# Table of Contents

# 10. Safety Requirements and Contracts

ASEMS Document Version:
4.4
Effective From:
Friday, 24 June, 2022 - 00:15
Summary:
This procedure provides guidance for defining the requirements of the Safety Management System (SMS), and how it will be demonstrated that safety targets have been met. The procedure also provides guidance for the development of contractual terms with external contractors where they are required.

## 10.1. Introduction

### 10.1.1. Definitions

10.1.1.1.

A **Safety Requirement** is defined in Def Stan 00-056 [1] as:

“A requirement that, once met, contributes to the safety of the system or the evidence of the safety of the system.”

### 10.1.2. Objectives

10.1.2.1.

The two ways in which a Delivery Team can have the greatest influence in ensuring that the system design can achieve adequate safety performance throughout its life, are through:

1. Setting appropriate safety requirements;
2. Having effective Contract(s) with competent Contractor(s) for development and support.

10.1.2.2.

DE&S should define clearly what the system will do and what behaviour (e.g: performance, reliability) it will exhibit for it to be considered adequately safe. Only the Duty Holder can decide what levels of safety risk can be tolerated in different circumstances, and balance the military or other benefits of the system against these risks.

10.1.2.3.

The overall aim the SMS is to reduce risk to a level that is Broadly Acceptable or tolerable and As Low As Reasonably Practicable (ALARP). However, with the wide variety of defence systems, safety targets or criteria should will a measurable approach to the achievement of safety. The targets may be either qualitative or quantitative, but both types need to be tailored to the individual project. Numerical values should be used with caution: they will be auditable and applicable to the project in hand.

10.1.2.4.

Safety requirements form the basis against which the safety of the system will be tested and assessed. The activity of establishing Safety Requirements is iterative because of the iterative nature of safety analysis.

10.1.2.5.

This procedure defines the various forms that Safety Requirements can take and identifies when and how they should be derived. It also identifies safety issues for inclusion in contracts and discusses some potential project risks associated with inadequate requirements and contracts.

## 10.2. Procedure

### 10.2.1. Method

10.2.1.1.

Deriving and recording appropriate safety requirements that are tailored to the system and its function will ensure that:

1. The system design and development is influenced to achieve a level of safety performance through life, that is tolerable and in proportion to the benefits brought by its (military) capability;
2. The needs of stakeholders (eg: authorities for higher-level systems, safety regulators and approval authorities) are recognised and addressed from the earliest stages of the project life cycle;
3. System functionality that is safety-related is recognised early in the life cycle and designed to achieve the necessary level of performance and integrity;
4. A record exists in the Safety Case (SC) to justify why the system safety requirements are appropriate.

10.2.1.2.

Contracts which adequately cover safety will ensure that:

1. Safety requirements are clearly specified;
2. Safety interfaces between the MOD and contractor are clearly defined;
3. The risk acceptance regime relevant to the contract is clearly specified and any MOD regulatory requirements are given proper consideration;
4. The contractor's safety data is provided in an auditable and acceptable form to MOD, including the Delivery Team (DT), Functional Safety Management Offices (FSMOs) and any authorities who act as regulator or provide safety approvals.
5. The contractor provides access to MOD safety authorities for audit as required.

10.2.1.3.

Tender assessment and contract negotiations should seek to ensure that the selected contractors are professionally competent to undertake the work in respect of safety engineering and safety management.

#### 10.2.2. Initial Safety Objectives

10.2.2.1.

Flowing from MOD's safety policy, every acquisition project should have three main safety objectives:

1. Compliance with relevant legislation;
2. Achievement of safety levels at least as good as statute where legislation does not apply;
3. Safety Risks to be Broadly Acceptable or tolerable and ALARP.

10.2.2.2.

In addition to this, the Project will satisfy any relevant safety regulators or approval authorities who may have their own requirements for system features or information.

10.2.2.3.

The production of project-specific safety requirements will entail an examination of the capability requirements, the context (e.g. environment and interfacing systems) and the design solution, to define a complete set of safety requirements which should satisfy these common safety objectives and approvals requirements.

#### 10.2.3. Definition of User Requirements Document Safety Requirements

10.2.3.1.

The User Requirements Document (URD) is an all embracing, structured expression of the user need for a bounded operational capability, and is the means by which the Customer develops, communicates and maintains the user's requirement throughout the life of the system. In systems engineering terms, safety is a constraint that adds quality to the required capability, and the application of safety constraints to a system may lower the risks to that system's capability. The inclusion of safety requirements in a User Requirements Document should be the principal aspect in ensuring that the risks associated with a system are ALARP.

10.2.3.2.

Safety user requirements will include acceptance criteria (safety targets) against which the system will be assessed and accepted.

#### 10.2.4. Deriving Safety Requirements by Preliminary Analysis

10.2.4.1.

This is the first stage of detailed safety analysis and includes setting detailed safety targets derived from the baseline criteria. It should be carried out prior to tendering as part of the process of establishing safety requirements. The industrial Designer will refine this safety analysis early in the development contract when more detailed design information is available.

10.2.4.2.

In some cases the mitigation strategies will include new safety requirements (for example new protective functions to be designed in). The Project should identify the safety requirements that realise the selected mitigation strategies, and should ensure that where necessary these are incorporated into the overall safety requirements and Through Life Management Plan where appropriate. The Project should ensure that records are maintained to show traceability between hazards and accidents, and the associated safety requirements.

#### 10.2.5. Categories of Safety Requirements

10.2.5.1.

The requirements for safety will vary significantly with the type of project. Some of the different types of safety requirements that may need to be considered are:

1. **Legal requirements**. Such as the Health and Safety at Work, etc. Act 1974 [1] and its accompanying legislation, the Merchant Shipping Act 1995 [1], Civil Aviation Act [1] and its various amendments or the Road Traffic Act 2006 [1];
2. **MOD Certification**. Historically the MOD has developed a large number of certification requirements in order to manage hazardous aspects of defence equipment. Examples include; Military Aircraft Release, Ship Stability Certification and Laser Safety Clearance Certificate. QSEP can provide advice on certification requirements and advise on MOD specialist safety authorities involved in certification requirements;
3. **Safety Objectives**. This includes the general requirements for safety management, e.g. producing a Safety Case (see Procedure SMP12 – Safety Case and Safety Case Report [2]). It also includes complying with the specialist MOD policy and procedures which are relevant to the particular project or equipment;
4. **Safety Targets**. Further guidance is contained in the domain-specific Safety JSPs and Def Stan 00-056 [1].

10.2.5.2.

Legislation includes absolute, prescriptive and proscriptive requirements, as well as those requiring Risk to be made tolerable and ALARP. Thus the Safety Requirements for an equipment or service are likely to include absolute aspects as well as Risk-based aspects. The Safety Case will therefore do more than show that all identified Risks have been made ALARP.

#### 10.2.6. Safety Requirements Depending on System Function

10.2.6.1.

Where a system has a safety-related function, it means that failure to achieve the function can result in harm. It is therefore important that the function is achieved with appropriate reliability and performance. The critical first stage should be to recognise functionality which is safety-related so that appropriate Safety Requirements can be derived.

10.2.6.2.

Reliability targets should be assigned to safety systems or functions. The targets should be established on the basis of the safety criteria and be consistent with the roles of the systems or functions in different accident sequences.

10.2.6.3.

Some systems have a defensive role whereby inaction under hostile circumstances may constitute a hazard. Safety targets for such systems will address the requirements to reduce to a tolerable level, the risk resulting from inaction under hostile circumstances. Where there is a conflict between the practical realisation of safety targets for action and inaction within the system’s operational role, a reasonable balance of risk reduction should be established and agreed after consulting the Safety Panel and other key stakeholders.

10.2.6.4.

Safety-related functionality can result from the Capability requirement or from the context in which it operates. It is therefore important that the system requirements and the boundary interfaces should be examined in a systematic and exploratory way to identify and explore the effects of potential functional failures. The safety-related functionality can result from any parent systems and the use they make of

outputs from the system of interest.

10.2.6.5.

A target should describe the level of risk that is tolerable in terms of severity and probability of harm. They should address specific technical requirements, legislation to be met and require that all residual risks are reduced to a level that is tolerable and ALARP. The target may be either qualitative or quantitative, but both types need to be tailored to the individual project.

#### 10.2.7. Qualitative and Quantitative Safety Targets

10.2.7.1.

A quantitative target may be expressed in several ways, such as:

1. The probability of death per operating hour;
2. The probability of death per year;
3. The probability of death over the expected lifetime of the equipment;
4. The probability of loss of the platform or system.

10.2.7.2.

The way of expressing the target will vary according to the nature of the equipment, the Military Aviation Authority Regulatory Publications cite aircraft safety targets in terms of probability of death/aircraft hull loss per operating hour.

10.2.7.3.

It should be remembered that although quantitative, demonstration that these targets have been achieved or bettered is not generally practicable, either over the lifetime of a project or during a relatively short design and development process. They are to be used to indicate the level of performance/integrity expected from the equipment, and as a baseline against which to argue the Safety Case.

10.2.7.4.

The system safety targets will be included within the MOD's invitation to tender. The prospective contractors should develop the target further and flow the target down through the design into individual sub-system safety allocations.

10.2.7.5.

In addition to the probability of death, there are other targets which should be considered, such as the probability of a major or minor injury, the loss of platform/system and the effect on the environment. When there is more information available, usually after the Preliminary Hazard Analysis (see Procedure SMP04 – Preliminary Hazard Analysis [3]), then projects will be more able to develop targets for particular hazardous events. This process is known as "goal setting" and follows the safety best-practice of several other industry sectors in the UK.

10.2.7.6.

The system safety targets should be generated at the Concept stage and included within the safety requirements section of the User Requirements Document. During Assessment and Demonstration further analyses will be undertaken with the aim of refining the safety targets for inclusion in the System Requirements Document.

10.2.7.7.

It should be remembered that only MOD can set the levels of Risk which they will be prepared to tolerate for the military capability which a system brings them. This requires the involvement of many MOD stakeholders, but cannot be done on their behalf by Contractors working in isolation.

#### 10.2.8. Individual and Societal Risk Criteria

10.2.8.1.

The Health & Safety Executive has published criteria which define the limits of Tolerability for Safety Risks to Individuals (e.g. workers and general public) and also for safety risks which might affect many people simultaneously (e.g. a major accident at an industrial facility). These generic criteria should help Delivery Teams to define the limits of tolerability for their systems.

10.2.8.2.

The Health & Safety Executive's published figures for individual risk apply for the whole working year and individual Projects should only take a proportion of the total Risk budget because their system will not be the only source of risk throughout a working year. Guidance should be sought from Operating Centre Programme Management Offices or QSEP on the apportionment of risk to individual systems.

10.2.8.3.

These criteria are relevant to all the potential sources of Risk of fatality, taken together. Thus it would be wrong to use these criteria as a comparator for the different possible fatal accidents on an individual (accident by accident) basis.

10.2.8.4.

If the criteria for Societal Risk are applicable to a system, it should be remembered that the Individual risk criteria are still relevant and both should be satisfied for the system to be considered to be Tolerably Safe.

#### 10.2.9. Apportionment of Safety Requirements

10.2.9.1.

Whilst MOD should set the overall Safety Requirements for a system, it is appropriate to allow Contractors to decide how these requirements are to be achieved. For example, this can involve the apportionment of requirements to lower-level sub-systems or functions.

#### 10.2.10. Responsibility for Safety and Managing Risk

10.2.10.1.

Within the scope of MOD Policy, corporate responsibility for safety should remain with the MOD, but responsibility for Managing Risk can be shared according to who is best-placed/competent to manage it. Contractual documents should clearly state the division of work so that all parties understand the requirements to manage those aspects of safety placed on them.

10.2.10.2.

Projects must ensure that the contractor produces an adequate Safety Management System for the contracted work. Interfaces, lines of responsibility and accountability between the Project and its contractors should interface effectively and be described in the Project's and contractor's Safety Management Systems. Projects should ensure that their contractors are competent, with appropriate knowledge and experience of civil and MOD safety requirements. Advice on the competence of contractors and managing the safety interfaces should be sought from the Operating Centre Programme Management Offices or QSEP.

#### 10.2.11. Manufacturers' and Others' Duties as Regards Articles for Use at Work

10.2.11.1.

Section 6 of Health & Safety at Work, Act 1974 [1] places specific duties on those who can ensure that articles and substances are safe and without risks to health as it is reasonably practicable to make them before they are used and that articles are properly erected and installed. The following extract from Section 6 states; It should be the duty of any person who designs, manufactures, imports or supplies any article for use at work to:

1. Ensure, so far as reasonably practicable, that the article is so designed and constructed so as to be safe and without risks to health at all times when it is being set, used, cleaned or maintained by a person at work;
2. Carry out or arrange for the carrying out of such testing and examination as may be necessary for the performance of the duty imposed on him by the preceding paragraph;
3. Take such steps as are necessary to secure that persons supplied by that person with the article are provided with adequate information about the use for which the article is designed or has been tested and about any conditions necessary to ensure that it will be safe and without risks to health at all such as are mentioned in paragraph a) above and when it is being dismantled or disposed of; and
4. Take such steps as are necessary to secure, so far as is reasonably practicable, that persons so supplied are provided with all such revisions of information provided to them by virtue of the preceding paragraph as are necessary by reason of its becoming known that anything gives rise to a serious risk to health or safety.

10.2.11.2.

Designers, manufacturers, suppliers, importers and installers are required to make articles and substances without risks to Health and Safety which are reasonably foreseeable. Operator error or inattention, for

example, is reasonably foreseeable and should be taken into account when seeking to ensure safety. The use of articles and substances for wholly inappropriate purposes is not reasonably foreseeable and does not need to be taken into account.

#### 10.2.12. Contractual Arrangements for Sub-contractors

10.2.12.1.

The contractor is responsible to the Project for their sub-contractor's work. The contractor should make such arrangements with their sub-contractors, and they with theirs, as will ensure that the sub-contracted materiel is satisfactory.

#### 10.2.13. Prescriptive and Performance-based Standards

10.2.13.1.

The MOD's acquisition philosophy has moved away from "tell me how to do it" (prescriptive standards) towards "tell me what to achieve and leave me to decide how I do it" (performance based standards). However, prescription can still be useful in certain contexts. For example, this could include situations where systems are of well understood technology and functionality and there is established good practice for controlling the safety risks.

10.2.13.2.

Performance based standards align well with the goal setting principles of the Policy. However, prescriptive/deterministic rules should still form effective parts of a Safety Management System for specific risks, as they:

1. Are often widely used and understood;
2. Do not require advanced knowledge or deep competence to apply, making them easier to contract against;
3. Enable low-tech designs to be quickly and repeatedly generated in a reliable/predictable format;
4. Capture expertise/historic lessons learnt into a readily useable format or formulae, permitting benchmarking;
5. Support established feedback and review systems from in-service experience, permitting easier survey, verification and acceptance into service;
6. Provide a more clear-cut route to achieving a safety Requirement, which is less susceptible to corruption by programme or resource considerations.

10.2.13.3.

However, prescriptive/deterministic standards have disadvantages over performance based standards since:

1. The application is based on past practice, often making them inappropriate for new technology, unusual circumstances and stifles innovative approaches or solutions;
2. The original purpose of the standard can be hidden or may no longer apply, the reasons for specific criteria are not expressed;
3. Compliance with the standard discourages further work to seek safety improvements;
4. Often do not account for human error or violation of procedures.

#### 10.2.14. Hierarchy of Standards

10.2.14.1.

To comply with Secretary of State's policy, the MOD should ensure that the management and technical standards that are adopted are consistent with best civil and international standards. To achieve maximum harmonization it is therefore MOD policy to utilise international standards where appropriate and an agreed hierarchy is as follows:

1. European Union civil standards;
2. International civil standards;
3. UK civil standards;
4. Standardised NATO Agreements (STANAGs);
5. UK Defence Standards.

#### 10.2.15. Defence Standards for Safety

10.2.15.1.

It is recommended that appropriate standards should be used, for example:

1. Defence Standard 00-056 [1] Safety Management Requirements For Defence Systems;
2. Standards applicable to the system environment, for example, Def Stan 00-970 Design & Airworthiness Requirements for Service Aircraft [1] etc.

#### 10.2.16. Software Safety Requirements

10.2.16.1.

The MOD has adopted the term Complex Electronic Elements for systems which rely on software. Ensuring the safety of such systems can require the application of specialist techniques, but guidance has been produced in the form of publication “Acquisition Guidance on the Assurance of Safety in Systems Containing Complex Electronic Systems”. This Complex Electronic Elements guidance document compliments Def Stan 00-056 [1] regarding the safety of systems containing Complex Electronic Elements. It has been written for MOD Acquisition staff to assist in the formation of recommendations on the sufficiency of safety evidence for Complex Electronic Elements. It takes the form of a handbook, offering practical advice, but assumes the reader has a Professional Competency level of at least ‘Supervised Practitioner’ as defined by the IET/BCS Competency Guidelines. Def Stan 00-055 [1], is the MOD’s recognised standard in this area and should be used when developing contracts for software safety.

#### 10.2.17. Justification and Validation of Safety Requirements

10.2.17.1.

When defining Requirements, a top-level Safety Assessment should be used for categorising Requirements and justifying their selection as follows:

1. Requirements for full compliance with relevant legislation;
2. Requirements to provide evidence that MOD has safety levels at least as good as statute where legislation does not apply;
3. Requirements proving from first principles that target levels demonstrably reduce risks to ALARP levels.

10.2.17.2.

When an action or decision is challenged, the Safety Case is likely to be scrutinised by military Service Inquiries and civil courts of law. Those with formally-delegated responsibility for safety should therefore ensure that safety requirements for their projects are clearly recorded for external readership or for auditors together with clear justifications that they are suitable and sufficient.

10.2.17.3.

Each Safety Case should include a collation of Safety Requirements with associated safety justifications, structured using high-level qualitative Safety Assessment. These safety justifications should be constructed using a combination of evidence that each system’s Safety Requirements have been set at levels specified by:

1. Compliance with deterministic standards, demonstrated as good or best-practice, for a risk in a mature or well understood domain or;
2. Achievement of qualitative Requirements, (high-level principles, work practices etc.) for more novel risks, or for systematic failure mechanisms;
3. Numerical targets often supported by quantitative Safety Assessment for random events, which can benchmarked against historic data and to target levels where that is considered best practice.

#### 10.2.18. Demonstration that Requirements have been Satisfied

10.2.18.1.

Provision should be made for the validation of the Safety Requirements made in the design and build phase during the lifetime of the system or equipment.

10.2.18.2.

After the safety requirements apportioned to system elements and components are verified to have been met, an assessment should be conducted to verify that the total system meets its overall Safety requirements.

#### 10.2.19. Inability to Satisfy the Safety Requirements

10.2.19.1.

When it is determined that safety requirements cannot be met by a system element, there are three options:

1. It may be decided to accept the risk, in which case the appropriate management level as defined in SMP09 – Risk Acceptance [4] should endorse the decision,
2. Changes may be made to the design or
3. The apportionment of the safety requirements may be changed to alter the balance of safety significance between the elements. For example, when procedures are used to overcome limitations in equipment, the safety dependency on the equipment is reduced, and so its safety requirements can be revised.

10.2.19.2.

The Safety Requirements will be recorded in the following:

1. Project Requirements Management System (e.g. DOORS);
2. Hazard Log;
3. Safety Case.

#### 10.2.20. Records and Project Documentation

10.2.20.1.

Within the Project Requirements Management System, it may be desirable to annotate Safety Requirements as “safety”, so that they can be readily recognised and traced.

10.2.20.2.

Management of this procedure may be delegated to a member (Safety Manager) or members of the Delivery Team, but responsibility for its completion rests with the member of the team with formally-delegated safety responsibilities.

10.2.20.3.

The Hazard Log may contain some of the Safety Requirements relating to particular mitigation actions. However, it is unlikely to contain all the Safety Requirements.

10.2.20.4.

The Delivery Team must ensure that appropriate Safety Requirements are developed sufficiently early in the Project life cycle.

10.2.20.5.

The Safety Case should contain all the Safety Requirements, together with the justification of how they were derived. The Safety Case should include Claims that each of the requirements has been satisfied, together with the Argument and Evidence to justify the Claim.

10.2.20.6.

As the MOD is a self-regulating organisation, its Policy requires Projects to make decisions using risk-based techniques. Safety Requirements should be developed for particular projects or activities, using the Project Safety Committee to review the target levels set for those requirements and the success in their achievement at least at agreed milestones.

10.2.20.7.

Where relevant, the outputs from this procedure should feed into the following:

1. System Requirements Document – for any specific Safety requirements;
2. Customer Supplier Agreement – to document agreements on Safety information to be delivered by the Delivery Team;
3. Through Life Management Plan;
4. Safety elements of Outline Business Case and Full Business Case submissions.

10.2.20.8.

The Delivery Team is also responsible for the Safety content of Invitations To Tender and Contracts and will use specialist Safety and Contracts support to ensure that they are appropriate.

#### 10.2.21. Warnings and Potential Project Risks

10.2.21.1.

Safety Requirements should be established at the earliest stages of the Project life cycle, since they have a fundamental role in shaping the subsequent project. Failure to do so can have far reaching effects on both cost and programme.

10.2.21.2.

If contractors with inadequate competence in Safety Management are chosen, then there are likely to be significant impacts on Project Time and Cost as they struggle to understand and apply the necessary requirements and standards. There can also be an impact on the achieved levels of safety performance as they fail to apply the “Safety-led engineering” philosophy in a timely manner.

#### 10.2.22. Procedure Completion

10.2.22.1.

The Project Safety Manager and Project Safety Committee will be responsible for the completion of the procedure. However, in many cases a large part of the detailed work underlying Safety requirements definition will be conducted by contractors during the Assessment phase.

10.2.22.2.

The Project Safety Manager and Project Safety Committee will be responsible for formally documenting the Safety requirements and justifying that they are appropriate in the Safety Case.

10.2.22.3.

The Project Safety Manager and Project Safety Committee will be responsible for generating the safety content of Invitation To Tenders and Contracts calling on specialist Contracts support as necessary.

### 10.3. Timing

#### 10.3.1. Safety Requirements

10.3.1.1.

Every Project starts with a need to satisfy common safety objectives which derive from MOD Safety Policy. These are then interpreted into Project-specific terms to produce:

1. Safety Requirements in User Requirements Document;
2. Safety Requirements in System Requirements Document;
3. Requirements for safety mitigation features required to reduce identified Risks.

The derivation of these is an iterative process, but it must be undertaken sufficiently early in the Project life cycle to ensure that the design process is influenced and any major Project Risks (e.g.: of inability to achieve Requirements) are identified in a timely manner.

#### 10.3.2. Reviewing Safety Requirements

10.3.2.1.

The Safety Requirements must be reviewed to ensure that they are appropriate and complete, particularly before Authorisation of Safety Case Reports.
The Safety Requirements must also be reviewed as part of the periodic Safety Case review process (see Procedure SMP12 – Safety Case and Case Report [2]) to ensure that any missing or emergent Safety Requirements are identified. These can include:

1. New Requirements due to changes in usage (e.g.: new functionality, new system context or environment);
2. New Requirements due to emergent Legislation, both retrospectively applicable and that defining “good practice”. Note that this Legislation will include that which is directly applicable and that for comparable areas if statute does not apply to MOD;
3. New Requirements due to changes in Safety Regulation or Safety Approvals applicable to the Project.
4. New Requirements due to developing technology;
5. New Requirements due to recently identified Hazards.

#### 10.3.3. Coverage of Safety in Invitations To Tender and Contracts

10.3.3.1.

Safety issues must be addressed in Invitations To Tender and Contracts whenever the Delivery Team is considering using Contracted support for a function that may have an effect on Safety Management. This will obviously include System Development, Design Authority and Support, but also Trials, Documentation, Training and specialist Safety support to the Delivery Team. Safety must be addressed sufficiently well to ensure that Safety responsibilities and interfaces are understood by all parties and that the Contractor has sufficient competence in Safety to discharge their responsibilities.

The Project should obtain sufficient information at the tendering stage to enable a judgement to be made on the tenderers' competence with particular regard to equipment safety management (e.g. require the provision of safety personnel CVs at the Invitation To Tender stage). If the tendering process provides evidence that a particular contractor is not competent to carry out the work, then the bid should be deemed non-compliant and the contractor deselected.

The amount of safety information requested at the tender stage is dependent upon the size and complexity of the project, along with the perceived safety risks. A sample questionnaire is included in Guidance Sheet SMP10/G/01 - Safety Topics for ITT Questionnaires [5]. [6] This should be tailored to the requirements of the individual project. Ideally the tender responses should be provided in the form of a draft Contractor's Safety Management Plan which would then be formally agreed prior to contract award.

#### 10.3.4. Demonstration of Compliance with Safety Requirements

10.3.4.1.

The Safety Case is the mechanism both for justifying that the Safety Requirements are appropriate and for demonstrating that they are being achieved. It is particularly important that demonstration of compliance is attained before people are exposed to risks, for example at the time of equipment trials or Introduction to Service.

### 10.4. Required Inputs

10.4.0.1.

This procedure for Safety Requirements and Contracts requires inputs from:

1. Outputs from Procedure SMP01 – Safety Initiation [7];
2. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [3];
3. Outputs from Procedure SMP11 – Hazard Log [8];
4. Outputs from Procedure SMP12 – Safety Case and Safety Case Report [2];
5. Outputs from Procedure SMP05 - Hazard Identification and Analysis [9];
6. Outputs from Procedure SMP06 - Risk Estimation [10];
7. Outputs from Procedure SMP07 - Risk and ALARP Evaluation [11];
8. Outputs from Procedure SMP08 - Risk Reduction [12];
9. Outputs from Procedure SMP09 - Risk Acceptance [4].

10.4.0.2.

Generation of the Safety Requirements should use the following reference inputs:

1. MOD, domain and Top Level Budget Policy for Safety;
2. Defence Regulatory requirements;
3. Description of Capability requirements;
4. Design description;
5. Completed Form EMP03/F/01 SMP01/F03 - Register of Legislation and Requirements [13] .

### 10.5. Required Outputs

10.5.0.1.

The primary output of this part of the procedure is a clear and consistent set of Safety requirements that are justified as being appropriate to the system.

10.5.0.2.

Safety Requirements should be included within the Project's Requirements Management System and can be annotated as "Safety", so that they can be readily recognised and traced. DOORS is DE&S's preferred tool for Requirements Management.

#### 10.5.1. Safety Elements of Invitations To Tender and Contracts

10.5.1.1.

The primary outputs of this part of the procedure should be a clear and consistent set of Contractual terms that can be used to select and contract effectively for the required Safety Management aspects of the Project.

10.5.1.2.

Further Guidance - Safety Topics for Invitation to Tender Questionnaires, contains a list of topics which should be tailored to specific project characteristics and used in preparing a Safety Management questionnaire as part of an Invitation To Tender.

## 10.6. Annex A

#### 10.6.1. Safety Topics for Invitation to Tender Questionnaires

10.6.1.1.

Note: The following list of topics should be tailored to meet the requirements of individual projects.

10.6.1.2.

### a. Organisation and Personnel

1. Who within the company would have overall responsibility for safety on the project?
2. Would a project safety officer be appointed?
3. What would be the lines or communication for safety issues?
4. Who would be responsible for carrying out the individual safety tasks?
5. Will the company hold any safety panel meetings?
6. Would subcontractors to be used for safety related work?
7. What criteria would be used for selecting subcontractors?
8. What qualifications and experience do the key safety personnel have (provision of senior safety personnel Curriculum Vitae may be requested)?

10.6.1.3.

### b. Company Safety Policy and Track Record

1. Provide details of the company’s track record in Health and Safety and Equipment Safety Assurance;
2. What is the company’s safety policy?
3. Have there been any enforcement actions against the company?

10.6.1.4.

### c. Safety Management System

1. Describe the safety management system for the project;
2. Describe how the system will be audited.

10.6.1.5.

### d. Safety Assessment

1. Define the scope of the safety assessment;
2. Describe the tools and techniques to be used.

10.6.1.6.

### e. Safety Case

1. Define the scope of the safety case.

10.6.1.7.

### f. Safety Targets

1. Detail specific safety targets for the project;
2. Detail the evidence that will be provided to MOD to demonstrate that these targets have been met.

10.6.1.8.

### g. Safety Standards and Certification

1. List any standards with which the project should comply;
2. Detail the evidence that will be provided to the MOD to demonstrate that the standards have been met.

10.6.1.9.

### h. Independent Safety Auditor

1. Define the terms of reference for the Independent Safety Auditor including scope of work and lines of communication;
2. Propose an Independent Safety Auditor and demonstrate their independence from the prime contractor;
3. Detail the qualifications and previous experience of the Independent Safety Auditor.

10.6.1.10.

### i. Safety Work Schedule

1. Provide a programme of work that illustrates how the safety tasks will be carried out;
2. Are all safety deliverables to be linked into project milestones?

## 10.7. Version Control

#### 10.7.1. Version 2.3 to 3.0 Uplift

10.7.1.1.

Major uplift from the Acquisition System Guidance (ASG) to online version. POEMS has undergone major revision. Refer to the POEMS Transition Document for details.

#### 10.7.2. Version 3.0 to 3.1 Uplift

10.7.2.1.

A minor uplift to correct spelling, grammar, and to remove some duplication of text.

#### 10.7.3. Version 3.1 to 4.0 Uplift

10.7.3.1.

Major reorganisation of all SMPs:

- Restructure into a consistent format.
- Responsibilities, Alignment with Environment and guidance for different acquisition strategies have been removed and included in the POSMS summary.
- All further guidance has been placed into the Procedure section, and duplicated text has been removed
- An Annex A for 'Safety Topics for Inivitation to Tender Questionnaire' previously found in Further Guidance

#### 10.7.4. Version 4.0 to 4.1 Uplift

10.7.4.1.

Minor text changes to align with ASP taxonomy.

#### 10.7.5. Version 4.1 to 4.2 Uplift

10.7.5.1.

Text change replacing Project Team with Delivery Team.

#### 10.7.6. Version 4.2 to 4.3 Uplift

10.7.6.1.

Minor amendment to replace reference to Initial Gate and Main Gate and change these to Strategic Outline case, Outline Business Case and Full Business Case. This change brings terminology in line with JSP 655.

#### 10.7.7. Version 4.3 to 4.4 Uplift

10.7.7.1.

Update to Form SMP01/F/03 - Register of Safety Legislation and Other Significant Requirements to align with the form available on the DLST.

---

**Source URL:** https://www.asems.mod.uk/guidance/posms/smp10

**Links**
[1] https://www.asems.mod.uk/ExtReferences
[2] https://www.asems.mod.uk/guidance/posms/smp12
[3] https://www.asems.mod.uk/guidance/posms/smp04
[4] https://www.asems.mod.uk/guidance/posms/smp09
[5] https://www.asems.mod.uk/sites/default/files/documents/SMP/smp10-g-01.pdf#overlay-context=
[6] https://www.asems.mod.uk/sites/default/files/documents/SMP/smp10-g-01.pdf?_t=1481031057
[7] https://www.asems.mod.uk/guidance/posms/smp01
[8] https://www.asems.mod.uk/guidance/posms/smp11
[9] https://www.asems.mod.uk/guidance/posms/smp05
[10] https://www.asems.mod.uk/guidance/posms/smp06
[11] https://www.asems.mod.uk/guidance/posms/smp07
[12] https://www.asems.mod.uk/guidance/posms/smp08
[13] https://www.asems.mod.uk/sites/default/files/documents/SMP/20220624%20EMP03_F_01_SMP01_F_03%20-%20Register%20of%20Legislation%20and%20Requirements.xlsx#overlay-context=guidance/posms/smp10