

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 1

0	SHOWING CONFORMANCE
0.1	Options
0.1.1	There are four options to demonstrate conformance when applying this system procedure: <ul style="list-style-type: none"> a. Follow the defined system procedure using the recommended guidance and tools, including allowed variations and options. b. Use an equivalent process and tool set generated elsewhere and document evidence of procedural equivalence. c. Use a bespoke process and tool set for the project and document how the bespoke procedure achieves the objectives defined for this system procedure. d. Where the procedure is considered to be not relevant, document the basis for this decision.
1	INTRODUCTION
1.1.1	The two ways in which an IPT can have the greatest influence in ensuring that the system design can achieve adequate Safety performance throughout its life, are through: <ul style="list-style-type: none"> a. Setting appropriate Safety Requirements; b. Having effective Contract(s) with competent Contractor(s) for development and support.
1.1.2	A Safety Requirement is defined in Def Stan 00-56 Issue 4 as: <p>“A requirement that, once met, contributes to the safety of the system or the evidence of the safety of the system.”</p>
1.1.3	MOD must define clearly what the system must do and what behaviour (eg: performance, reliability) it must exhibit for it to be considered adequately Safe. Only MOD 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.
1.1.4	The overall aim of all safety management systems is to reduce risk to a level that is tolerable and ALARP. However, with the wide variety of defence systems, safety targets or criteria are needed to provide 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 must be used with caution: they must be auditable and applicable to the project in hand.
1.1.5	Safety Requirements form the basis against which the safety of the system is tested and assessed. The activity of establishing Safety Requirements is iterative because of the iterative nature of safety analysis.

Issue	Authorised by CESO DE&S	ISSUE LEVEL:	Release V2.2s
Approval	Authorised by DG S&E	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 2

1.1.6 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.

2 PROCEDURE OBJECTIVES

2.1.1 Deriving and recording appropriate Safety Requirements that are tailored to the system and its function will ensure that:

- a. 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;
- b. 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;
- c. System functionality that is Safety-related is recognised early in the life cycle and designed to achieve the necessary level of Performance and Integrity;
- d. A record exists in the Safety Case to justify why the system Safety Requirements are appropriate.

2.1.2 Contracts which adequately cover Safety will ensure that:

- a. Safety Requirements are clearly specified;
- b. Safety interfaces between the MOD and contractor are clearly defined;
- c. The Risk Acceptance regime relevant to the contract is clearly specified and any MOD regulatory requirements are given proper consideration;
- d. The contractor's safety data is provided in an auditable and acceptable form to MOD, including the IPT, FSMOs and any authorities who act as regulator or provide Safety approvals.
- e. The contractor provides access to MOD safety authorities for audit as required.

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.

3 RESPONSIBILITIES

3.1 Accountability

3.1.1 The IPTL is accountable for the completion of this procedure.

3.2 Procedure Management

3.2.1 The IPTL may delegate the management of this procedure to a member (Safety

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

	Manager) or members of the IPT.
3.2.2	The IPT must ensure that appropriate Safety Requirements are developed sufficiently early in the Project life cycle.
3.2.3	As the MOD is a self-regulating organisation, its Policy requires individual IPT Leaders to make their own 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.
3.2.4	The IPT is also responsible for the Safety content of ITTs and Contracts and will use specialist Safety and Contracts support to ensure that they are appropriate.
3.3	Procedure Completion
3.3.1	The Project Safety Manager and PSC 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.
3.3.2	The Project Safety Manager and PSC will be responsible for formally documenting the Safety requirements and justifying that they are appropriate in the Safety Case.
3.3.3	The Project Safety Manager and PSC will be responsible for generating the Safety content of ITTs and Contracts calling on specialist Contracts support as necessary.
4	WHEN
4.1	Safety Requirements
4.1.1	Every Project starts with a need to satisfy common Safety Objectives which derive from MOD Safety Policy (see Section 7.1). These are then interpreted into Project-specific terms to produce: <ul style="list-style-type: none"> a. Safety Requirements in URD; b. Safety Requirements in SRD; c. Requirements for safety mitigation features required to reduce identified Risks.
4.1.2	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 (eg: of inability to achieve Requirements) are identified in a timely manner.
4.2	Reviewing Safety Requirements
4.2.1	The Safety Requirements must be reviewed to ensure that they are appropriate and complete, particularly before Authorisation of Safety Case Reports.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

- 4.2.2 The Safety Requirements must also be reviewed as part of the periodic Safety Case review process (see Procedure SMP12 – Safety Case and Case Report) to ensure that any missing or emergent Safety Requirements are identified. These can include:
- New Requirements due to changes in usage (eg: new functionality, new system context or environment);
 - 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;
 - New Requirements due to changes in Safety Regulation or Safety Approvals applicable to the Project.
 - New Requirements due to developing technology;
 - New Requirements due to recently identified Hazards.

4.3 Coverage of Safety in ITTs and Contracts

- 4.3.1 Safety issues must be addressed in ITTs and Contracts whenever the IPT 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 IPT.
- 4.3.2 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.
- 4.3.3 The IPT Leader 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 (eg require the provision of safety personnel CVs at the ITT 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.
- 4.3.4 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**. 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.

4.4 Demonstration of Compliance with Safety Requirements

- 4.4.1 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.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 5

5 REQUIRED INPUTS

5.1.1 This procedure for Safety Requirements and Contracts requires inputs from:

- a. Outputs from Procedure SMP01 – Safety Initiation;
- b. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis;
- c. Outputs from Procedure SMP11 –Hazard Log;
- d. Outputs from Procedure SMP12 –Safety Case and Safety Case Report;
- e. Outputs from Procedure SMP05 –Hazard Identification and Analysis;
- f. Outputs from Procedure SMP06 –Risk Estimation;
- g. Outputs from Procedure SMP07 –Risk and ALARP Evaluation;
- h. Outputs from Procedure SMP08 –Risk Reduction;
- i. Outputs from Procedure SMP09 –Risk Acceptance.

5.1.2 Generation of the Safety Requirements may use the following reference inputs:

- a. MOD, domain and TLB Policy for Safety;
- b. Description of Capability requirements;
- c. Design description;
- d. Completed Form **SMP01/F/03** - Register of Safety Legislation and Other Significant Requirements.

6 REQUIRED OUTPUTS

6.1 Safety Requirements

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

6.2 Safety Elements of ITTs and Contracts

6.2.1 The primary outputs of this part of the procedure are 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.

7 DESCRIPTION

7.1 Initial Safety Objectives

7.1.1 Flowing from MOD's Safety Policy, every Acquisition Project has three main Safety Objectives:

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 6

<p>a. Compliance with relevant legislation;</p> <p>b. Achievement of safety levels at least as good as statute where legislation does not apply;</p> <p>c. Safety Risks to be Tolerable and ALARP.</p> <p>7.1.2 In addition to this, the Project must satisfy any relevant Safety Regulators or Approval Authorities who may have their own Requirements for system features or information.</p> <p>7.1.3 The production of Project-specific Safety Requirements entails examination of the Capability Requirements, the context (eg. environment and interfacing systems) and the design solution, to define a complete set of Safety Requirements which will satisfy these common Safety Objectives and Approvals Requirements.</p> <p>7.2 Definition of URD Safety Requirements</p> <p>7.2.1 The URD is an all embracing, structured expression of the user need for a bounded operational capability, and is the means by which the Equipment Capability Customer (ECC) 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 URD is therefore the principal aspect in ensuring that the risks associated with a system are ALARP.</p> <p>7.2.2 Safety user requirements shall include acceptance criteria (safety targets) against which the system will be assessed and accepted.</p> <p>7.3 Deriving Safety Requirements by Preliminary Analysis</p> <p>7.3.1 This is the first stage of detailed safety analysis and includes setting detailed safety targets derived from the baseline criteria. It is to be carried out prior to tendering as part of the process of establishing safety requirements. The industrial Designer is to refine this safety analysis early in the development contract when more detailed design information is available.</p> <p>7.3.2 In some cases the mitigation strategies will include new safety requirements (for example new protective functions to be designed in). The Project shall identify the safety requirements that realise the selected mitigation strategies, and ensure that where necessary these are incorporated into the overall safety requirements and TLMP where appropriate. The Project shall ensure that records are maintained to show traceability between hazards and accidents, and the associated safety requirements.</p>	<p>8 RECORDS AND PROJECT DOCUMENTATION</p> <p>8.1.1 Where relevant, the outputs from this procedure should feed into the following:</p> <p>a. SRD (System Requirements Document) – for any specific Safety requirements;</p> <p>b. CSA (Customer Supplier Agreement) – to document agreements on Safety</p>
--	--

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 7

information to be delivered by the IPT;
c. TLMP (Through Life Management Plan);
d. Safety elements of Initial Gate and Main Gate submissions.
8.2 Safety Requirements
8.2.1 The Safety Requirements will be recorded in the following:
a. Project Requirements Management System (eg DOORS);
b. Hazard Log;
c. Safety Case.
8.2.2 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.
8.2.3 The Hazard Log is likely to contain some of the Safety Requirements relating to particular mitigation actions. However, it is unlikely to contain all the Safety Requirements.
8.2.4 The Safety Case must contain all the Safety Requirements, together with the justification of how they were derived. The Safety Case will eventually include Claims that each of the requirements has been satisfied, together with the Argument and Evidence to justify the Claim.

9 RECOMMENDED TOOLS AND FORMS
9.1.1 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.
9.1.2 Guidance Sheet SMP10/G/01 - Safety Topics for ITT 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 ITT.

10 GUIDANCE
10.1 Alignment with Environment
10.1.1 The key alignment opportunity in SMP10 is to ensure wherever possible that Safety and Environmental Requirements are consistent and compatible, and where possible can be achieved by the same action.
10.1.2 It is important, both for Safety and Environmental Management that the location and amount of hazardous and restricted materials in the equipment is known and recorded. Suppliers and service providers should be required to declare this inventory information, with due regard to possible future legislation, and that it should be recorded in the Safety Case.
10.2 Categories of Safety Requirements

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

- 10.2.1 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:
- Legal requirements.** Such as the HSWA and its accompanying legislation, the Merchant Shipping Act 1995, Civil Aviation Act 1982 as amended 2006 or the Road Traffic Act 1991;
 - 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. The respective FSMO can provide advice on certification requirements and advise on MOD specialist safety authorities involved in certification requirements;
 - Safety Objectives.** This includes the general requirements for safety management, eg producing a Safety Case (see Procedure SMP12 – Safety Case and Case Report). It also includes complying with the specialist MOD policy and procedures which are relevant to the particular project or equipment;
 - Safety Targets.** See Section 10.4 below. Further guidance is contained in the domain-specific Safety JSPs and Def Stan 00-56.

10.2.2 It should be recognised that 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 must therefore do more than show that all identified Risks have been made ALARP.

10.3 Safety Requirements Depending on System Function

10.3.1 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 is to recognise functionality which is safety-related so that appropriate Safety Requirements are derived.

10.3.2 Reliability targets shall 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.

10.3.3 Some systems have a defensive role whereby inaction under hostile circumstances may constitute a hazard. Safety targets for such systems shall 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 shall be established and agreed by the IPT Leader after consulting the Safety Panel.

10.3.4 Safety-related functionality can result from the Capability requirement or from the

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

context in which it operates. It is therefore important that the system requirements and the boundary interfaces are 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.

10.4 Qualitative and Quantitative Safety Targets

10.4.1 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.

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

- a. the probability of death per operating hour,
- b. the probability of death per year,
- c. the probability of death over the expected lifetime of the equipment;
- d. the probability of loss of the platform or system.

10.4.3 The way of expressing the target will vary according to the nature of the equipment, eg JSP553 cites aircraft safety targets in terms of probability of death/aircraft hull loss per operating hour.

10.4.4 It must 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.

10.4.5 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), then projects should 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.

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

10.4.7 The system safety targets should 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.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 10

10.4.8 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.

10.5 Individual and Societal Risk Criteria

10.5.1 HSE has published criteria which define the limits of Tolerability for Safety Risks to Individuals (eg workers and general public) and also for Safety Risks which might affect many people simultaneously (eg a major accident at an industrial facility). These generic criteria can help IPTs to define the limits of Tolerability for their systems.

10.5.2 It must be remembered that the HSE's published figures for individual risk apply for the whole working year and individual Projects can only be permitted to 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 FSMOs on the apportionment of Risk to individual systems.

10.5.3 It must also be remembered that 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.

10.5.4 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 must be satisfied for the system to be considered to be Tolerably Safe.

10.6 Apportionment of Safety Requirements

10.6.1 Whilst MOD must 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.

10.7 Responsibility for Safety and Managing Risk

10.7.1 IPT Leaders and contractors negotiating contracts for safety tasks, are reminded that, within the scope of MOD Policy, corporate responsibility for safety remains with the MOD, but responsibility for Managing Risk can be shared according to who is best-placed/competent to manage it. Contractual documents must clearly state the division of work so that all parties understand the requirements to manage those aspects of safety placed on them.

10.7.2 The IPT Leader should ensure that the contractor produces an adequate SMS for the contracted work. Interfaces, lines of responsibility and accountability between the IPT Leader and their contractors should interface effectively and be described in the Project's and contractor's SMSs. IPT Leaders are to ensure that their contractors are

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 11

competent, with appropriate knowledge and experience of civil and MOD safety requirements. Advice on the competence of contractors and managing the safety interfaces can be sought from the FSMOs.

10.8 Manufacturers' and Others' Duties as Regards Articles for Use at Work

10.8.1 Section 6 of HSWA 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 shall be the duty of any person who designs, manufactures, imports or supplies any article for use at work:

- a. to 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;
- b. to 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;
- c. to 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
- d. to 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.

10.8.2 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.

10.9 Contractual Arrangements for Sub-contractors

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

10.10 Prescriptive and Performance-based Standards

10.10.1 Changes brought about by the SMART Acquisition philosophy supports the MOD's move 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

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 12

include situations where systems are of well understood technology and functionality and there is established good practice for controlling the Safety Risks.

10.10.2 Performance based standards align well with the goal setting principles of the Policy. However, prescriptive/deterministic rules can still form effective parts of a SMS for specific risks, as they:-

- a. are often widely used and understood;
- b. do not require advanced knowledge or deep competence to apply, making them easier to contract against;
- c. enable low-tech designs to be quickly and repeatedly generated in a reliable/predictable format;
- d. capture expertise/historic lessons learnt into a readily useable format or formulae, permitting benchmarking;
- e. support established feedback and review systems from in-service experience, permitting easier survey, verification and acceptance into service;
- f. provide a more clear-cut route to achieving a safety Requirement, which is less susceptible to corruption by programme or resource considerations.

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

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

10.11 Hierarchy of Standards

10.11.1 To comply with Secretary of State's policy, the MOD needs to 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:

- a. European Union civil standards.
- b. International civil standards.
- c. UK civil standards.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 13

d. Standardised NATO Agreements (STANAGs).

e. UK Defence Standards.

10.12 Defence Standards for Safety

10.12.1 It is recommended that appropriate standards are used, for example:

- a. Defence Standard 00-56 Issue 4 Safety Management Requirements For Defence Systems;
- b. Standards applicable to the system environment, for example, Def Stan 00-970 Design & Airworthiness Requirements for Service Aircraft, Def Stan 05-123 Technical Procedures for the Procurement of Aircraft Weapons & Electrical Systems etc

10.13 Software Safety Requirements

10.13.1 For programmable systems, it is normal to derive a Software Requirements Specification (although other titles may be used). This should define the functions that the software must perform which, taken together with the capabilities of the hardware components, will allow the overall system to meet its requirements.

10.13.2 In just the same way as safety requirements are set at the system level and form part of the overall system requirements, it is usual to establish a Software Safety Requirements Specification, either as a subset of the Software Requirements Specification or as a separate document.

10.13.3 The software safety requirements will normally include requirements for features which can tolerate faults as well as requirements for dependability of the software. PrEN 50128 provides guidance on fault-tolerant features. Dependability should be treated by specifying the SIL of the software.

10.13.4 Evidence of validation of the software against its requirements should be produced. This is usually documented in a software Safety Case Report or a software assessment report and a software validation report. This evidence will form an important part of the overall system Safety Case.

10.14 Justification and Validation of Safety Requirements

10.14.1 When defining Requirements, a top-level Safety Assessment is useful for categorising Requirements and justifying their selection as follows:-

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

10.14.2 When an action or decision is challenged, the Safety Case is likely to be scrutinised by military Boards of Inquiry (BOI) and civil courts of law. IPT Leaders should therefore ensure that safety Requirements for their projects are clearly recorded for

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 14

external readership or for auditors together with clear justifications that they are suitable and sufficient.

10.14.3 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:-

- a. Compliance with deterministic standards, demonstrated as good or best-practice, for a risk in a mature or well understood domain or;
- b. Achievement of qualitative Requirements, (high-level principles, work practices etc.) for more novel risks, or for systematic failure mechanisms;
- c. 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.

10.15 Demonstration that Requirements have been Satisfied

10.15.1 Provision must be made for the Validation of the Safety Requirements made in the design and build phase during the lifetime of the system or equipment.

10.15.2 After the safety requirements apportioned to system elements and components are verified to be met, it is necessary to conduct an assessment to verify that the total system meets its overall Safety requirements.

10.16 Inability to Satisfy the Safety Requirements

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

- a. it may be decided to accept the risk, in which case the appropriate management level as defined in SMP09 – Risk Acceptance should endorse the decision,
- b. changes may be made to the design or
- c. 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.

10.17 Domain-Specific Guidance and References

10.17.1 Additional guidance on Safety Requirements and Contracting is contained in the following references:

- a. Land Systems: JSP 454 Issue 4:
 - i. Safety Requirements Part 1 Section 4
- b. Ship Safety Management: (JSP 430 Issue 3):
 - i. Design Safety Requirements (Section 6.2);

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

MOD	SMS Procedures	Procedure SMP10
SMP10: Safety Requirements and Contracts		Page 15

- ii. Contractor Interfaces (Section 7.2);
- c. Airworthiness: (JSP 553 1st Edition):
 - i. Safety Criteria (1.37 et seq.);
 - ii. Responsibility for Design and Development (Annex N);
 - iii. It should be noted that for air systems, contractors should be Design Approved Organisations (Def Stan 05-123 refers).
- d. Ordnance, Munitions & Explosives (OME): (JSP 520 Issue 2.0):
 - i. Safety Standards (0109-0112);
 - ii. Safety Requirements (0408-0410).
 - iii. 0409 “Generic OME safety user requirements are generated, reviewed and maintained by DOSG. For each new OME capability, the appropriate generic requirements shall be developed into project specific safety requirements. The output from this process should be a set of OME safety user requirements, written in safety criteria terms.”
- e. Nuclear Propulsion (JSP 518 Issue 1.2):
 - i. Principle 24 – Reliability Targets (A63).

10.18 Guidance for Different Acquisition Strategies

10.18.1 The IPT Leader is required to positively assure that safety has been adequately addressed, on the MOD’s behalf, wherever Design Authority resides with industry (COTS), according to the legal principles of civil liability, the sale and purchase of goods.

10.19 Warnings and Potential Project Risks

10.19.1 It is most important that Safety Requirements are 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.

10.19.2 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.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007