DE&S SAFETY & ENVIRONMENTAL PROTECTION LEAFLET 08/2013
SAFETY MANAGEMENT GUIDANCE FOR SOFTWARE ONLY PROJECTS

Guidelines for achieving confidence that the integrity of software products delivered to military systems, that are not considered to be safety related, is assured.

Sponsor: DES TECH-QSEP-Hd	**Version No**: 1.3[1]	**Date of issue**: 03 Sep 2014
Author: DES TECH-QSEP SUPPORT		
Contact: 030 679 825520		

References:

A. ASEMS Acquisition Safety and Environmental Management System.
B. Def Stan 00-56 Safety Management Requirements for Defence Systems[2].

INTRODUCTION

1. Reference A contains the mandated DE&S Project Oriented Safety Management System (POSMS) that provides the framework for managing safety at all stages of acquisition. The Safety Management System (SMS) is needed to show that all necessary safety activities have been, and will continue to be, undertaken to an adequate standard throughout the life of the project. A Safety Case contains 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. Safe does not imply that there is an absence of risk, but that the risk can be demonstrably reduced to a level that is Broadly Acceptable, or at least Tolerable and As Low As Reasonably Practicable (ALARP).

2. Reference B, defines Programmable Elements (PE) as elements of Products, Systems or Services (PSS) that are implemented in software or custom hardware. Annex D of Reference B[3], identifies 5 principles on which the integrity of PE is to be based, these are:

a. Principle 1. PE Safety Requirements shall be defined to address the PE contribution to system hazards.

b. Principle 2. The intent of the PE Safety Requirements shall be maintained throughout requirements decomposition.

[1] Version 1.3 has hyperlink updates only.

[2] Definitions used in Defence Standard 00-56 Issue 5 are extant within this leaflet.

[3] Definitions used in Defence Standard 00-56 Issue 5 are extant within this leaflet.

c. Principle 3. PE Safety Requirements shall be satisfied.

d. Principle 4. Hazardous behaviour of the PE shall be identified and mitigated – addressed by failure modes and supported by designing for safety.

e. Principle 5. The confidence established in addressing the other PE safety principles shall be commensurate to the contribution of the PE contribution to system risk and will be addressed by Design Integrity requirements.

3. Where a software product is required to perform or support a safety related function, the requirement for evidence is understood. However, where a PE does not appear to have either any safety related functionality nor provide a service in support of a safety related function in a PSS, the requirement for sufficiency of evidence is not clear.

PURPOSE

4. An essential element of SMSs is the recording of evidence in support of Safety Cases or safety assessments that must be retained for audit and assurance or a legal or regulatory requirement. This document identifies guidance for achieving confidence that the integrity of software products that are developed for a specific function systems that are not considered to be safety related, is assured. It identifies a means of compliance, within the principles of an SMS, for making a claim that the software product does not have a failure mode that contributes to a credible hazard to the PSS that it is intended to operate with, or support.

POLICY

5. The Secretary of States' Policy on safety is delivered through JSP 815 which requires duty holders to put in place safety management arrangements to control their activities, conduct them safely and manage risk. The degree of rigour applied by a duty holder to risk assessment for an activity is proportionate to the consequences of failure.

6. Part 1 of Reference A mandates the use of ASEMS for all DE&S Projects. The doctrine delivered through POSMS identifies that:

a. For acquisition of material, equipment and services of all kinds, safety management is to begin at the requirements definition stage and is to be carried forward through-life to disposal/termination.

b. Suitably Qualified and experienced personnel carry out safety assessments.

c. Risks are managed to broadly acceptable, or tolerable and ALARP.

d. Safety requirements for all aspects of maintenance and operational use are to be taken into account.

e. For a software product, where the functionality within or in support of the PSS changes from those originally identified, the risks will need to be re-assessed. Examples of changes necessitating reassessment of risk:

(1) Where the delivered software product is to be used with or interfaced with a new PSS.

(2) Changes in the specification of the PSS. ie, additional functionality for the

software product or use of built-in functionality (eg OTS[4]) not previously required or assessed.

(3) Changes to stakeholder requirement, ie any change to the defined use in the defined environment, eg for a developing PSS capability.

(4) Where an emerging or unexpected behaviour occurs.

7. POSMS requires that a hazard log should contain all identified hazards and accidents for the system including those considered as not credible and must show that they have been considered ALARP. Where an analysis identifies a credible hazard, further safety assessments must be carried out to support the appropriate Safety Case.

APPLICATION

8. Consideration must be given to the relevant PSS boundaries, integration and interfacing affected by the software product for its given use and operating environment within or supporting a PSS. This should also ensure that all stakeholders are identified and can be engaged in the process.

9. This guidance can be used by PTs to support assurance that the claim that the software product does not contribute to a credible hazard to the PSS, can be justified and is compliant with the DE&S POSMS. It also supports the 5 Principles of PE integrity.

10. Where a possible hazard[5] is identified that is considered reasonable and realistic based on the best design information available[6]. Where the software product has been assessed as having a potential to contribute to a credible hazard in a PSS, further safety assessments must be carried out.

11. Any change to requirements for the software product or PSS used for the original argument, or divergence from the given use or operating environment negates the claim that the software product does not contribute to a credible hazard to the PSS and its use should be discontinued until an appropriate risk assessment is carried out.

12. This good practice should also be used by Operational/Platform Duty holders for identifying safety risks within their areas of responsibility which are presented through the use of software tools; i.e. through over-reliance on such tools, the use of incorrect information for decision making or lack of procedural coherence between software tools and operational tasks.

a. The user community may not have Suitably Qualified and Experienced Persons (SQEP) to make a valid judgement in completion of the questionnaire nor confidence in acceptance of the safety statement.

b. It is good practice to consult with SQEP Subject Matter Experts (SMEs), particularly safety practitioners.

c. Regulator SMEs must be consulted where the software is to be used within a regulated

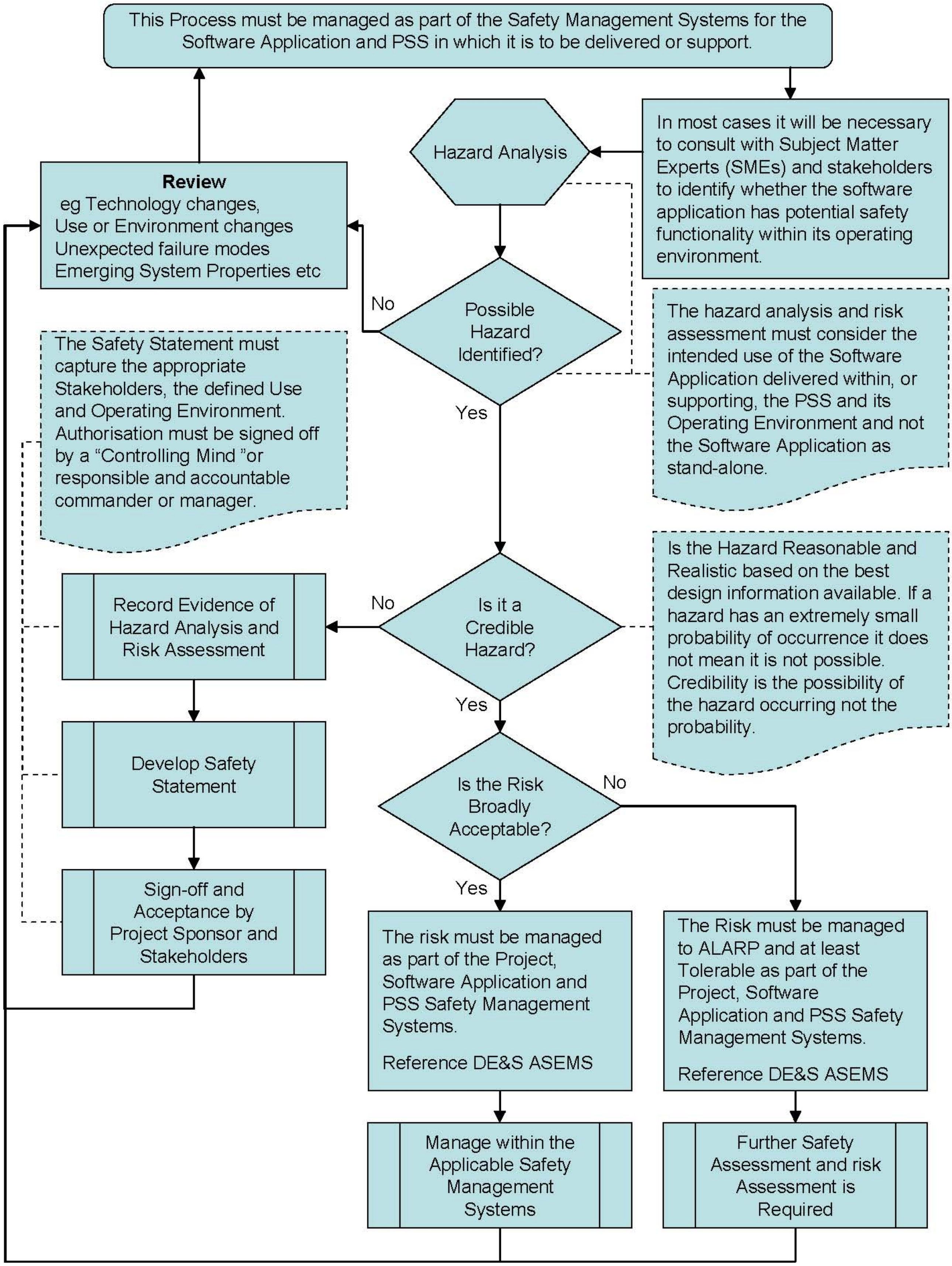
[4] Off the Shelf includes all variations eg Commercial off the Shelf or Military Off the Shelf (COTS/MOTS). An issue to be monitored particularly where there is additional built-in functionality that was not intended to be used in meeting the original requirement but may be still be accessible to the user.

[5] Unlike hardware, software cannot directly cause physical harm. Software is an enabler of additional functions which as a consequence of error and/or failure may lead to a hazardous event and possibly to harm; therefore the evaluation of software must be able to determine its potential for contributing to system hazards. This can only be done by fully appreciating the role the software plays in the operating environment it is being utilised in.

[6] If a hazard has an extremely small probability of occurrence it does not mean it is not possible. Credibility is the possibility of the hazard occurring, not the probability.

domain.

13. This guidance may be considered as good practice only as part of an SMS. This good practice does not override obligations for meeting legislation, MOD policy or Regulations. A Flowchart of the assessment process is shown in Figure 1.



This Process must be managed as part of the Safety Management Systems for the Software Application and PSS in which it is to be delivered or support.
Hazard Analysis
In most cases it will be necessary to consult with Subject Matter Experts (SMEs) and stakeholders to identify whether the software application has potential safety functionality within its operating environment.
Review
eg Technology changes,
Use or Environment changes
Unexpected failure modes
Emerging System Properties etc
No
Possible Hazard Identified?
Yes
The hazard analysis and risk assessment must consider the intended use of the Software Application delivered within, or supporting, the PSS and its Operating Environment and not the Software Application as stand-alone.
The Safety Statement must capture the appropriate Stakeholders, the defined Use and Operating Environment. Authorisation must be signed off by a “Controlling Mind ”or responsible and accountable commander or manager.
Is the Hazard Reasonable and Realistic based on the best design information available. If a hazard has an extremely small probability of occurrence it does not mean it is not possible. Credibility is the possibility of the hazard occurring not the probability.
Record Evidence of Hazard Analysis and Risk Assessment
No
Is it a Credible Hazard?
Yes
Develop Safety Statement
Is the Risk Broadly Acceptable?
No
Yes
Sign-off and Acceptance by Project Sponsor and Stakeholders
The risk must be managed as part of the Project, Software Application and PSS Safety Management Systems.
Reference DE&S ASEMS
The Risk must be managed to ALARP and at least Tolerable as part of the Project, Software Application and PSS Safety Management Systems.
Reference DE&S ASEMS
Manage within the Applicable Safety Management Systems
Further Safety Assessment and risk Assessment is Required

FIGURE 1. THE ASSESSMENT PROCESS.

SAFETY GUIDANCE FOR SOFTWARE ONLY PRODUCTS

14. Purpose. To provide a consistent method of deciding the scale of safety evidence necessary when utilising a particular software product within a defined operating environment and therefore helping prevent excessive and possibly nugatory safety management work.

15. Description. The Questionnaire (Annex A), in conjunction with knowledge of the intended/perceived/actual system in which the software product is intended to be utilised, can be used to determine whether the use of the software product is capable of contributing to hazardous events which may, if left unattended lead to unintended consequences (harm). Although there are two possible outcomes to the questionnaire, only one is defined.

a. Safety Benign: The software product (when utilised in a given operating context) has no effect on operational safety, otherwise;

b. Safety Related: The software product or system is not safety benign and further safety management risk assessment is required.

16. Questionnaire Guidance. The questionnaire (Annex A) must be completed by persons with suitable knowledge of the platform of system the software supports. It is expected that it will be completed by stakeholders who utilise the software directly and by those who are affected/influenced by the software products output in conjunction with the PT delivering the product and not in isolation by a single individual. Consultation with SMEs and Stakeholder representatives from relevant Platforms, Systems, other business functions or regulatory bodies will be required to support completion of the questionnaires.

a. Each question in the questionnaire must be answered as either 'Yes' or 'No'. If there is any uncertainty about an answer then a suitable SME must be consulted before making a decision. If the answer to any question is 'Yes, then further safety assessment work is required.

b. The completed questionnaire must be retained with the Software Safety Statement to provide an auditable trail to show how the final result was gained along with any supporting documentation.

c. Question 8 requires consultation with stakeholders SMEs particularly where the software product is to be used within a Regulated domain.

17. Results. There are two possible results from the questionnaire:

Safety Benign	Not safety benign, (Safety Related)
If all the answers in the questionnaire are **'No'** then the software is considered to be Safety Benign (within the operational context in which it has been assessed). Evidence that the software product is benign should consist of the completed questionnaire and completed Safety Statement. Other supporting documentation may be included if needed. These documents should be presented to the appropriate duty holder and/or Regulator to support the relevant Project or Service delivery milestone and in support of JSP 604 compliance.	If any of the answers are **'Yes'** then the system and/or software is not Safety Benign. A detailed and thorough assessment of how the software product contributes to operational safety risks must now be explored and presented within a System Safety Case. The level of evidence necessary to satisfy the applicable duty holders, regulatory body(s) and/or system owner is to be determined through a Project Safety Panel set up by the PT delivering the software product following extant POSMS methodology and MOD safety standards.

18. Software Safety Statement. A template for a Software Safety Statement is at Annex B.

a. Where the Safety Statement identifies the software product as Safety Benign then it must be authorised at appropriate management levels on behalf of the software product sponsor, owner and Delivery Team.

b. Where the Safety Statement identifies the software product as Not Safety Benign then it must be authorised at appropriate management levels on behalf of the sponsor and Delivery Team and accepted by the system owner/applicable duty holder. This also identifies that further safety analysis is required at the software product and PSS level and should provide authority for the Delivery Team to develop a System Safety Case for their software product and/or support a PSS safety assessment.

c. Any supporting documentation must be referenced and retained for audit.

d. Benign Safety Statements must be periodically reviewed by the Delivery Team to ensure they remain extant through the life of the system in which they are being used.

19. Operational Information. The software product owner/duty holder/user should be aware that:

a. The information output from the software product is not to be used as source to inform safety related decisions without further safety and risk assessment.

b. The accuracy/validity/timeliness of the information cannot be claimed to be unfailingly correct.

c. Where the software product is used in support of a system that has a Safety Case the Benign Safety Statement and any supporting evidence should be included and where necessary, further assistance sought from the Delivery Team to support system Hazard Identification and Analysis.

d. Relevant Safety Cases should include evidence to support the claim that the software product is safety benign or, if safety related, is managed through the appropriate SMSs to mitigate the risk to at least tolerable and ALARP.

20. Operational Requirements. The following requirements underpin the categorisation of the software product as Benign

a. The software product sponsor understands the limitation of the software product in the defined operating environment and context of use and the necessity that any contrary evidence must be brought to the attention of the Delivery Team as soon as possible..

b. The software product sponsor provides sufficient information to the software product owner, duty holder and user to ensure the software product is employed within the defined limitation of use, within the defined operating environment.

c. The software product sponsor will inform the Delivery Team immediately of any change to the circumstances in which the software product is employed or impact on assumptions supporting the assessment.

d. Where this software product is assessed as **not safety benign** (Safety Related), ie where a credible hazard is identified, the safety and risk assessment must be managed through the appropriate PSS SMS[7].

Meeting the Principles

21. This guidance intends to meet the Principles identified in Ref B:

a. Principle 1 and 4. This guidance identifies that the safety analysis must be carried out for its' defined use in its operational environment, to ensure that the software product does not contribute to system (or PSS) hazards.

b. Principle 2 and 3. The intent of the PE Safety Requirements shall be maintained throughout requirements decomposition. This guidance meets this principle in as much as where there are safety requirements (derived from credible hazards) it requires them to be managed within the appropriate SMSs and where there are no credible hazards identified, there is a requirement for regular review as part of a software product SMS.

c. Principle 5. This guidance directs the Delivery Team, owner, duty holder and users to manage the software product appropriate to the outcome (level of risk) of the safety analysis for a defined use and operating environment.

FEEDBACK & CONTINUOUS IMPROVEMENT

22. Any comments or suggestions for improvement of this instruction should be directed to the author, who will maintain them on behalf of the sponsor.

ANNEXES

A. Questionnaire for Assessment of Safety Benign Software
B. Safety Statement

Word versions of the Annexes are available from the Defence Intranet QSEP ASEMS Page.

[7] The software product can be used by a System with a safety function in a way that can affect control and, therefore, safety. In such circumstances the software product must have sufficient integrity and reliability to ensure that the safety functionality of the system (rather than the software product) is not compromised.

QUESTIONNAIRE FOR ASSESSMENT OF SAFETY BENIGN SOFTWARE

No	Question	Yes/No	Guidance
1	Are there any functional safety requirements identified within the software or system User Requirement Document (URD), Systems Requirement (SRD) or other requirements documentation?		Check the URD/SRD for safety requirements and consider other formal documentation such as Concept of Use, Concept of Operations, Concept of Employment, Through Life Management Plan etc. This may be especially relevant to legacy software which may lack a full set of project documentation.
2	Does the software support systems that carry out or plan a potentially hazardous activity?		Consider the system that the software is part of. For example control of a critical system such as medical procedures. If so does the software play a part in the performance of that function? The system owner should be consulted when answering this question to determine the significance of the software’s role in the system.
3	If the Software captures data from external sources, is that data used by the Software for the control/analysis of systems with a safety function?		Consider the effects on the system receiving erroneous data from the software including the system’s sensitivity to errors.
4	Would the loss of the software cause the system to present a potentially hazardous situation?		Consider what would happen if the software became unavailable due to power failure, hardware failure etc. Look at this from a safety perspective rather than a Business Continuity perspective. Also consider if there is any redundancy or reversionary capability in the software and system.
5	Could the system present a potentially hazardous situation if stale information is received from or sent to the software?		Consider the impact on the system if the software delivers information either too late, too early or out of step.
6	Could the system present a potentially hazardous situation be caused by the system or operator receiving corrupt but credible data from the software?		Consider the impact on the system or operator if the software delivers corrupt but credible information, including whether the software is delivering the only source of information used to make a decision.
7	Could software error be the sole source of a potentially hazardous situation through the system or operator?		Consider if the system or operator is relying on the software to operate correctly, especially if the software is a single source of information being used.

No	Question	Yes/No	Guidance
8	Has the consultation with Subject Matter Experts (SMEs) and stakeholders identified that the software product has potential safety functionality within its operating environment?		Systems within these domains will typically pose safety issues requiring further safety management. SMEs and the user community **must** be consulted. **Note. SMEs (SQEP) eg:** **Ordnance, Munitions or Explosives;** **Nuclear Propulsion or Nuclear Weapons;** **Radiation (ionising/non ionising);** **Air, Land, Maritime; Safety** **System Safety,** **Software,** **Public Private Partnership arrangements;** **OGD**

The software product has been identified as **Safety Benign/ Safety Related.***^{**delete as applicable**}

Where the software product is **not** safety benign, the system owner/applicable duty holder has been notified.

Delivery Team Assessor	
Post	
Signature	
Date	

Sponsor Representative	
Post	
Signature	
Date	

System User Representative	
Post	
Signature	
Date	

Regulator SME *(where necessary)*	
Post	
Signature	
Date	

system owner/duty holder*(where necessary)*	
Post	
Signature	
Date	

ANNEX B TO
SEP LEAFLET 08/2013
DATED 25 JUN 2014

DELIVERY TEAM

SAFETY STATEMENT FOR

SOFTWARE NAME

AS UTILISED IN

OPERATING ENVIRONMENT/CONTEXT

AUTHORISATION

Prepared By Delivery Team	
Post	
Signature	
Date	

Approved By Delivery Team	
Post	
Signature	
Date	

Authorised By Delivery Team	
Post	
Signature	
Date	

Authorised By System User Representative	
Post	
Signature	
Date	

Accepted by System Owner/Duty holder	
Post	
Signature	
Date	

Authorised By Regulator	
Post	
Signature	
Date	

References: delete as applicable

Delivery Team Safety Management Plan

Products, Systems or Services (PSS)/Operating System Safety Management Plan

RECORD OF REVIEWS AND AMENDMENTS

No	Details	Name	Signature	Date

ISSUE STATE RECORD

Issue	Date	Remarks

SOFTWARE PRODUCT SAFETY STATEMENT FOR

SOFTWARE NAME

AS UTILISED WITHIN

OPERATING ENVIRONMENT/CONTEXT

EXECUTIVE SUMMARY

1. This is a Safety Statement for the above software product as utilised in the defined operating environment/context produced by the Delivery Team.

a. This statement covers the effects on the safety of the defined operational environment from the data produced, displayed and/or transmitted by this software product.

b. It does not address any associated hardware components. This software product has been classified as being:

- **Safety Benign** **delete as applicable** software product insofar as it **does not** have a safety impact in its' defined operational environment/Context and it is not being used as a source to support safety related decisions or functions.

- **Not Safety Benign** **delete as applicable** software product insofar as it **does** have a safety impact and it will be used as a source to support safety related decisions or functions.

c. A Benign Safety Statement meets the requirement for a Safety Case as defined in JSP 815 Defence Environment and Safety Management.

d. A Non-Benign (safety related) software product requires additional safety assessments to be carried out and the development of appropriate Safety Cases supported by the Delivery Team.

DESCRIPTION OF SOFTWARE PRODUCT

2. ***Note.*** *Insert brief software product description and its role in the customers system. This should include a list of stakeholders at Enclosure 2*.

HAZARD IDENTIFICATION AND ANALYSIS

3. Basic Hazard Identification and Analysis has been carried out and the results are recorded in the Safety Assessment Questionnaire, Enclosure 1 the result is:

- There were no safety risks or hazards identified relating to the use of this software product in its' given operating environment/context and therefore there is no requirement to carry out further safety analysis at this time. **delete as applicable**

- At least one safety risk or hazard has been identified relating to the use of this software product and therefore there is a requirement to carry out additional safety analysis for the software product before it can be considered for deployment within the defined operating environment/context. **delete as applicable**

SAFETY STATEMENT

4. It is claimed that:

- There are no associated credible hazards and hence there is no safety risk associated with the data produced, displayed and/or transmitted by this software product within the defined operating environment/context, and hence there is no requirement to declare ALARP as there is no risk that can be reduced. delete as applicable

- It has been identified that at least one hazard or safety risk related to the use of this software product within the defined operating environment/context and the Delivery Team should support development of appropriate Safety Case(s) in order to formally capture and manage risks to broadly acceptable, or tolerable and ALARP. The Safety Cases should be developed in accordance with POSMS and applicable MOD safety standards. delete as applicable

ASSUMPTIONS

5. The following assumptions underpin the categorisation of this software product as **Safety Benign/Not Safety Benign** delete as applicable within the defined operating environment/context:

a. The software product Sponsor, System User Representative (and Regulator where necessary) has read and agreed with Enclosure 1.

b. The software product Sponsor, System User Representative agrees to make users aware on the limitation of use within the defined operating environment/context and to review the safety assessment where an emerging risk or change of use is likely to occur.

***Note** Include any additional assumptions here relating to the use of the software product, the users/use of the data produced/displayed by the software and any links to other software that is used to either send or receive data*.

SAFETY MANAGEMENT ACTIVITIES

6. This software product is categorised as:

- **Safety Benign** within the defined operating environment/context. However, the analysis and safety statement is included in the Safety Management Plan (SMP Reference………………..) and the applicability of this Statement will be reviewed on an at least an annual basis (ie within 12 months of authorisation) and will be subject to internal and external audit and review procedures delete as applicable.

- **Not Safety Benign** within the defined operating environment/context, the Delivery Team are required to carry out additional safety analysis and support development of appropriate Safety Case(s) in accordance with the requirements of ASEMS. delete as applicable

CONCLUSIONS AND RECOMMENDATIONS

7. Conclusions. Software can be used by a System in a way that can affect information/data delivery or system functionality and hence unintended behaviour can contribute to a system hazard. In such circumstances the software must have sufficient integrity and reliability to ensure that the safety functionality of the system (rather than the software) is not compromised. However, in this case it is claimed the deployment of this software product within the defined operating environment/context is not used in this way and has been identified as Safety Benign[*].

[*] As there are no credible hazards ALARP justification is not requires as there are no risks to reduce.

8. Recommendations. The Sponsor, System user Representative or Duty holder must ensure it is understood that this software product is not used in a way other than as defined in this statement.

a. This software application should not be used as a source to support safety related decisions or activities.

b. If any changes to use or operating environment/context for this software product, its must not be used until an appropriate risk assessment is carried out. The Delivery Team is to be notified as soon as possible.

c. ***Note.*** *Include any additional recommendations relating to the use of the software product in the context of System Safety*.

Appendix: 1. References and Supporting Documentation.

Enclosures:

1. Safety Assessment Questionnaire dated dd mmm yyyy.

2. List of Stakeholders for **Error! Reference source not found.**

ANNEX A TO

Software Name Safety Statement

DATED DD MMM/ YYYY

REFERENCES AND SUPPORTING DOCUMENTATION

Ser	Document Title	Version	Description/Purpose of Document
1.			
2.			
3.			
4.			