the control measures put in place and provide reasoned argument and evidence of safety. However, the safety significance of the service may not be obvious to all readers of the safety case, since the harmful consequences may happen remotely from the service delivery location. Unlike for tangible equipment and systems, product safety Legislation and Standards are less likely to be relevant to service-provision contracts and therefore compliance with regulations and good practice is less relevant as part of the evidence of safety.

6.7 Safety Cases for Off The Shelf Equipment

MOD procures a wide variety of Off The Shelf (OTS) equipment. By definition, the equipment should not require development to meet MOD's requirement. However, many projects do involve modification of an existing commercial product to meet MOD-specific requirements.

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

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

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

6.8 Configuration Management

Configuration management is vital to good safety management. The safety evidence embodied in the safety case will apply to a particular defined design or build standard and usage of a system. If the actual build standard is different from this there may be different hazards or increased risks associated with the known hazards. JSP 945 defines Policy and Def Stan 05-57 provides requirements and procedures for the configuration management of defence materiel in support of MOD projects

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

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 *Log in to ASG required for access to these pages*	www.aof.mod.uk/aofcontent/tactical/safety/content/introduction.htm
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

DSEQT/QSEP/POL/01/WHITEBOOK_PT2_ ISSUE 04