

**MSc Project Report**

# Assessing the Use of a Safety and Support Questionnaire in Support of a Service Modification Process

Antony DH Gower MBE

Supervisor: Dr M Nicholson

Submitted in part fulfilment of the MSc in Safety Critical Systems Engineering in the  
Department of Computer Science at the University of York  
March 2006

This report contains 43,120 words in total, including Appendix A, using the Microsoft Word 2003 word count command.

## Abstract

The aim of this project was to confirm what safety and safety assurance knowledge exists within the military aviation engineering world of those completing a Safety and Support Questionnaire as part of a tri-service Service Modification process. It also investigated whether there is a requirement to provide some form of guidance tool in this area and to indicate what form this guidance should take. In particular, the study looked closely at the completion of a question (Q6.01a), which asks the person completing the Safety and Support Questionnaire whether there is an effect on the Safety Case, the required changes to the Safety Case, and associated actions, which are caused by the introduction of a Service Modification.

The Safety and Support Questionnaire is normally completed and reviewed by non-safety specific aviation engineers and this one small question presents a plethora of areas within the safety engineering world that the aviation engineer should be aware of. A questionnaire was developed in four sections covering the role, competencies and experiences of the aviation engineer, through knowledge of safety terms, tools used in support of completing the questionnaire and what guidance the aviation engineer feels is necessary to complete Q6.01a fully. The questionnaire sets the basis for the proposed guidance.

The questionnaire addressed aviation engineers within the rotary world IPT's who review the SM processes, Service Modification Teams and Trials teams within the three armed Services who develop the SM's for both rotary and fast jet aircraft operations and Engineering, Development and Investigation Teams who review SM's for fleet installations.

## Acknowledgement

*Dedicated to my wife Lesley and our two children Dale and Nicola – thank you for being so patient.*

My personal thanks to Dr Mark Nicholson who acted as my project supervisor and provided guidance, direction and encouragement throughout.

Finally to all those who responded to the questionnaire and to all the Staff in the SMS team at Middle Wallop who had to endure my incessant questioning of the Service Modification process.

# Table of Contents

<b>MSc Project Report</b> .....	<b>i</b>
<b>Abstract</b> .....	<b>ii</b>
<b>Acknowledgement</b> .....	<b>ii</b>
<b>Table of Contents</b> .....	<b>iii</b>
<b>List of Figures</b> .....	<b>vi</b>
<b>List of Tables</b> .....	<b>vi</b>
<b>Chapter 1 - Introduction</b> .....	<b>1</b>
<b>1.1 Background</b> .....	<b>1</b>
<b>1.2 Project Aims</b> .....	<b>1</b>
<b>1.3 Background to Service Modification</b> .....	<b>2</b>
<b>1.4 Motivation for the Project</b> .....	<b>4</b>
<b>1.5 Project Structure</b> .....	<b>4</b>
<b>Chapter 2 – Literature Review</b> .....	<b>5</b>
<b>2.1 Use of Single Modification Processes and Regulatory Requirements</b> .....	<b>5</b>
2.1.1 Requirements for a Single Policy .....	5
2.1.2 The Importance of Aviation Safety to the Ministry Of Defence .....	5
2.1.3 Aviation Safety .....	5
2.1.4 Military Aviation Safety Case .....	6
2.1.5 Flight Safety and Airworthiness Accountability.....	6
2.1.6 Joint Service Procedure 553 - Military Airworthiness Regulations.....	7
2.1.7 Military Aircraft Release .....	7
2.1.8 Release To Service.....	7
2.1.9 Release To Service Authority .....	7
2.1.10 The ‘As Flown’ Safety Case .....	8
2.1.11 Aircraft Document Set .....	9
<b>2.2 Reasons for Modification</b> .....	<b>9</b>
2.2.1 Advantages and Disadvantages of Using a Designer Modification.....	10
2.2.2 Design Organisation.....	10
2.2.3 Advantages and Disadvantages of Using a Service Modification .....	10
2.2.4 Modification.....	11
2.2.5 Service Modification.....	12
2.2.6 Cover Modifications .....	12
<b>2.3 Past Procedures Used To Modify Military Aircraft</b> .....	<b>12</b>
2.3.1 Service Engineered Aircraft Radio Installation Modification .....	13
2.3.2 The Service Engineered Modification .....	13
<b>2.4 The Safety Case and Management of Change</b> .....	<b>13</b>
2.4.1 Safety Case Change Management.....	14
<b>2.5 Safety and Support Questionnaire</b> .....	<b>15</b>
2.5.1 The Safety and Support Questionnaire .....	15
2.5.2 Safety and Support Questionnaire Response Form.....	18
2.5.3 Completing The Safety and Support Questionnaire .....	20

2.5.4	Knowledge and Competencies for the Safety and Support Questionnaire .....	21
2.5.4.1	The Airworthiness Competencies Set .....	22
2.5.4.2	The Institution of Electrical Engineers Competency Guidelines .....	22
2.5.4.3	Summary of Knowledge and Competencies for the SSQ .....	23
<b>2.6</b>	<b>Identify With Forms of Check Listing and Questionnaires .....</b>	<b>23</b>
2.6.1	What is a Questionnaire? .....	23
2.6.2	Questionnaires in Usability Engineering .....	23
2.6.3	Basic Types of Questions.....	25
2.6.3.1	Factual Type Questions.....	25
2.6.3.2	Opinion Type Questions .....	25
2.6.3.3	Attitude Type Questions .....	25
2.6.4	Closed and Open Ended Questionnaires.....	25
2.6.5	Examples of Questionnaires Used in Other Industries .....	26
2.6.6	Checklists.....	29
2.6.7	SSQ Summary.....	30
<b>2.7</b>	<b>Review of Standards and What Guidance They Provide .....</b>	<b>30</b>
2.7.1	Defence Standard 05-123.....	30
2.7.2	Defence Standard 00-56 – Safety Management Systems for Defence Systems .....	31
2.7.3	Superseded Defence Standards .....	33
2.7.4	MIL-STD-882B .....	33
2.7.5	Comparison of DS 00-56 and Mil Std 882B.....	34
2.7.6	Summary of Standards.....	34
<b>Chapter 3 – Defining the Requirements of Question 6.01a of the Safety and Support Questionnaire..</b>		<b>35</b>
<b>3.1</b>	<b>Identification of Terms Used in Support of Q6.01a of the SSQ .....</b>	<b>36</b>
3.1.1	Airworthiness.....	36
3.1.2	Aircraft Release and Flight Trials.....	36
3.1.3	Certificate of Design .....	36
3.1.4	Hazard.....	37
3.1.5	Hazard Log .....	37
3.1.6	Risk .....	38
3.1.7	The ALARP Principle.....	39
3.1.8	Safety .....	40
3.1.9	Probability Matrix.....	40
3.1.10	Safety Critical System.....	40
3.1.11	Safety Related System .....	40
3.1.12	Safety Case .....	41
3.1.13	Safety Case Contents .....	42
3.1.14	Safety Management System.....	43
3.1.15	Goal Structuring Notation.....	43
3.1.16	Summary .....	44
<b>Chapter 4 - Developing and Analysing a Questionnaire.....</b>		<b>46</b>
<b>4.1</b>	<b>Planning the Study .....</b>	<b>46</b>
<b>4.2</b>	<b>Basic Process of Survey Research.....</b>	<b>46</b>
4.2.1	Define the Research Aims .....	47
4.2.2	Identify the Population and the Sample .....	47
4.2.2.1	Sample Sizes .....	47
4.2.3	Distributing and Collecting of the Questionnaire .....	47
4.2.3.1	Self-Administered Questionnaire.....	48
<b>4.3</b>	<b>Design of the Questionnaire .....</b>	<b>48</b>
4.3.1	Determine the Questions to be Asked.....	48
4.3.1.1	Questionnaire Design.....	49
4.3.1.2	Wording of the Questionnaire.....	49

4.3.1.3	Examples of Questions Used .....	50
4.3.1.4	Questionnaire Format - Section 1 Questions .....	51
4.3.1.5	Questionnaire Format - Section 2 Questions .....	52
4.3.1.6	Questionnaire Format - Section 3 Questions .....	52
4.3.1.7	Questionnaire Format - Section 4 Questions .....	53
<b>Chapter 5 - Evaluation.....</b>		<b>54</b>
<b>5.1</b>	<b>Summary of Completed Questionnaires .....</b>	<b>54</b>
5.1.1	Initial Observations.....	56
5.1.2	Evaluation of Section 1 – Questions 1 To 12.....	56
5.1.2.1	Question 3 .....	56
5.1.2.2	Question 4 .....	56
5.1.2.3	Question 7 .....	57
5.1.2.4	Question 8 .....	58
5.1.2.5	Question 10 .....	59
5.1.2.6	Question 11 .....	60
5.1.2.7	Question 12 .....	61
5.1.3	Evaluation of Section 2 – Questions 13 To 21.....	62
5.1.3.1	Question 13 .....	62
5.1.3.2	Question 14 .....	62
5.1.3.3	Question 18 .....	64
5.1.3.4	Question 20 .....	64
5.1.3.5	Question 21 .....	65
5.1.4	Evaluation of Section 3 – Questions 22 To 27.....	66
5.1.4.1	Question 25 .....	66
5.1.4.2	Question 27 .....	67
5.1.5	Evaluation of Section 4 – Questions 28 To 41.....	68
5.1.5.1	Questions 35 and 36.....	68
5.1.5.2	Question 37 .....	69
5.1.5.3	Question 38 .....	70
5.1.5.4	Question 41 .....	71
<b>5.2</b>	<b>Summary and Observations.....</b>	<b>73</b>
5.2.1	Questionnaire Design.....	73
5.2.2	Section 1 of Questionnaire.....	74
5.2.2.1	Competencies and Qualities.....	74
5.2.2.2	Engineering Terms.....	74
5.2.2.3	Safety Critical and Safety Related .....	74
5.2.2.4	Safety Responsibilities.....	74
5.2.2.5	Other Questions Asked .....	74
5.2.3	Section 2 of Questionnaire.....	75
5.2.3.1	Knowledge of Safety Case and the Contents of the Safety Case .....	75
5.2.3.2	The Release To Service.....	75
5.2.3.3	ALARP, Hazards and Accidents.....	75
5.2.4	Section 3 of Questionnaire.....	75
5.2.4.1	Establishing Other Guidance Used in Completing Q6.01a.....	75
5.2.4.2	Hazard Logs .....	76
5.2.4.3	Other Questions Asked .....	76
5.2.5	Section 4 of Questionnaire.....	76
5.2.5.1	Determining the Support Provided by the SSQ Response Form .....	76
5.2.5.2	Inputs to Q6.01a.....	76
5.2.5.3	Outputs of Q6.01a.....	76
5.2.5.4	Final Catch All Question.....	76
<b>5.3</b>	<b>Conclusions .....</b>	<b>77</b>
5.3.1	Strengths and Weaknesses of the Questionnaire.....	77
5.3.1.1	Strengths .....	77
5.3.1.2	Weaknesses .....	78

<b>5.4</b>	<b>Other Observations</b> .....	<b>79</b>
	<b>Chapter 6 – Further Work</b> .....	<b>80</b>
<b>6.1</b>	<b>Provision of a Flow Chart</b> .....	<b>80</b>
6.1.1	Development of a Guidance Flowchart .....	80
6.1.2	Designing the Flowchart.....	80
<b>6.2</b>	<b>Competencies Framework</b> .....	<b>81</b>
<b>6.3</b>	<b>Checklist to Consider the Contents of the Safety Case</b> .....	<b>81</b>
	<b>Abbreviations</b> .....	<b>82</b>
	<b>References</b> .....	<b>83</b>
	<b>Appendix A Questionnaire on Engineering Knowledge of the Safety and Support Questionnaire</b> .....	<b>1</b>

## List of Figures

Figure 1	Overview of Service Modification Procedure.....	2
Figure 2	Military Aviation Safety Case Top Level .....	6
Figure 3	Relationship Between the RTS and SC .....	8
Figure 4	Relationship Between the ADS, RTS and SC .....	9
Figure 5	Role of the Safety Case in Management of Change Showing the SSQ Input.....	15
Figure 6	Example of a Safety and Support Questionnaire.....	17
Figure 7	Part Example of a Response Form Used With SSQ.....	19
Figure 8	The ALARP Principle .....	38
Figure 9	A Generic Graphical Argument Using a Claims-Arguments-Evidence Structuring.....	43

## List of Tables

Table 1	Example of a Hazard Analysis Table .....	36
Table 2	Example of a Risk Classification Table .....	37
Table 3	Example of a Risk Classifications.....	38
Table 4	Questions Answered by Each Respondent.....	54

# Chapter 1 - Introduction

## 1.1 Background

For many years, modifications (refer to Section 2.2.4 for definition of modification) to military aircraft have been carried out using different forms of modification processes. These modification processes have been undertaken using either Design Authority (DA) approved procedures or ‘in-Service’<sup>1</sup> procedures which have been derived and adopted by the three armed services – Royal Navy, Army and Royal Air Force and relevant agencies. Some examples of the types of in-Service modification processes that have been used are; Service Engineered Modifications (SEM) [1], Special Trial Fits (STF) [2], Service Engineered Aircraft Radio Installation Modification (SRIM) [3] and Naval Service Modification (NSM) [4]. These processes have been used in favour of the more formal approach using a DA modification process when an Integrated Project Team (IPT) requires a modification of:

- An urgent, special or short-term nature.
- For trial purposes.
- To address a safety issue.
- To increase capability, improved availability or maintainability and to ease production or overcome obsolescence.

The focus of this project is a Tri-Service single modification process, which replaces the above Service modification processes. In particular it is concerned with the completion of the safety element of a Safety and Support questionnaire (SSQ) [5] (refer to Section 2.5.1 for definition of SSQ). The SSQ is used as a thought provoking tool during the initialisation and design phase of the Service Modification (SM) process (refer to Section 2.2.5 for definition of SM).

## 1.2 Project Aims

The completion of the safety element of the SSQ will be used as the basis of this report from the viewpoint of an aviation engineer (not trained in safety analysis or assurance). The aviation engineer for the purpose of this project is employed by the Army in the Rotary aircraft world. However, engineers from other aviation industries and the military will be considered as part of the review to broaden the understanding. The aviation engineer is required to complete the SSQ as part of the initiation process for an SM. A study into what the safety element of the SSQ means and what information is required to answer the safety element will also be carried out.

A questionnaire will be used to establish what safety analysis and assurance knowledge of those completing the SSQ have in order to set a basis as to what guidance will need to be provided. These aviation engineers need to be familiar with the SM procedure so the questionnaire will be addressed to aviation engineers within the rotary world IPT’s who review the SM processes, Service Modification Teams and Trials teams within the three armed Services who develop the SM’s for both rotary and fast jet aircraft operations and Engineering, Development and Investigation Teams who review SM’s for fleet installations. This will provide a wide range of knowledge, experiences and competencies when gathering data for the questionnaire.

---

<sup>1</sup> The term ‘in-service’ when referring to military aircraft modifications is taken to mean modification activities undertaken or performed by a RN, Army or RAF team, and which can be either all uniformed personnel or a mix of both uniformed and civilian personnel.

### 1.3 Background to Service Modification

Due to the continuing ‘purplisation’<sup>2</sup> of the armed forces to achieve single and aligned operational requirements, a significant change has been brought about to the way that modifications are carried out to military aircraft. The now defunct processes discussed in the paragraphs above have been replaced by a single modification procedure. The single SM procedure that has been adopted is introduced as a policy document in the form of a Joint Air Publication (JAP) known as the JAP 100A-01 ‘Military Aviation Engineering Policy and Regulations’ [5].

The following model shown in Figure 1 [5], describes a simplified overview of the SM process, which will be discussed in later in this report. It shows three conditions when an SM will be used to modify a military aircraft; Safety, Operational and Engineering requirements.

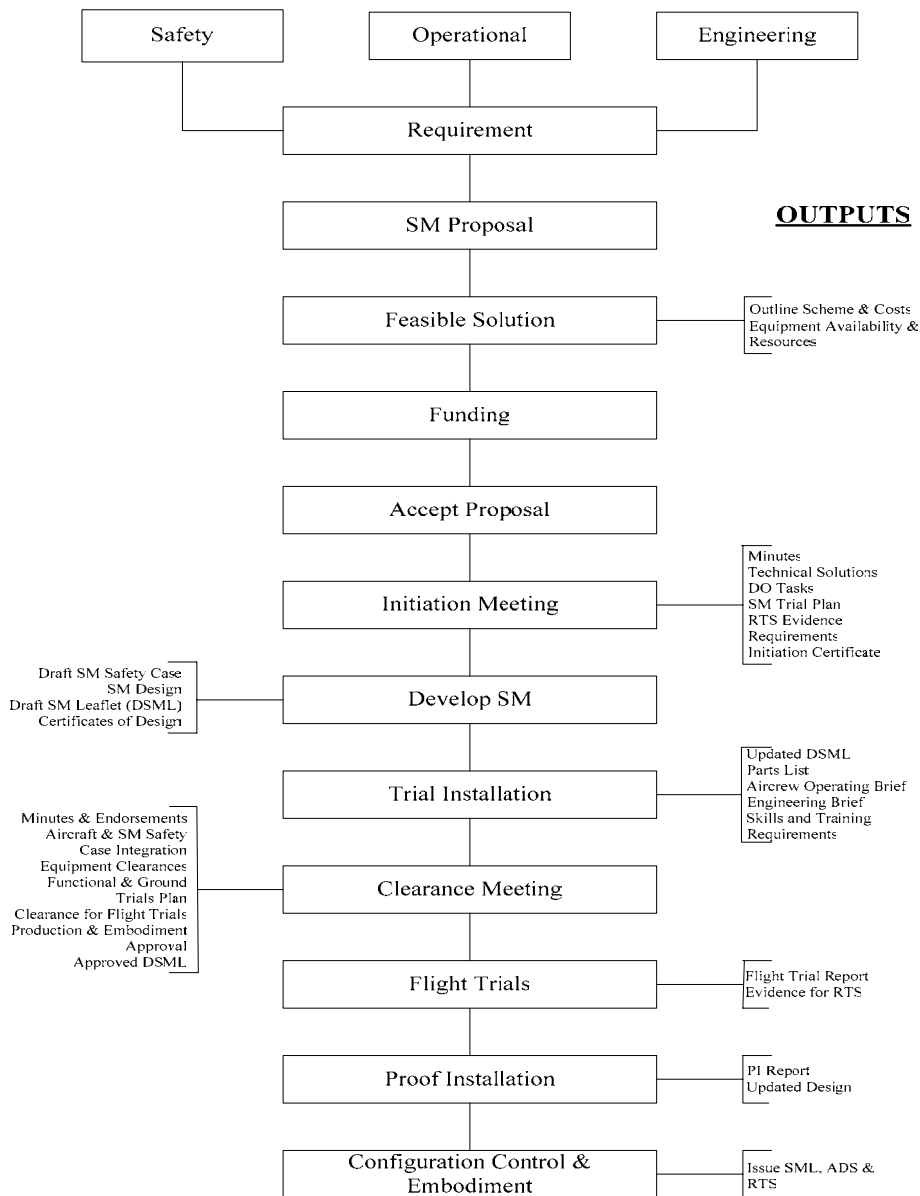


Figure 1. Overview of the Service Modification Procedure [5]

<sup>2</sup> The three arms working together as a Tri-Service organisation

The SM procedure is also used to embody modifications when the Designer Modification (DM) (refer to Section 2.2.2 for definition of DM) procedure will not meet the required timeframe, or where the IPT believes that it is more cost effective to introduce and support the SM. To quote:

*.... 'In the majority of cases, the decision to proceed with an SM in preference to a DM will be as a result of time or cost factors rather than for technical reasons' [5]*

Across all three armed Services, one of the most used applications for an SM is when a modification is required urgently to enhance the fighting capability of an aircraft for Urgent Operational Requirements (UOR). UOR's are normally used when the need for enhanced operational capability of military aircraft has been identified to meet the demands of the war during periods of military conflict. The SM provides the IPT with a flexible system that allows modification of either equipment or aircraft for the reasons above.

The introduction of the JAP and hence the SM draws together the requirements for Airworthiness, Human Factors Interface (HFI), Safety, Safety Case (SC) (refer to Section 3.1.12 for definition of SC) and a Safety Management System (SMS) (refer to Section 3.1.14 for definition of SMS) into a single process. The convergence of documents supports best practice, provides a common framework and supports streamlining. However, as with many converged processes there are benefits and drawbacks to be made when operating with a procedure in this way.

The benefits are:

- The same standard is maintained across the three Services, which are provided in a common architecture.
- It will ensure that all three Services address safety when carrying out aircraft modifications under the SM procedure. In the past this has not always been the case because of the formats of the previous procedures used and airworthiness has been the prime focus rather than safety.
- Using a common vocabulary may allow for portability of safety cases from one platform to another i.e. Mk 7 Lynx to Mk 8 Lynx.
- There is commonality with the use of one format to produce a SM.
- The same auditable process is easily managed by IPT's across all aviation platforms.
- An SM and SSQ produced for an Army Lynx aircraft maybe used with slight adjustment for installing the same piece of equipment to a Naval Lynx aircraft.
- Configuration management of the document is simplified, as there is only one version to update and maintain.

However, the drawbacks to using a single policy document are:

- If the process or procedure is incorrect then all three Services are getting it wrong.
- Using one policy does not encourage new ideas to breed in the three Service environments.
- The policy may not suit the intended environment and therefore may not be used as designed i.e. it is tailored to suit.
- Either the policy is outdated or the technology defined in the policy may not be readily applicable.

- The technologies may not be proven to operate on large-scale systems or in a domain as wide as the domain to which the policy applies. It may also be that the technology may simply be inappropriate for some systems for which the policy requires its use.
- There is resistance to changes in the policy by the user because the user may have to change their practices to be compliant with the new policy – a common problem experienced in both military and civil aviation engineering.

If the purpose of the JAP [5] is to bring the engineering community of the three armed Services to an acceptable level of quality, it is important that the level of quality defined by the JAP is acceptable to the system procurers and users.

## 1.4 Motivation for the Project

The author is employed at a unit whose primary task is to write SM leaflets to fit equipment to rotary aircraft in-support of front line Army operating units whose tasks vary. When the author joined the team, they were in the process of changing over from using the SRIM procedure to the SM process in the JAP and it appeared to the author that there was a lack of knowledge as to some of the requirements of the SM and in particular the SSQ. In addition, this was to be the first Army unit to adopt the procedures and they would set precedence for other Army user units to follow. It also appeared that there was a lack of knowledge in the team towards aircraft safety and in particular SC and SMS. The RAF and Navy use the same SM process but because of the broadness of its use, the source for this project is focused on the Army.

## 1.5 Project Structure

**Chapter 2** – reviews current practice, problems and thinking within the area of aircraft modifications and in particular the use of a Safety and Support Questionnaire used for initiating Service modifications. Particular focus is upon:

- Regulatory requirements for Release To Service (RTS) (refer to Section 2.18 for definition of RTS) of the aircraft.
- The relationships between the RTS, SC and Development lifecycles.
- The meaning of Airworthiness and Safety.
- The concept of the SSQ.
- Practical issues with completing the SSQ – will include guidance.
- The practical issues with using questionnaires and the difference between questionnaires and checklists.
- Competencies required by the engineer to complete the SSQ.
- What procedures are used by other industries to compile safety cases?

**Chapter 3** – defines the elements of the safety question 6.01a in the SSQ and looks at the safety and safety related terms and processes that the aviation engineer may be faced with considering the answers to the question. It also looks at the SC and what are perceived to be its elements/contents and attempts to define what are the minimum elements that should be reviewed if there is a modification change that affects the SC.

**Chapter 4** – describes the process of the case study, which includes the design, and development of a questionnaire to elicit information from aviation engineers regarding their knowledge of safety and safety assurance.

**Chapter 5** – looks at the completed questionnaires from a number of respondents to analyse and summarise the findings so as to formulate a conclusion and generate a possible solution.

**Chapter 6** – puts forward proposals of solutions or recommendations for further work to address the issues raised either by the author or the evaluators during the case study.

# Chapter 2 – Literature Review

## 2.1 Use of Single Modification Processes and Regulatory Requirements

### 2.1.1 Requirements for a Single Policy

*Why a single modification process for all three armed Services?*

Defence Logistic Organisation (DLO) (Strike) Eng Pol Reg introduced the JAP100A-01[5] in December 2001 for use by the three armed Services. It provides a policy framework for the regulation of tri-Service military aviation engineering in the UK Military Air Environment (MAE) [5]. It has been developed using the principles of deregulation and best practice, and with due regard to civilian regulations. It aims to ensure that aircraft-related engineering activities are conducted safely in peacetime and during operational deployments, and that the airworthiness chain of accountability remains intact [5].

The regulations apply to all personnel engaged in the maintenance of aircraft in the MAE. Its scope encompasses all organisations and activities related to engineering and support of military registered aircraft and airborne equipment. The applicability of the JAP to organisations and non-military personnel contracted to carry out maintenance or flying tasks for or on behalf of the MOD, including Civil Owned Military-Registered aircraft (COMAR)[5].

### 2.1.2 The Importance of Aviation Safety to the Ministry Of Defence

In a book written for the MOD by Advantage Technical Consulting (ATC), Principal Author Rhys David entitled ‘An Introduction To System Safety Management & Assurance’ [6], ATC highlight that in the case of the Gulf War and recent other conflicts there have been a significant number of casualties. Many of the casualties were not necessarily caused by enemy action but by accidents. They suggest that safe equipment, working practices and a safe environment are key force protection measures, which must be provided to maintain operational capability. It is normally the Service personnel who are exposed to the majority of safety risks whilst undertaking Service duties so it is important the user (Service personnel) must be involved in safety throughout the lifecycle, from setting appropriate safety requirements through to managing residual risk. They must play a major role in saying what Risk they will be prepared to tolerate for the benefits the new equipment will bring.

Safety and airworthiness is the responsibility of all personnel, who must be aware of the functions for which delegated authority is required. The JAP [5] specifies guidance and regulations in support of the delegation of airworthiness and other functions to be undertaken by personnel, to assure the safety of aircraft operations and the airworthiness of MOD aircraft.

### 2.1.3 Aviation Safety

The scope of aviation safety is described as:[5]

..... *‘every activity that could impact on the ability to deliver safe aviation.*

It includes:

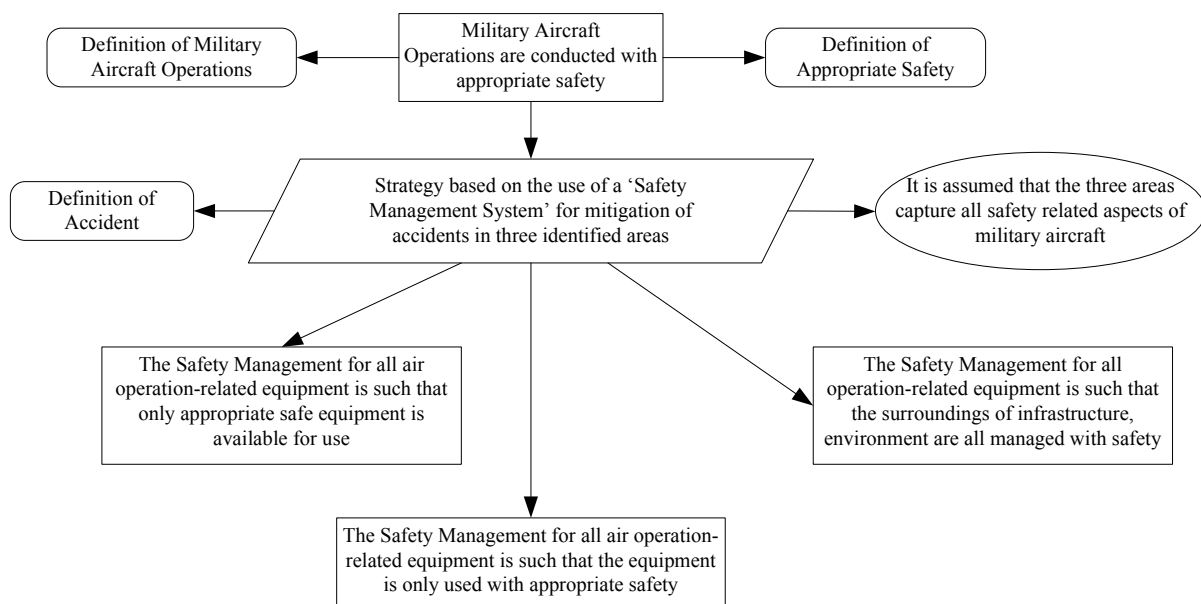
- The design, manufacture, build, maintenance and support of aircraft.
- Operating aircraft.
- Support to aircraft operation including, for example, infrastructure, air traffic management and emergency services.

- The provision of appropriately trained and competent personnel.

Aviation safety is achieved when the operation of aircraft poses no significant risk to aircrew, ground crew, passengers, and other airspace users or to the general public over which such aircraft are flown [5]. The Defence Aviation Safety Board (DASB) endorses this statement.

#### 2.1.4 Military Aviation Safety Case

The purpose of the Military Aviation Safety Case is to scope the extent of aviation safety; this information can then be used to ensure all elements are managed, enable documentation of the SMS and allow target setting and performance monitoring. The following top-level Goal Structuring Notation (GSN) (refer to Section 3.1.15 for definition of GSN) structure demonstrates this:



**Figure 2. Military Aviation Safety Case Top Level**  
(Source Brennan [8])

#### 2.1.5 Flight Safety and Airworthiness Accountability

The operation of military aircraft is carried out under Crown prerogative. The Crown has a legal duty of care, arising from the Health and Safety etc at Work Act (HSWA) [9], to ensure that such operation is safe. The MOD is also subject to a legal duty of care and has a responsibility to ensure its aircraft are operated safely. Authoritative Crown responsibilities for Military Aviation are espoused in Joint Service Procedure (JSP) 553 Military Airworthiness Regulations [10]. Responsibility for airworthiness is vested in the Secretary of State (SofS) for Defence, with authority delegated to competent personnel in the air environment. This is normally delegated to platform IPT Leaders who are responsible for retaining the ownership of the contents of the Generic Aircraft Release Process (GARP) Military Aircraft Release (MAR), RTS and the Aircraft Document Set (ADS). The MAR, RTS and ADS are described in detail later in this project.

To meet the military safety and airworthiness requirements, the SM procedure is a complex and thorough process. It comprises several defined levels of activities which are required to be completed before the modification can be authorised to be flown and used for its intended purpose. The authority that allows the aircraft to fly in its 'as flown' configuration with the introduced modification/modifications is provided by the Release To Service Authority (RTSA) (refer to Section 2.1.9 for definition of RTSA) in the form of a Service Deviation (SD) for Army Lynx and Gazelle as part of the RTS.

## 2.1.6 Joint Service Procedure 553 - Military Airworthiness Regulations

JSP553 [10] (formerly JSP 318B) describes the SMS for the management and regulation of military aircraft airworthiness; it contains mandatory requirements, advice and guidance. These processes provide the mechanism for complying with MOD policy supported by the analysis methodologies detailed in the safety Defence Standard (DS) 00-56 [11]. The JSP is produced and intended for personnel who are concerned with the policy aspects of MOD aircraft, Project Sponsorship, and the preparation of MAR, SD and other Service initiated changes of an operational or engineering nature. The requirements of JSP 553 are interpreted by the Director General Equipment Support Air (DG ES (Air) through Business Procedure (BP) 1201 [12].

## 2.1.7 Military Aircraft Release

Prior to the introduction of the Generic Aircraft Release (GARP)[10] the MAR was the IPT Leader's statement to the relevant Service on behalf of the Chief of Defence Procurement (CDP) or Chief of Defence Logistics (CDL) to the Directorate Equipment Capability (DEC), that an acceptable SC has been prepared for the aircraft and its equipment and a statement of the limitations within which the safety case remains valid. The SC supporting the MAR uses as its baseline; the SC produced by the industrial designer of the aircraft, which is supplemented by all the additional safety evidence commissioned by the IPT. The certification and supporting evidence produced by the industrial designer forms the foundation upon which the safety justifications for Test Flying the MAR and RTS are based. For legacy aircraft, the MAR does not always relate to the 'as flown configuration', but it is key to the SC in particular it represents the datum condition from which the In-Service's SC evolves.

## 2.1.8 Release To Service

The RTS is described in the Acquisition Management System (AMS)<sup>3</sup> [13] as the Service authority for the 'as flown' configurations of an aircraft to be operated under Service flying conditions. It is the release document which gives authority for Service regulated flying. The RTS is derived from the initial Release To Service Recommendation (RTSR) or MAR but includes a safety justification of subsequent changes. The RTS is required to be supported by a SC and this uses as its baseline the SC supporting the MAR with additional documented safety justifications for Service changes to the design or changes to the limitations promulgated in the MAR. These additional safety justifications are authorised by the Service through the issue of a Service Deviation for Director Army Aviation (DAAVn) aircraft.

The RTS for an aircraft that has been modified using a SM is supported by extensive documentation including a SC for the as flown configuration. It will also include for example; certification for the new system/s that have been introduced, airworthiness documentation, F100A, Declaration of Design Performance (DDP), Certificate Of Conformity (COC), SM leaflet and supporting SM documentation, results of any independent testing ground and flight testing.

## 2.1.9 Release To Service Authority

For the Army, the DAAVn provides the RTSA who manage the RTS for Lynx, Gazelle, Islander and Apache aircraft. The RTSA personnel are responsible for managing the RTS of each platform that defines the limitations within which the aircraft is considered to be tolerably safe for service flying. This means the RTSA personnel have a strong influence on the effects of airworthiness. The RTSA also have an effect on the SM process. To briefly explain their remit with regards to the SM process and the SSQ as this is covered later in this project, the RTSA will inform the SM Initiation meeting of what documented evidence is required in support of the SM so that it can be put in the RTS. Following successful trials of the installed SM the RTSA will consider the build standard and associated restrictions or limitations stated in the Aircraft Release and shall decide as appropriate whether the RTS should be amended or not. The RTSA is involved throughout the SM process and will be present at the SM Clearance meeting to advise on the RTS, following

---

<sup>3</sup> Created to offer the Acquisition community a gateway to Acquisition business and process, the AMS pulls together all the strands of acquisition into one web site. Providing top level information on the Acquisition process and hosting specialist web sites, the AMS aims to be a comprehensive information resource. An on-line 'one-stop shop' for policy, instructions, guidance, templates, best practice and user expertise relating to defence equipment acquisition under Smart Procurement.

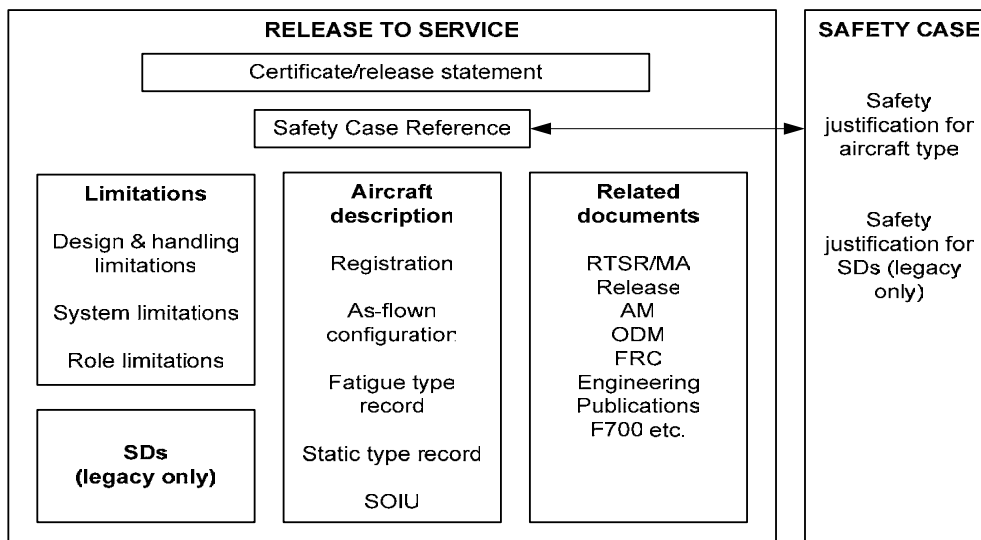
the trials of the installed equipment. The RTS certificate is one of the deliverables for the SM modification process.

### 2.1.10 The ‘As Flown’ Safety Case

The SC for the ‘as flown’ aircraft is built up from the safety cases produced by the Designer, the IPTL and the RTSA. These safety cases are as follows:

- **Designer’s Safety Case.** The Designer’s SC should address the whole aircraft configuration as identified in the Master Record Index (MRI) or other master configuration document and certified in his Certificate of Design (COD).
- **The IPTL’s Safety Case.** The IPTL’s SC is made up of the Designer’s SC for the ‘as built’ standard of aircraft plus the safety justifications used by the IPTL’s to underpin his certification of the initial draft of the RTS or, for legacy platforms the issue of the MAR. The IPTL will have sourced these justifications by the use of competent contractors, standards, independent assessment and safety management. The majority of the justification for the SC will be in the Designers SC that forms part of the evidence for the IPTL SC. It will also be made up of additional evidence which has been provided as the results of independent assessments and safety evidence which has been produced in support of Service originated design changes and will reconcile any differences between the various sources of evidence.
- **The RTSA’s Safety Case.** The RTSA’s SC will initially consist of the IPTL’s SC plus the safety justifications used by the RTSA. These safety justifications will be used to underpin the issue of the RTS and will demonstrate that the aircraft is safe and that all essential requirements are in place to ensure safe operation in Service. The RTSA SC will be made up of the safety justifications which are in the IPTL’s SC. The RTSA SC is an ever evolving SC as the aircraft matures and is changed from it’s as built configuration to meet Service or DA requirements.

The following figure shows the relationship between the RTS and the SC.



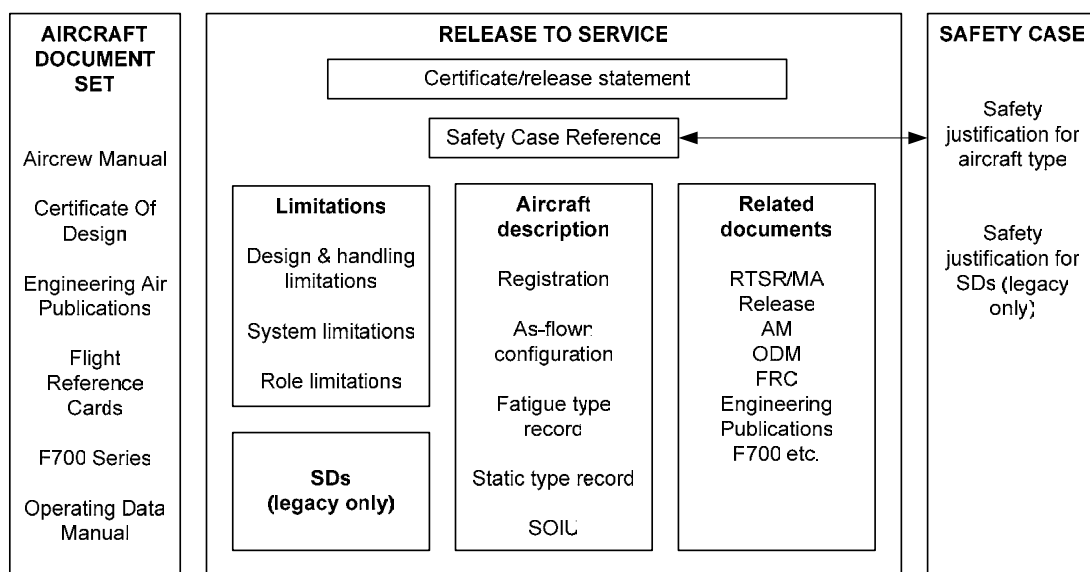
**Figure 3 - Relationship Between the RTS and Safety Case**  
(JSP553 Chap 5 Fig 5.2[10])

### 2.1.11 Aircraft Document Set [10]

The Aircraft Document Set is used in support of the safety case and the RTS and is made up of the following documents:

- Aircrew Manual
- Certificate of Design (COD)
- Engineering Air Publications
- Flight Reference cards
- F700
- Operating Data Manual

The ADS documentation is owned by the relevant platform/equipment IPT leader and provides the supporting documentation to enable maintenance and aircraft flight operations. The relationship of the ADS to the RTS and SC is provided in Figure 4 below.



**Figure 4. Relationship Between the ADS, RTS and SC**  
(Based on Vaughn [7] and JSP 553 [10])

## 2.2 Reasons for Modification

There are three conditions/reasons when a SM will be used in place of DM (previously DA modification) which are; Engineering, Safety and Operational requirements and are applicable to all military aircraft. Much of the requirements for modification within the military is for enhancement to extend capability and is often a requirement of military conflict. Modifications are also used to improve availability and maintainability of the aircraft. Improving availability will also be required to increase the longevity of the aircraft to overcome obsolescence. The introduction of new and advanced technologies and more complex systems and hence complex aircraft make modification very difficult to manage especially when considering the SC. With so many systems dependant on others, the analysis and identification of what effects or impact on the SC the addition of a new system has, becomes extremely difficult. This is made even more difficult when the system SC has been decomposed into subsystem SC's which is normally carried out to manage the complexity of the SC construction. Kelly [14] notes that there are many examples of these conditions in current safety-critical systems.

When systems are modified and or maintained, many accidents occur. Systems continue to evolve to meet progression in technology or users requirements and demands. Operators and management change procedures to adapt to these requirements or simply to improve their own culture towards understanding the required processes. New equipment may be added to existing systems as in the case of the SM procedure

and repairs and replacements are carried out. Changes that affect the design of the system must be re-analysed for their impact on the safety of the system. However, it is not only the design of the system that has to be considered but that change to an already approved system. When re-analysis is carried out, it is essential for the system documentation to be updated with the design rationale that supports the changes. This will help to preserve the system safety sought in the initial system design.

### 2.2.1 Advantages and Disadvantages of Using a Designer Modification.

There are advantages and disadvantages of using a DM instead of a SM and vice-versa, these are explained thus.

A benefit of using the DM to modify an aircraft is that the DA will provide a complete airworthiness and safety package towards certification, which will have been completed using in-house specialists. This therefore places the responsibility for safety assurance processes firmly within the DA. Westland Helicopters (Lynx) and Britten Norman (Islander) are DA's for example who will provide this package for the respective platform. However, it will be the case that as the designer the DA cannot provide certification and this will be undertaken by an independent agency such as QinetiQ. Another advantage of the DA completing a DM on a platform is that it means that many responsibilities and requirements of the modification process are transferred to the DA rather than being provided by the Service (in this case the Army). From a legal point of view it alleviates the Service from having to adopt any legal rights towards the design.

The down side to using a DM is one of time and cost. Invariably to avoid any subsequent operational loss of the aircraft from military duty, the military require that any modification to their aircraft is carried out efficiently and expediently and in many cases against constrained and short time-scales. Unfortunately DM's have a tendency to take a significant amount of time and effort and at times can incur costs to the Defence purse.

Although in the past the tendency has been for DA's to perform large and complex modifications to military aircraft using their own DM processes it is not unusual today to find DA's or Design Organisations (DO) as they are now known, carrying out modifications to military aircraft using the SM process. This has come about due to the policy change within JAP and how modifications are carried out to military aircraft. IPT's are now free to choose a DO from almost any aviation domain as long as the IPT has confidence that the proposed DO has the competency and ability to undertake the intended scope of work. If the selected DO is not listed in the Design Approved Organizations Scheme (DAOS), the IPT is to have an assurance mechanism in place to evaluate and monitor the competency of its selected DO in accordance with regulatory requirements in JSP 553.

### 2.2.2 Design Organisation

The term Design Organisation (DO) which has replaced the term 'Design Authority' is defined as:

‘ an organisation appointed by the contract to be responsible for a design or modification of a design’.

This has been brought about to reflect that whilst the contracted organisation is responsible for the design and for signing the Certificate of Design, the authority for acceptance of a design and any change to that design is vested in the IPTL. The competency requirement of these DO's has been discussed previously.

### 2.2.3 Advantages and Disadvantages of Using a Service Modification

Although the SM process is aimed at the Tri-Service domain these comments are based on the authors experiences within the Army aviation world. The SM is normally produced by a DO within the Army aviation engineering domain as required by the relevant platform IPT - the Service Modification Section produce several SM's for Army aviation. However, as already mentioned it is not unusual now for an industry DO to be contracted to produce a SM under the terms of the JAP and DS 05-123 [15] (explained

later). We will concentrate on the advantages of the Service producing the SM against an industry DO as much of the benefits of using an industry DO for DM's is appropriate to the production of SM's.

The aim of the SM is for the Service to complete the modification process using its own resources and in-house departments. On the whole much of this is achieved, but there are certain areas where the Service is still dependant on outside agencies, particularly those agencies with specialist qualities that can provide advice on airworthiness and safety assurance matters. As already mentioned, time is a factor which does not favour the industry DO but within the Service the SM modification process is one process which allows modifications to be introduced quicker. Much of the requirement for SM's is for UOR's and this generally involves a fleet fit in quick succession and against short timescales. The Service system allows for more than one modification to be embodied at any one time. On many occasions the operational upgrade package may consist of several Service modifications to the platform to meet the requirements of the theatre in which the Service is involved. Using in-Service resources not only speeds up the modification process, but in most cases reduces cost and as already discussed is a significant factor in the choice of SM over DM.

However, it must not be forgotten that the modification will still need airworthiness and safety assurance certification for the RTS and although there are departments within the Service to supply some advice and analysis, the trend within the Army rotorcraft IPT's is to source this advice from independent agencies such as the DA for the platform or other agencies. These other agencies for example are Advantage Technical Consultancy, Praxis High Integrity Systems (Praxis HIS) and QinetiQ.

#### 2.2.4 Modification

As this report is focused upon a SSQ for a Service modification process and 'modification has been discussed consistently so far throughout this report, it is pertinent at this point to describe what is meant by the meaning of modification in the context of this project.

The term 'Modification' is defined in DS 05-123 [15] as:

'a design change to equipment, after the design has been brought under direct Ministry control (DMC) and fulfils certain criteria'

"...when ...a change to the design records... affects one or more of the following:

- Safety, operational use, reliability, maintainability or other specific MOD requirement.
- Production or which may involve retrospective embodiment.
- Cost or delivery programmes of the item or its Service spares.
- Interchangeability of the item or its Service spare."

For each new build of aircraft there will be a set of design records, which set the base line standard for each aircraft. The change to the design records would normally be affected by the introduction of some form of modification, whether it is introduced by a DA/DM or it is required as a service requirement. Modification action may necessitate the re-issue or amendment of the Certificate of Design (COD) and, where appropriate, the Certificate for Flight Trials (CFT) and Aircraft Release.

Modification is also defined as:

'..the alteration of an aircraft/aeronautical product in conformity with an approved standard'

This definition comes from the Federal Aviation Authority (FAA) Civil Aviation Regulations Part 5 [16] and is saying that a modification alters an aircraft or aeronautical product when carried out using an approved standard. In the case of the SM it would be the JAP 100A-01. Although the JAP is not a standard in its own right but a procedural document that directs and guides the user through the SM process, Defence Standards 05-123 and 00-56, JSP 970 and JSP553, support the JAP.

### 2.2.5 Service Modification

The term 'Service modification (SM)'<sup>4</sup> is described as:

'A modification to an aircraft or equipment designed, developed, produced and embodied by, or for, the Service. The IPT retains responsibility for the modification until such time as it is superseded by a cover modification'.

At the behest of the appropriate IPTL, the SM can be produced by:

- Service resources.
- Contractors
- Any other recognised and approved engineering agency.

IPTL's will normally seek advice from the DO on a SM proposal, especially when it could:

- Interfere with any design change already in hand or being considered.
- Require safety or specialist testing.
- Require significant re-design if a cover modification is being considered.
- Require cost estimates for changes to design records.
- Require an assessment on its compatibility with other aircraft systems or equipment.

### 2.2.6 Cover Modifications

It is the intention that SM's are used for short-term applications or limited applicability limitations. However, should there be a requirement to retain the modification past its short-term life and make it a permanent fit; there is a mechanism that caters for this in the form of a Designer cover modification. The Designer cover modification incorporates much of the details of the SM as long as the SM satisfies the design standards that the Designer is contracted to maintain. If it does, the Designer may adopt the SM design and produce a cover modification which 'is satisfied by' the SM. However, if the SM design does not meet the Designer standards, the Designer will redesign the modification. This has other implications in that by redesigning the modification, the IPT may have to pick up the bill for the redesign. Although the Designer adopts the SM design they do not however adopt responsibility airworthiness responsibility for the design, this will remain with the appropriate platform/Service body.

## 2.3 **Past Procedures Used To Modify Military Aircraft**

As briefly mentioned, modifications to military aircraft have in the past been carried out using different modification procedures. This next sub-section briefly looks at the two most common procedures that were used by the Army and how they were used, how they compare against the SM procedure and any problems that are associated to these modifications and the SM process.

---

<sup>4</sup> The definitions are for words, or technical vocabulary, specific to military air environment use. Where a word appears in the Oxford English Dictionary (OED), the definition is specific only to the associated context and OED definitions should be used in all other usages.

### 2.3.1 Service Engineered Aircraft Radio Installation Modification

The SRIM is a well-tried and tested procedure within the Army much like the SEM and NSM procedures, which are used by the RAF and Navy respectively, and its implementation has been well used. The SRIM would have been used to carry out modifications to; Communications equipment, Navigation equipment, Radar equipment, Electro-optical equipment and Electronic Warfare equipment or its associated system. However, the SRIM procedure does not have an SSQ but does address safety in its procedure. Safety assessment is addressed at two points within the SRIM process: Initiation of the proposal and the second, which is at the Clearance meeting. The Clearance meeting is held post the Trial Installation (TI) and is the next stage towards aircraft release following a Proof Installation (PI) and completion of the ADS.

For both Initiation and Clearance phases, safety and airworthiness issues are dealt with as an agenda item where consideration is made towards weight and balance of the aircraft, EMC safety, weapon systems safety and flight safety critical systems. During the Clearance phase, DM clearance of the modification is addressed; EMC safety test results and EED test results are produced. As Graham [17] identifies, these tasks are normally dealt with by other MOD or industry agencies, however, there was no detail on the methods to be adopted in attaining these test results and clearances. This is discussed in Chapter 3 of this report and in particular reference is made to further comments made by Graham [17] on this subject detailed in his Thesis. The JAP SM procedure attempts to embrace many of the activities in the SRIM.

### 2.3.2 The Service Engineered Modification

*Extract from Graham Thesis [17]*

*.....The initial safety analysis on a SEM is completed by a safety questionnaire during the feasibility assessment of the modification. This does leave the PHA process open to potential gaps in the safety analysis, as can be frequently experienced through the use of questionnaires. However, the safety questionnaire in use is thorough and has been adopted for use during the PHA of many projects, hence lending confidence to its completeness. Despite this, further safety expertise is called for by [AP 100B-04] to fully assess the proposal during the SSA phase. In addition the advice of the relevant DA is also called for, to allow them to raise comments and voice concerns, which they may have over the safety and airworthiness affects that the proposed SEM may hold for the legacy system.*

The SEM used a similar safety questionnaire (SQ) [1] as the SM-SSQ and was similarly populated by the unit compiling the SEM procedure for the modification. Graham [17] suggests that the SEM SQ was not overly complicated and could be completed by the average aircraft engineer. This is true for the SEM SQ and the same may be argued for the SM SSQ, however, unlike the SEM where the originating unit raised the SQ, any Design Organisation can be tasked by the IPT to complete the SSQ on it's behalf and subsequently also be tasked to conduct a detailed risk assessment of the SM proposal and appropriate SSQ items during the progression phase. They may also be required to develop and produce the SM Safety Case. Graham identified concerns regarding what levels and standards of knowledge and competencies the engineers had who were required to populate the SEM SQ. However, although this was an issue with the SM, Graham rightly identifies that the SEM SQ would be reviewed during the SSA phase as called for by AP100B-04.

## 2.4 **The Safety Case and Management of Change**

The beginning of Chapter 2 looked at the RTS stage for in-Service military aircraft which was the final part of the overall modification process and which allows the aircraft to fly in the 'as flown' configuration. However, before we can get to the RTS stage the aircraft must first be modified following a prescribed number of activities. Modifying an in-Service aircraft for one of the reasons previously mentioned causes changes within the overall airworthiness and safety of the aircraft. Remembering the three conditions when a SM may be used; Engineering, Operational and Safety, any SM raised to accommodate one of these requirements will incur a requirement to review the SC and the RTS.

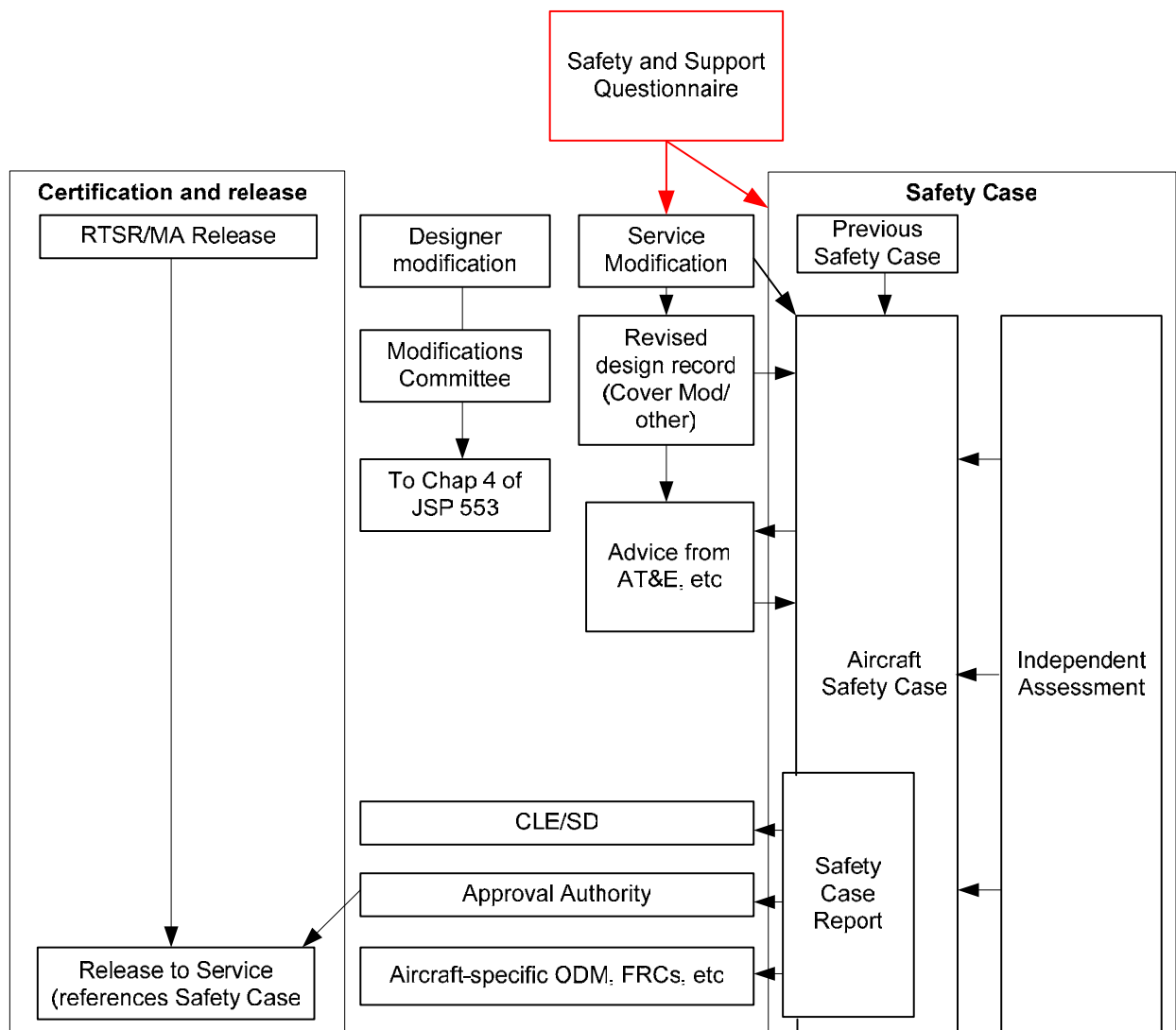
### 2.4.1 Safety Case Change Management

The management of change in particular to the SC is a requirement of the in-Service Safety Management System (SMS). In-Service changes to either hardware or software may affect the safety case (SC) and alter the limitations or restrictions that are defined in the current release documents for the platform. Following SM action it may also be possible that there will be some procedural changes which some may affect or change flying or operating techniques and limitations. The introduction of an SM may also affect the SC and release documents. The relevant airworthiness component is 'management of change', which is implemented through:

- The RTS, which as discussed permits Service regulated flying following changes.
- Emergency clearances, which permit accelerated changes during times of emergency.
- Implementation of changes.

Although not the direct focus for this project, it is worthy of mention and the author also feels that management of change is a very important aspect of safety management. There is the possibility for confusion when a change is implemented to an existing system; operational requirement; maintenance process, and/or procedure. This increases the risk to the SC and the risk must be identified early so that it can be addressed and any change managed in co-operation with the affected work areas. Kelly and McDermid [18] recognise that change management is a problem within SC maintenance. They identify that that the initial impact of a change is only the starting point of the change management process. As they state, safety arguments are a web of dependencies and it is necessary to identify the 'knock on' effect of changes. The more complex the safety case is, the more dependencies there are likely to be. In complex aircraft systems with complex safety critical systems, the SC will have many dependencies. It is suggested that it is important for engineers to see the structure of the argument and where the dependencies lie so as to identify the 'knock on' effect of changes (source [18]). This is made all the more difficult in poorly presented safety arguments especially those SC that are in text based safety arguments and where the dependencies are inadequately presented.

Figure 5 shows the role of the SC in management of change and how it is linked to the aircraft's development, modification and Service release. It shows the relationship between two forms of modification process, Designer Modification (DM) and SM to the safety case and how the outputs from the SC are fed into the RTS. This figure also shows where, in the process the SSQ inputs into the overall SM and SC process.



**Figure 5. Role of the Safety Case in Management of Change Showing the SSQ Input**  
(Based on JSP553 Chap 5 Fig 5.1 [10])

## 2.5 Safety and Support Questionnaire

### 2.5.1 The Safety and Support Questionnaire

One of the activities of the SM process is to produce a technical installation leaflet which is the main document used as an instruction document for modifying the platform with the new system. However, before the draft SM leaflet (DSML) can be produced, there are several other activities which must be completed, and one of these activities is the production of a Safety and Support Questionnaire (SSQ). This is described in the next paragraphs.

One very important engineering requirement of the JAP is that **every** SM is to be supported by its own **Safety Case**, which is to be assessed against, and integrated into, the whole aircraft SC. In addition, one of the fundamental requirements of the SM process is the completion of the SSQ. The SSQ is used during the proposal phase to identify safety and business risks during the early stages of the SM process. Subsequently, the completed SSQ is used to assist in the compilation of the SM safety case. The SM SC is used to assess the effect of the SM on the whole aircraft SC. However, the SSQ is a living document and can be reviewed and updated at any time during the SM process.

For a DM, an initiation process like the SSQ to start the modification process may be used. It is not unusual for industry to use thought provoking in-house questionnaires/checklists similar to the one shown in Figure 6 and in some industrial companies who are contracted to write SM's rather than DM's the SSQ method has been adopted. Companies such as Westland Helicopters and QinetiQ when contracted by MOD to provide an aircraft modification under SM conditions are required to complete the SSQ as part of the overall SM process. Previous to this and when assessing SRIM and SEM proposals from an airworthiness requirement for the Army, Westland Helicopters produced and used their own version of a questionnaire that was not unlike the safety questionnaire within the SEM and SM.

The SSQ is normally populated by the Design Organisation (DO) who is chosen by the Integrated Project Team Leader (IPTL) placing the task. The DO does not necessarily need to hold Design Approved Organisations Scheme (DAOS) [15] accreditation but must be able to satisfy the IPT that it can carry out the requirements of the SM process as described in the JAP. DAOS provides the IPTL's with assurance of a contractor's suitability to undertake a defined scope of activity. AD/ADRP will approve contractors for inclusion in the scheme, following an assessment that will normally involve IPT's. AD/ADRP maintains a register of DAOS approved contractors and provides advice on the DAOS assessment.

The SSQ is a questionnaire that is made up of several categories of airworthiness and support questions, which are shown grouped together by category in the coloured boxes on the example provided in Figure 6. Each question is required to be answered by the DO during the initiation and design phase of the SM. However, the SSQ is a living document and should evolve over the SM life cycle. Since it records the top level argument for the airworthiness, safety and support of the proposed system, the basic structure should remain broadly similar over time, but the status of the evidence will change.



- Test Equipment and Training (Turquoise).

The category that is the focus for this project is the Safety Case activity within the Airworthiness and Flight Safety category in the red box. Taking this box we can regroup the Airworthiness and Flight Safety elements into further sub-categories as follows:

- **Flight Safety**
  - Aircrew health
  - Aircrew safety and operating procedures
  - Handling, performance and operations
  - Human Machine Interface
  - Safety Case
- **Airworthiness**
  - Certificates of Design.
  - Compatibility.
  - Environmental Control System
  - Heat treatment.
  - Interchangeability.
  - Material specification.
  - Operating Data Manual.
  - Performance and reliability.
  - Release to Service.
  - Safety Case.
  - Statement of Operational Intent and Usage.
  - Structural Integrity.
  - Structural classification.
  - Weight and Moment.

### 2.5.2 Safety and Support Questionnaire Response Form

It can be seen that much of the questionnaire in Figure 6 is directed toward airworthiness and support issues, and only briefly mentions safety. The area where it questions safety is in question 6.01a, which asks:

- Does the design have an effect on the Safety Case?
- Does the proposed design have an effect on Aircrew safety and operating procedures?

This project only looks at the SC activity of the above observations. It can be seen from the SSQ; each question is supplied with a 'yes/no' answer and does not lend its self to any justification as to why the answer is 'yes' or 'no'. However, the form is supported by a set of guidelines for each question to assist the person in completing the form. The next figure is an example of the guiding words provided in the 'Response' support form [5].

## RESPONSE FORM TO (SSQ)

**Box 6:** Select “Yes” or “No” for each subject. A statement should be made for each subject and supporting information is to be supplied to the IPT such as: test results, reports, certification, proofs, requirements, approvals, data, records, procedures, methods, minutes and conditions.

<p><b>Box 6.01:</b> Statements are to be provided with regard to airworthiness and flight safety.</p> <p><b>Box 6.01a:</b> State the effects on the Safety Case, the required changes and associated actions.</p>	<p>← Area of Project Interest</p>
<p><b>Box 6.01b:</b> State the effects on the Statement of Operational Intent and Usage (SOIU). If the SOIU is affected it is to be updated in accordance with JAP100A-01.</p>	
<p><b>Box 6.01c:</b> State the effects on the Operating Data Manual.</p>	
<p><b>Box 6.01d:</b> With the assistance of the Release to Service (RTS) Authority, state the effects on the RTS.</p>	
<p><b>Box 6.01e:</b> State if Certificates of Design are required.</p>	
<p><b>Box 6.01f:</b> State how the Structural Integrity (SI) is affected. If the effect either directly or indirectly alters the static strength, fatigue life or corrosion resistance of the primary structure then the IPT is to refer findings to an appropriate SI working group for specialist advice.</p>	
<p><b>Box 6.01g:</b> State the classification, reference numbers and nomenclature of the structure to which the modified equipment will be attached or the modification work will alter.</p>	
<p><b>Box 6.01h:</b> State the material specifications, reference numbers, standard wire gauge and nomenclature of the modification structural parts, except where these are given in the drawings provided.</p>	
<p><b>Box 6.01i:</b> State the heat treatments required during manufacture including a list of relevant publications and/or British Standards Institution leaflets. If heat treatment is not required, a statement can include “may be cold worked.”</p>	
<p><b>Box 6.01j:</b> State the effects on the Environment Control System.</p>	
<p><b>Box 6.01k:</b> State the effects on aircrew safety and operating procedures including changes of:</p> <ol style="list-style-type: none"> <li>1. Primary displays, equipment interfaces, aircraft assisted escape systems, ejection seat profiles, crew access or movements.</li> <li>2. Normal or emergency operating procedures.</li> <li>3. Maintenance schedules, test programmes, check lists or change of role procedures or other documentation.</li> <li>4. Operational flight software.</li> <li>5. Special Instructions - Technical (SI (T)).</li> </ol>	

**Figure 7. Part Example of a Response Form Used With SSQ**  
(Based on JAP100A-01 Chap 10.4 [5])

Many DO's across the three Services have tailored this form to be able to answer each question appropriately along side each question. There are slight variations in format of how the form is presented. The example, which is only part of the Response form, shown in Figure 7, is taken from the format used by the Service Modification Section (SMS) based at Forward Support Rotary Wing (FSRW).

Examining the SSQ closer, the area of interest for this project is question 6.01a under the heading of Airworthiness and Flight Safety and it asks:

***'Is there an effect on the Safety Case?'***

This question in itself is not very definitive and does not clarify whether the SC in question applies to the Platform SC or whether it is referring to the SC that is produced for the system being introduced under the SM. For the purpose of this project it will be taken as the Platform SC.

In his Thesis, Graham [17] discussed the service modification process for legacy aircraft using the now defunct SEM process. He made observations regarding the completion of questionnaires for the SEM that are also applicable to SM's and the following extract details this:

Extract from Graham Thesis [17]

*'When examining the use of a safety questionnaire, there is instantly a concern raised over this approach to assuring safety. The Achilles heel of a questionnaire-based approach is always how thorough its contents may be and as a result, what areas of safety analysis may be overlooked during the modification process. Although the safety questionnaire used in SEMs is completed at an initial stage, its completion is necessary to highlight potential safety issues during the proposal phase. It is also completed by non-safety experts and, although the personnel completion the questionnaire will have significant type related and general engineering or operational experience, their training will not be directly related to safety analysis and assurance.'*

Much of what Graham states in the extract above is relevant to a SEM, however, much of his rationale is also appropriate to the SSQ. The JAP uses the SSQ as a questionnaire to invoke thought processes as to whether the proposed system under design may cause an effect on the aircraft platform SC or other airworthiness issues. How this is achieved in relation to the SM process defined in Figure 1 will be the focus of discussion later in this project. There is some question as to the apparent level of knowledge and competency of those required to populate the SSQ and this is possibly due to as Graham identifies, the fact that they are not trained in safety analysis and assurance. This observation will be further evaluated as part of Chapter 5 to assess what the level of knowledge is.

### 2.5.3 Completing The Safety and Support Questionnaire

Based on the author's knowledge and experiences, many of the DO's who are designated by the IPT to complete the SSQ, and more so the risk analysis and SC activities do not have the appropriate skill level and competencies to accurately complete the documentation. There also appears to be a lack of understanding by those populating the SSQ as to exactly what they are being asked.

In the military rotary world, it is practice for the SMS team to compliment the SSQ with the response form (above) to justify the answers given in the SSQ, using the guidance words supplied. A statement should be made for each subject and supporting information is to be supplied to the IPT such as: test results, reports, certification, proofs, requirements, approvals, data, records, procedures, methods, minutes and conditions. These are put forward as a package to the Aircraft Safety Case manager along with the SSQ and Amplification of Proposal (AOP), to assist in making an assessment of the effects caused by the proposed system on the ASC. It is the author's experience that in most proposals for a SM design, the answer to the question as to whether the proposed design affects the SC is always 'yes'. The answer is completed thus because the person populating the SSQ has a lack of safety knowledge and it is answered in this way as a precautionary measure to ensure that the ASC is reviewed by an expert.

Box 6.01a on the Response form provides the guiding words for the comments on the SC statement required on the SSQ and are as follows:

‘State the effects on the Safety Case, the required changes and associated actions’.

Normally this box is completed by the DO when the SM is in the proposal phase and before the Initiation meeting, and much of the design work has still to be carried out and it is the norm for the answer to be something like:

*‘With the proposed system fitted to the aircraft, the existing Aircraft Safety Case (ASC) will be invalidated. Consultation will be required between the relevant IPT and the ASC manager to agree an amendment to the ASC to include the new system/s’*

This form of answer does not exactly answer what is being asked by the question but merely makes a statement that the relevant IPT and ASC manager are required to look at the platform SC and pass judgment that it is to be amended. It does suggest that the ASC will be invalidated by the introduction of the new system but does not state why? This type of answer is not uncommon when SSQ’s are completed and as suggested above, is done as a precautionary measure. One reason for this, is that in most cases although the aviation engineer may be suitably skilled and experienced regarding the platform they are modifying, but will probably not be familiar with safety analysis and assurance techniques. This is reiterated by Graham [17] who states the same reasoning applies to SEM documents. To quote; ‘*It is also completed by non-safety experts and, although the personnel completing the questionnaire will have significant type related and general engineering or operational experience, their training will not be directly related to safety analysis and assurance’*.

The implications of this are that there is a risk of the SSQ not being completed thoroughly and completely. Answers provided may be misleading or inaccurate and safety critical components may have been overlooked and any mitigation to reduce Risk has not been put in place. This will in turn reduce the effectiveness of the SC argument and may at the worst lead to an unsupportable SC.

From a top level perspective, most SM proposals will have some effect on the SC and it would not be unreasonable for the engineer to attempt some PHA/PHI here. It would however, be unreasonable though to expect an untrained (in safety techniques) engineer to go any further than this without appropriate training and guidance especially to identify the associated actions. The guidance on providing the appropriate answers to Q6.01a are not clear in the SM procedure and the aviation engineer is not directed on how to find these answers. This is where this project is intended to help.

#### 2.5.4 Knowledge and Competencies for the Safety and Support Questionnaire

The policy in the Army SM teams is for the aviation engineers to be the project manager of their own tasks. This means that they may be required not only to populate the SSQ but also to compile the Draft Service Modification Leaflet (DSML) and coordinate the installation both to Trial Installation (TI) and Proof Installation (PI) levels. They will also be required to produce the supporting documentation for the aircraft documentation set (ADS). As already discussed, it is the author’s experience that at the basic engineering level where SSQ’s are populated there is a lack of knowledge as to what constitutes the components of airworthiness, safety, support and human factors interface. This in itself runs the risk of the SSQ being incorrectly compiled or questions not answered or completed fully.

Brennan in ref [8] identifies that many safety posts within the IPT are project posts, which are supported by MOD policy and DPMT training. However, it can be argued that the inadequacy of training and corporate direction does not ensure provision of an appropriate knowledge for these posts operating through a safety case; rather it focuses on the requirement and methodology for a safety case. However, to overcome these shortfalls, the MOD will employ a contractor to produce both an SMS and SC for their platform.

Within the aviation world across the three Services, DO teams can be made up of a variety of aircraft engineers with varying skill sets and aircraft backgrounds in rotary or fixed wing aircraft or both? These engineers will be; avionics, electrical, mechanical, airframe, propulsion and weapon engineers with varying

levels of competencies and degrees of experience. JSP533 requires that competent personnel are employed in posts with responsibilities for airworthiness; this includes safety [10]. To that end and in order for MOD to be able to fully discharge their legal duty of care, ADRP developed an Airworthiness Competencies Set (ACS) [19].

#### 2.5.4.1 The Airworthiness Competencies Set

The ACS [19] was developed to provide a disciplined, consistent and auditable approach to the assessment and recording of competence. The ACS is based on the IEE competency model, which is becoming increasingly popular as an industry standard. The ACS is intended for the DPA and DLO air sector IPT's, RTSA's, and those areas within the Department that provide airworthiness advice, support or regulation, down to headquarters staff of the Front Line Commands (FLC). It is however, not specifically aimed at SM teams who are compiling or reviewing SM's and SSQ's. The ACS does not introduce new competency requirements but provides a disciplined, consistent and auditable methodology for assessment using the main existing airworthiness competency requirements. However, it would not be unreasonable to take elements of the ACS and use as an assessment tool for those in the SMS teams. This will be reviewed in the evaluation phase.

The ACS is used for selecting the competencies that best describe the scope of the proposed delegation and completing the context section at the start of each function containing relevant competencies. The applicant then conducts the self-assessment and then carries out a self-assessment against the selected competencies.

#### 2.5.4.2 The Institution of Electrical Engineers Competency Guidelines [20]

The Institution of Electrical Engineers (IEE) has produced a set of guidelines to help organisations assess and record the competencies of personnel working on all aspects of safety related systems. This guidance is primarily for safety-related system practitioners working in the field of safety-related Electrical, Electronic and Programmable Electronic Systems (E/E/PES). The guidelines are made up of a set of competency statements and guidance on an assessment procedure. The IEE [20] states that competence in safety-related tasks requires all personnel involved having qualifications, experience and qualities appropriate to their duties. They suggest that for these personnel, the attributes include training, knowledge of hazards and failures, understanding of working practices, communication skills and an appreciation of personal limitations. The IEE have identified four specific types of competencies which are [20]:

- **Technical Skills** For example, hazard analysis and report writing.
- **Behavioural Skills** For example, a personal integrity, interpersonal skills, problem solving and attention to detail.
- **Underpinning Knowledge** For example, a person performing hazard identification must have knowledge of the particular application to be able to identify the likely hazards that exist.
- **Underpinning Understanding** For example, it is unlikely that somebody could establish risk tolerability levels for a particular problem without an understanding of the principles of safety and risk.

The competency scheme described in the guidelines is based on a set of twelve functions that the organisation must execute to support the specification, development, procurement, operation and maintenance of safety-related E/E/PE systems. Much like the ACS, the IEE Competency guidelines are not specific to the completion of Q6.01a. However, like the ACS, it would not be unreasonable to take elements of the IEE Competency guidelines and use as an assessment tool for those in the SMS teams. This will be reviewed in the evaluation phase.

### 2.5.4.3 Summary of Knowledge and Competencies for the SSQ

There are several SM's being produced for Rotorcraft and Fixed Wing aircraft. The requirement and who is responsible to produce a SC for the SM design always creates much discussion at the Initiation meeting. On the whole it is the IPT representative who will decide as to who will compile it. The norm is for the IPT to contract out to a specialist organisation that can provide the relevant safety case. This is because the DO aviation engineer who is producing the SM design is normally not competent to carry out this safety element requirement of the SM process. However, it is possible that by using the ACS and the IEE Competency Guidelines, a specific competency framework can be derived for the aviation engineer that would furnish him with the appropriate competencies and knowledge of how to produce a SC so as to address the safety case issue. This will be evaluated during the evaluation phase of this project.

## 2.6 Identify With Forms of Check Listing and Questionnaires

### 2.6.1 What is a Questionnaire?

The SM uses a questionnaire (the SSQ) as a thought provoking tool in the early stages of the SM process to make IPT project leaders aware of airworthiness and safety issues that are affected by the SM. So, what is a questionnaire? The Concise Oxford English Dictionary (COED) [21] defines a questionnaire as:

*'a set of printed questions usually with a choice of answers, devised for a survey or statistical study'.*

The definition implies that the type of questions asked by the SSQ falls into the category 'devised for a survey'. A Survey is used to examine, investigate or assess what potentially starts out as an unknown quantity. The SSQ questions are thought provoking and encourage the reader to consider the effects that the proposed design may have on other elements of the design process, the aircraft and its armaments and airworthy and safety issues. However, the SSQ requires just a yes or no answer to answer each question. In most cases this is pretty meaningless unless some substantial evidence as to why it is yes/no is provided. This is also heavily reliant on those persons completing the responses accurately and thoroughly. In some senses the SSQ is a form of check listing where the person completing it is required to follow a prescribed process. However, it could also be argued that the questionnaire is requesting statistical evidence for some of the answers especially those that request information regarding weight and balance. The author therefore feels the SSQ takes the form of both statements given in the definition of a questionnaire above.

The FAA [22] describes questionnaires as a series of questions designed to elicit specific information from their readers (participants). Some questionnaires require yes/no answers; others ask for a choice from a set of pre-supplied answers and others ask for a longer response or comment. Well-designed questionnaires are good at getting answers to specific questions from a large group of people, and especially if that group of people is spread across a wide geographical area, making it infeasible to visit them all.

Whilst searching around for information on the use of questionnaires it became apparent that identifying literature relating to the use of Safety Critical Questionnaires for aviation is limited, so to gain an understanding of questionnaires it has been necessary to step outside the domain and investigate the use of questionnaires elsewhere.

### 2.6.2 Questionnaires in Usability Engineering

Kirakowski [23] describes a questionnaire as a *method* for the *elicitation*, *recording*, and *collecting* of information. The four italicised words in this definition summarise the essence of what questionnaires are about.

[Kirakowski] decomposes this statement further and suggests that each of the four italicised words in the above definition have the following meanings:

**Method**            Used in this context means that a questionnaire is a tool to be used rather than an end in it self. Kirakowski suggests that before we start thinking of using a questionnaire, a useful

question to ask is: 'what do I need to know and how best can I find this out?' Some forms of information are not reliably gathered when using questionnaires (e.g. how often people do things, or self-reports about aspects of life where status is involved.). Kirakowski suggests that it is also very useful at the start to ask your self, 'how will I summarise the information I am seeking to give me a true picture of what I want to know?'

The COED definition of Method is:

*.. a way of doing something or the orderliness of thought or behaviour.*

The COED definition agrees with what Kirakowski is saying and follows that the SSQ is presented in such a way that it is a tool required to gather information regarding the safety and airworthiness of the proposed SM design.

**Elicitation** A questionnaire may bring out information from the respondent or it may start the respondent thinking or even doing some work on his or her own in order to supply the requested information. A questionnaire is a device that starts off a process of discovery in the respondent's mind.

From the definition of elicitation, it can be seen that this applies to the SSQ. The SSQ is set of questions that require answers to a set number of questions. The answers to the questions are derived from a thought process by the respondent who examines what effect the proposed design will have on safety and airworthiness of the platform or equipment. The successful completion of the SM is based upon the important input derived from answers formulated in the SSQ. It must be remembered that the completion of the Trials Installation (TI) leaflet (used to embody the SM) is heavily influenced by the outcome of the SSQ as well as forming the input and influence on the system Safety Case. The set of guidewords in the response form for each question asked provide the elicitation guidance for the yes/no answers.

**Recording** The answers the respondent makes are somehow recorded onto a permanent medium, which can be re-played and brought into analysis. This is usually by writing, but also possibly by recording voice or video.

Completing the yes/no boxes on the front of the sheet provides the answers to the SSQ. The response form in support of the SSQ is also a set of written/typed answers and forms a piece of evidence or information which can be used in support of the SC and the SM process and which also supports the SSQ.

**Collecting** Kirakowski suggests that people who use questionnaires are collectors. Given the amount of effort involved in creating a questionnaire, if you only ever needed to use it for one respondent, you would probably find some more efficient method of getting the information. However, unless there is no intention of using the collected information, it is important to consider what and how the amassed information will be used.

So what happens to the SSQ? The completed SSQ is sent, with an amplification of the original proposal (AOP) to the IPT. The AOP will be completed by the DO that has been chosen by the IPT and provides further information on the proposed SM i.e. safety, airworthiness, and other information such as weight and balance, size of any LRU's that are required to be fitted, power analyses and operating requirements that are appropriate to the engineer and the aircrew.

Following analysis of the SSQ, the IPT will decide whether any specialist advice is required regarding any of the issues raised. This will encourage the IPT to consider all aspects of the SM process and the SC for both system design and platform. The SSQ will also be passed to the platform SCM who will then decide what actions to take regarding changes that affect the original platform safety case. The completed SSQ can be distributed by the IPT to specialist departments and those staffs that will form and be involved with providing specialist advice for the SM process. At a minimum it is felt that a PHA will be required.

### 2.6.3 Basic Types of Questions

Kirakowski identifies that there are three basic types of questions:

- a. Factual type questions.
- b. Opinion type questions.
- c. Attitude type questions.

#### 2.6.3.1 Factual Type Questions

Kirakowski states that factual type questions ask questions about public, observable information that it would be tedious or inconvenient to get any other way. For instance, numbers of years that a respondent has been working with computers or what kind of education did the respondent get.

#### 2.6.3.2 Opinion Type Questions

These ask the respondent what they think about something or someone. There's no right or wrong answer, all we have to do is give the strength of our feeling: do we like it or not, or which do we prefer? Opinion questions direct the thought of the respondent outwards, towards people or artefacts in the world. Responses to opinion questions can be checked against actual behaviour of people, usually, in retrospect.

#### 2.6.3.3 Attitude Type Questions

Attitude questions focus the respondent's attention to inside themselves, to their internal response to events and situations in their lives. There are a lot of questionnaires consisting of attitude questions about experiences with Information Technology, the Internet, and Multi-media and so on.

Questions are frequently used in evaluation work and are used to ask respondents what their expectations are about the system that will be evaluated. The SSQ asks both factual and opinion questions. The person/s completing the SSQ is required to provide answers to a question based on the thought provoking guidance supplied with the SSQ. They are asked to consider any implications or effects that the proposed design has on the safety and airworthiness of the system/platform/equipment that the proposed design is to modify.

### 2.6.4 Closed and Open Ended Questionnaires

Blackwell [24] introduces that there are different formats of questionnaires; closed-ended/open ended questionnaires. A closed ended questionnaire is one that leaves no room for individual comments from the respondent. The respondent replies to a set of questions in terms of pre-set responses for each question. These responses can then be coded as numbers. An open-ended questionnaire requests the respondent to reply to the questions in their own words, maybe even to suggest topics to which replies may be given. Kirakowski [23] refers to the same thing calling the questionnaires closed/open format questionnaires. Closed format questionnaires might ask respondents to agree or disagree with a statement, to select one of several categories as corresponding most closely to their opinion, or to express their opinion as a position on an ordered scale.

For analysis it is suggested that closed format response are easier to analyse but do have the disadvantage that one must anticipate what the respondents want to say. The SSQ falls into the category of both closed and open ended/format questionnaire containing both factual and opinion based questions, however, analysis of the SSQ is not carried out using a numbered scale technique. An assessment of the effect in the first instance is carried out qualitatively by the platform IPT.

Kirakowski [23] supports the contention that it is possible to mix factual and opinion questions, closed and open-ended questions as in the SSQ. It is suggested that it is a good idea to mix the two together and to have some open-ended questions in a closed-ended opinion questionnaire. It is also not a bad thing to have

some factual questions at the start of an opinion questionnaire to find out who the respondents are, what they do, and so on. Some factual questions may need to be open-ended, for instance if respondents are being asked for the name of the hardware they are using. Open-ended questionnaires are advantageous when used in an exploratory phase of research or if very specific comments or answers that can't be summarised in a numeric code are required as such in the SSQ.

There is limited information regarding the use of questionnaires in aviation safety related and safety critical activities however; both the Acquisition Safety and Environmental Management System (ASEMS) [25] and Acquisition Safety and Environmental Support Group (ASESG) [8] have provided questionnaires for safety related activities. Both use a similar style using opinion/factual based type questions in open-ended questionnaires. In the ASEMS the 'Safety Operating Environment Questionnaire' takes a similar form to the SSQ. The study conducted by the ASESG [8] on the fast jet IPT's also used a similar form to that of the SSQ. The ASEMS also uses checklists for Hazard analysis and Risk reduction.

### 2.6.5 Examples of Questionnaires Used in Other Industries

Questionnaires are used in other areas of industry for example rail, nuclear, medical and by other military organisations to question safety related and safety critical issues. The following three examples show the use of questionnaires for these activities.

#### Example 1 - Railways (Safety Critical Work Regulations 1994 (the 'Regulations')) [26]

Although the Railways are outside the context of this report the following example provides a good example of alternate methods used in a questionnaire. The Business Strategy Group (BSG) was commissioned by the Health and Safety Executive (HSE) to produce an evaluation report on the Railways (Safety Critical Work) Regulations 1994 (the 'Regulations'). The survey was undertaken in three main sections: review of published statistics; discussions with key stakeholders and organisations representing a wide spectrum of the rail industry, and gathering views of safety critical workers and those who supervise them by means of a postal questionnaire distributed by stakeholders.

This project will look at the third main section detailed in the paragraph above. Gathering the views of safety critical workers and those who supervise them was carried out using two questionnaires, one for the safety critical workers and the other for the safety critical managers. The type of questionnaire used was one requiring an answer that provided a rating to the specific question about the regulations on a rating scale 0 to 5, where 5 would indicate a high impact. This type of questionnaire according to Kirakowski is a closed-ended questionnaire, which leaves no room for the individual to comment. They answer a pre-set of questions. It also provides answers in data format which are numeric and quantitative. Quantitative data is easier to analyse using statistical techniques and is representative of collecting data using objective techniques.

#### Example 2 - Perception of Procedures by Operators and Supervisors [27]

In example 2, Hudson van der Graaf and Verschuur carried out a study on the perceptions of supervisors, technicians and operators of the procedures for seven safety-critical activities. This was achieved using a questionnaire in which the subjects rated a variety of attributes, and ranked the different procedures in terms of dangerousness, controllability and susceptibility to violation.

The questionnaire was constructed with a number of general questions and sets of questions specific for each of the activities chosen. The types of questions asked were as follows:

- a. Paired comparisons of the seven activities – each activity is set against each of the other activities so that there are twenty one comparisons in total.
- b. Rankings of each of the activities on four attributes:
  - Perceived dangerousness (Which activity is the most dangerous?)

- Importance (according to the respondents own criteria) (Which is the most important?).
  - Controllability (Which is the most controllable?)
  - Sensitivity for violations (Which is most likely to have people committing violations?).
- c. Each activity is given a rating on a 5-point scale using 18 items, with respect to:
- The probability of accidents.
  - Controllability of the activity.
  - The content and quality of procedures.
  - Perceived sensitivity of the activity for violations.
  - The amount of experience the respondent has with the activity.

Respondents made comparisons of the seven activities on a 5-point scale (running from not at all, similar to very similar). Again the process of answering this questionnaire was the same as the one produced for the BSG study above and the results were in the form of quantitative measurement.

What is interesting, in the above examples both ratings and rankings were used to answer the questions within the questionnaires which unlike the SSQ, which uses yes/no. This data was then modelled to represent the respondent's answers. This is an easier task when using quantitative data, but more difficult with qualitative data as that provided in the SSQ. It may be possible that a ranking/rating method could be carried out on the SSQ.

### Example 3 - Software System Safety Activities [28]

When we look at the questions asked in a safety critical software questionnaire produced by the U. S. Army Communications-Electronics - Life Cycle Management Command [28], we see a qualitative type questionnaire being asked about Software System Safety activities and these questions are similar to those of the SSQ and only require a yes/no answer. An example is shown below. Both simple and highly integrated multiple systems are experiencing an extraordinary growth in the use of computers and software to monitor and/or control safety-critical subsystems or functions. A software specification error, design flaw, or the lack of generic safety-critical requirements can contribute to or cause a system failure or erroneous human decision. Safety-critical software must then receive continuous management emphasis and engineering analysis throughout the development and operational lifecycles of the system. So for these reasons questions regarding the software are as follows:

### Example of Questionnaire

1. Does the system contain software/firmware?
2. Does the software/firmware have complete control over hardware and its subsystems or components without the ability of operator intervention?
3. Does the software/firmware have control over a hazardous system and does it allow for operator intervention?
4. Does the software/firmware generate information which will be used in the making of critical decisions?
5. Do adequate controls exist in the design of the software to minimize the risk of potentially critical hazards?

6. Will credible failures of single hardware input or output devices result in the occurrence of a catastrophic or critical hazard?
7. Does the system power-up to a safe state and revert back to a safe state in the event of the failure of critical components, such as: Primary computer or Power failure?

Any one of the questions above could be answered with a simple yes or no, and much like the SSQ the answers would be useless without supporting evidence. The process does go on to provide some guidance and thought provoking prompts that are detailed as such:

#### **How do you approve existing safety in old software?**

1. Get all information on field history such as:
  - a. Hours of use.
  - b. Type of actual use.
  - c. Environmental conditions.
  - d. Experienced personnel.
  - e. Existing hardware configuration (sensors, computer, I/O)

#### **Analyse all changes to the above, including new missions, use and time.**

2. Determine the true "delta" of the software package. What are the new functions vs. the new hazards? Are the old hazards being corrected in the new version?
3. Review the process that produced new version. Does it look like they are developing good code?
4. Review the S/W audit minutes. If SSWG's are available then get them and review for S/W hazards.
5. If the code is written, you will have to go with testing. If code is not yet written, give the S/W developer code and design checklists. Tailor the checklist with the known hazards, the error set known in the language, CPU, and architecture. If testing is the only means available, you should develop tests, which are derived from the hazards (and resulting requirements specification). Use the error sets for language, CPU, checklists, and examples.
6. Ensure that all hazards have been addressed by all tests, including all field history-derived hazards.
7. Review test procedures/cases and problem reports for safety critical applications during formal qualification and regression testing on the target hardware.
8. Recommend and implement corrections to all safety critical issues that resulted from formal testing.

So in comparison to the SSQ, the above format of questionnaire appears more thorough than the SSQ and the guiding questions ask the respondent relevant topical questions i.e. 'What are the new functions vs. the new hazards?', 'Are the old hazards being corrected in the new version?' It is possible that this form of asking questions relevant to safety related and safety critical aviation systems could be applied to the SSQ – this will be investigated in the evaluation Chapter 5.

## 2.6.6 Checklists

The previous paragraphs discussed different forms of gathering data in questionnaires and it was also suggested that the SSQ is a form of questionnaire. However, can the SSQ be viewed as a 'checklist'? The following paragraphs investigate this concept

Scriven [29] describes a checklist as:

*..... a list of factors, properties, aspects, components, criteria, tasks, or dimensions, the presence or amount of which is to be separately considered, in order to perform a certain task.*

The SSQ is used to provide qualitative information/data which in many cases because of the nature of the task can be very vague or even ambiguous. It does not gather statistical evidence or require the output to be used for empirical data entry. Scriven [29] also suggests that there are many different types of checklist, although they have at least one non-definitional function in common—that of being a mnemonic device. This function alone makes them useful in evaluation, since the nature of evaluation calls for a *systematic* approach to determining the merit, worth, etc., of what are often complex entities. Hence, a list of the many components or dimensions of performance of such entities is frequently valuable. The Hutchinson Encyclopaedia [30] describes a 'mnemonic' as any device or method that helps memory. The word 'mnemonic' comes from the name Mnemosyne, who was the Greek goddess of memory. Mnemonics are particularly useful for remembering lists, or the order that things come in.

A checklist is also defined in the Concise OED [21] as:

'...a list of items required, things to be done, or points to be considered'.

A checklist is described in Data and Computing Guidelines/ Standards Definitions [31] as:

'.....lists containing brief questions which when properly answered will reveal possible weakness in a system.'

To expand on the above definitions, a checklist can be used to describe the assessment process step by step, where each step is an action item or an element that is required for a task. It could be argued that the SSQ questions form elements for the SM task, which in this case is to provide information on the effects of the proposed design with respect to safety and airworthiness activities on the platform systems. In the COED definition it mentions 'points to consider'. These points in the SSQ are raised when the respondent uses the SSQ response form guide words to consider what effect the proposed design has on the safety and airworthiness applications of the platform. In comparison with the definition provided by Data and Computing guidelines it is true to say that the SSQ is more like this definition and not only will the questions, if answered properly, identify weaknesses, they will also highlight strengths of the system.

A new definition of checklists that represents the SSQ could be derived from the above two definitions and would look like this:

'....lists containing brief questions and points to be considered which, when properly answered will reveal possible strengths/weakness in the proposed system'.

The Data and Computing guidelines use the word 'properly' in their definition and this is something that raises concerns when the SSQ is being completed. The completeness and integrity of the answers supplied for the SSQ especially Q6.01a is totally dependent on the knowledge, skills system knowledge and competencies of the person completing the SSQ. The author feels the guidance provided for completing the SSQ is weak and very much open to interpretation. To reiterate a point made by Graham, these questionnaires are completed by people who are not familiar with safety analysis and assurance and without some knowledge within this field; the questions will not be answered fully.

The guidance given for answering Q6.01a 'does the SM have an effect on the safety case' makes an assumption that the respondent knows what they are doing. Although an independent third party may

produce the SC, the respondent still has to answer this question. There is no model guide on how to complete it and in what format it should be.

### 2.6.7 SSQ Summary

In summary, questionnaires are made up of items to which the respondent supplies answers or reactions. Answering a questionnaire focuses the respondent's mind to a particular topic and almost by definition, to a certain way of approaching the topic. The SSQ asks both factual and opinion type questions using both open and closed format questions. However, without the SSQ Response guidance sheet, the SSQ would be pretty meaningless in its form as just a sheet of yes/no answers. Graham makes the point that although specialist advice is sought during SEM investigation, it is possible that a potential hazard could have been overlooked during the proposal phase and continues to remain un-investigated during the later phases of an SEM project. This is also true of the SM; however, unlike the SEM, the SM process requires that a SC be provided for all new systems. This is articulated down from the Secretary of State (SofS) through the DASB. By providing a SC for each proposed SM system ensures that any hazards that have been overlooked during initial investigations would be addressed and dealt with in the SC process.

The SSQ is generic form of questionnaire and a response to each question is requested. Some generic checklists are provided to prompt the system safety analysis process; however, their generic approach will dictate a certain degree of care in their application to ensure that the process is thoroughly completed.

In supporting Graham's comments, there is a possibility that particular and very relevant safety issues regarding the design will be missed, overlooked or not considered when using the format detailed in the SSQ. It must not be forgotten that this form provides essential information, in particular to the SCM, on factors that may affect the platform SC. It also provides the basis on which the system design is to base its SC. With that in mind, it is felt the SSQ does not provide sufficient information to avoid the concerns raised by Graham and the intent is to attempt to investigate whether it is possible to make the SSQ more appropriate to safety analysis activities, without making the form incomprehensible so that it can still be used by all three services.

## 2.7 **Review of Standards and What Guidance They Provide**

In the preceding paragraphs much has been discussed on the completion of Q6.01a of the SSQ, what is required to complete the question and that the guidance provided is not comprehensive to enable the aviation engineer to complete the question thoroughly. These next paragraphs review the documents and standards associated with the requirements of the JAP and hence the SSQ to ascertain what guidance is available.

### 2.7.1 Defence Standard 05-123

DS 05-123 [15] is the standard for 'Technical Procedures for the Procurement of Aircraft, Weapons and Electronic Systems'. To quote the standard, its intended purpose is that it:

'Provides requirements for the technical procedures to be applied to Ministry of Defence (MOD) contracts for the procurement of service aircraft, their installed systems and associated equipment, guided weapons (GW) systems and associated equipment, and specified electronic equipment'.

The standard in its own right is not a safety document but does set out requirements for contractors to ensure safe design of their products.

DS 05-123 covers information on activities and topics as follows:

- Approval procedures and responsibilities - including design and development responsibilities, certification procedures and allowable material specifications.
- Development procedures - including certification for flight trials, preparation of specifications and flight-test procedures.

- Control of designs and design records - including amendment and modification procedures.
- Supply of technical information - including provision of technical publications and operational documentation.
- Production procedures - including maintenance of engineering records.

As already discussed DS 05-123 describes a modification as:

“...when ...a change to the design records... affects one or more of the following:

- Safety, operational use, reliability, maintainability or other specific MOD requirement.
- Production or which may involve retrospective embodiment.
- Cost or delivery programmes of the item or its Service spares.
- Interchangeability of the item or its Service spare.”

Here the processes for initiating, classifying and approving modifications are outlined and it also details the various committees within the industry contractor’s domain and the MOD who are required to review the modification process.

DS 05-123 also details the contractor responsibilities for completing a full design and development package. This also includes all relevant test and development data, including the appropriate drawings and technical information required by the contract associated with the project. There is no emphasis placed on safety documentation and as such it does not provide a source of guidance for completing the safety elements of the SSQ.

The IPTL will decide if modification action requires the re-issue or amendment of the Certificate of Design (COD). However, where trials of a modified aircraft or modified airborne equipment flight are considered necessary, a COD is required to support the Certificate for Flight Trials (CFT). The certification of design point is reached when the IPTL, the contractor and the DO if not the contractor, agree that the design of the materiel adequately meets the requirements of the specification within the limits and exceptions that have been stated. Both the COD and CFT are discussed later in this project.

Much of the evidence provided for the COD can be used as supporting evidence in the production of the SC and can be used to strengthen the argument that the system that has been modified and the platform it is embedded into is safe for its intended purpose. In turn it is required as part of the data gathering exercise within the SSQ and it is therefore important that the engineer compiling the SSQ is to be aware of the DS requirements so that this evidence is collected. This forms part of the evidence that is put forward to the RTSA when reviewing the RTS. This DS does not however, contain any specific detail or guidance as to how the SSQ 6.01a question should be completed and can only be used as a reference document.

This COD and CFT documentation is a requirement of the SSQ and forms evidence as to airworthiness/safety of the equipment and is used by the RTSA when reviewing the RTS. Directly related with the SSQ it does provide technical engineering information appropriate to design, which can be used and is required when completing the SSQ.

## 2.7.2 Defence Standard 00-56 – Safety Management Systems for Defence Systems

At the time of writing this report DS 00-56 [11] has been revised and republished as an interim document in the form of DS 00-56 Issue 3. Issue 3 replaces the current safety-related Defence Standards; 00-54 (Requirements for Safety Related Electronic Hardware in Defence Equipment) [32], 00-55 (Requirements for Safety Related Software in Defence Equipment) [33] and 00-58 (HAZOP Studies on Systems Containing Programmable Electronics) [34]. The document is written in two parts, both parts are applicable and a

requirement for defence contractors. DS 00-56 is the main standard for system safety engineering within the UK defence industry. It defines a safety case to be ‘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 environment’.

Part 1 contains the mandatory safety management requirements and focuses on key principles and is applicable to in service operation, maintenance and modification. Issue 3 has moved away from the prescriptive approach towards development processes as was taken by issue 2 and now concentrates on the emphasis of the provision of a structured argument, supported by a compelling body of evidence (product and process), as the core of a safety case.

Part 2 contains guidance to enable contractors to establish a means of complying with Part 1 and includes specific material on the provision of safety evidence for software and electronic hardware (known as complex electronic elements). It does not automatically follow that use of these guidelines will result in full compliance with the requirements of Part 1.

When reviewing the DS to investigate what guidance is provided that would be of use in completing Q6.01a of the SSQ it was decided that Part 2 would give the engineer a starting point as to what the deliverables are when providing evidence in support of the argument for the SC. Although part 2 does not prescribe specific deliverables, there will be a contractual requirement to deliver certain documents. A typical list of deliverables (not exclusive) specific to safety is detailed in the standard as:

- Safety Case.
- Safety Case Reports (SCR).
- Safety Management Plan (SMP).
- Definition of the Safety Management System (if not documented in the SMP).
- Safety Audit Plan.
- Hazard Log (or summary of as appropriate).
- Safety Audit Reports.
- Minutes of Safety Committee meetings.

In the context of this report, DS 00-56 applies to the SM process. Although the SSQ does not require what are perceived to be the main elements of a SC to be provided, it does enquire as to whether the DO regard that the proposed system will have an effect on the SC. There is however, no prescribed format in the DS that the SC should take. Graham [17] also made comment on this.

Although no particular format is given, the guidance provided in Part 2 steers the reader through the requirements of each element of the SC in particular the types of evidence that should be supplied to formulate a cohesive and robust argument in support of the SC. Much guidance is provided in particular guidance on an explicit SC. The explicit argument in the SC should be structured and contain references to the documented evidence. In the case of the SM, this evidence is provided in the traceable and auditable paperwork process SM1 through SM10. This supporting evidence can be used in support of the SC although it does not supply evidence such as System Safety Analysis, Risk and Hazard Management.

In summary, DS 00-56 provides useful information to assist the engineer when answering 6.01a of the SSQ. Although the DS does not provide specifics as to what the SC should contain it does detail the safety basis for answering the questions. This new issue of DS 00-56 moves away from a prescriptive approach and adopts a goal based approach. This is similar to the approach taken by the Civil Aviation Authority's SW01. DS 00-56 requires that a safety case be developed. Later in this report it will be discussed as to what are the possible contents of a SC.

### 2.7.3 Superseded Defence Standards

DS 00-55 and 00-58 have been superseded by issue 3 of 00-56, so there is no longer particular defence standards relative to safety related software or E/E/PE devices. Part 2 of DS 00-56 does provide some guidance towards the 'Safety of Systems Containing Complex Electronic Element', which is in support of the now defunct 00-55. This part of the standard is primarily concerned with safety requirements, derived safety requirements and provision of evidence for complex electronic systems'. However, another change included in Iss 3 of 00-56 is the move away from Safety Integrity levels 1-4 where level 4 is safety critical. IEC 61508 maintains SIL levels and are discussed in some depth, and numerical failure rates are linked to each of the integrity levels. As Storey [35] says 'the standard adopts a risk based approach to the determination of safety integrity level requirements. SILs are common place within the safety analyses of software and this is applicable to military designed software as well. However, it is unlikely that this standard will be adopted and used as a military standard as it is processed based and designed more for the plant/nuclear type function, and as far as I am aware, it has not been used as such.

DS 00-55 does provide good source of information regarding SILs as does IEC61508 which again can be used by the engineer in understanding what these particular safety critical levels are. It does not provide information on what areas should be considered that can help the aviation engineer establish as to what the effects are on the SC following a service modification.

### 2.7.4 MIL-STD-882B

Military Standard (Mil Std) 882 is going through significant change and is now at Mil Std 882D. However, as far as the author is aware, versions A-C are still extant and still being used. It is important the aviation engineer is aware of this fact as he may come in to contact with a system that has been contracted to one of the Mil Std 882 versions. Mil Std 882B [36] was developed by the US Department of Defence (DoD) in 1984. It requires that contractors establish and maintain a formal system safety program that ensures:

- Safety consistent with the mission is designed into the system.
- Hazards associated with the system are identified evaluated and eliminated or the associated risk is reduced to an acceptable level.
- Uses historical data concerning failures.
- Records significant safety data for use in other systems.

The standard provides requirements for developing and implementing a System safety program to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps (accidents) by eliminating hazards or reducing risks. It applies to every activity of the system life cycle; e.g., research, technology development, design, test and evaluation, production, construction, checkout/calibration, operation, maintenance and support, modification and disposal. Typical tasks are system safety program plan, preliminary hazard analysis, and software hazard analysis.

Hazards are categorised into four levels: Catastrophic, critical, marginal, and negligible. The standard states that for hazards that are either catastrophic or critical, unless a waiver is granted, a safer design or safety devices must be used to reduce the risk. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. In the UK the normal approach to reducing risk is carried out to As Low As Reasonably Practicable (ALARP). ALARP is discussed later in this project.

In summary, this standard describes many tasks that contractors must perform. It is similar in format to that of DS 05-123 and is not unlike DS 00-56. Like DS 00-56 it does not describe specific techniques that must be used, but outlines the tasks which in turn allow the program/project manager to choose techniques. If instead the contractor chooses the techniques, the standard requires that the program/project manager approve of the techniques. This particular stand is different to that of DS 00-56 where DS 00-56 requires the

contractor to comply with the requirements of the standard. The Mil Std takes a systems view of safety and discusses the particular approaches to be taken if there is a significant software element to the system. In the rationale, the standard lists various techniques for ensuring safety. These include software fault tree analysis, software sneak analysis, code walk-through and Petri net analysis. However, this standard is more prescriptive than that of DS 00-56.

### 2.7.5 Comparison of DS 00-56 and Mil Std 882B

Both DS 00-56 and Mil Std 882B describe processes that will allow safety risk to be identified; however, the approach by both is different. DS 00-56 is a 'top-down approach which requires platform-level safety targets to be specified, hazards identified, safety risk to be estimated (this will be probability and severity), safety compliance and verification. In the DS 00-56 process, accident risk is calculated as a portion of the overall safety target. Mil Std 882 however, is a 'bottom up' approach that requires hazards to be identified, safety risk assessed (accident probability and severity), safety compliance and verification. This type of approach focuses on the hazards, with safety risk to a platform being a combination of the probability and severity of all associated accidents. Both of these systems enable equipment hazards to be identified, their probability to be defined and an assessment of platform safety to be made.

### 2.7.6 Summary of Standards

To summarise the standards reviewed above, each one does provide some information that can be used by the aviation engineer when completing Q6.01a (SSQ). Although not actually specific in the intended format of the answer and exactly what the aviation engineer should consider, all the standards provide some guidance as to what is required in the overall SC package. However, there is nothing specific in any of the standards that provide a useful format which can be adopted and used as an aid by the aviation engineer to completing Q6.01a of the SSQ.

## Chapter 3 – Defining the Requirements of Question 6.01a of the Safety and Support Questionnaire.

As already discussed, the SSQ is made up of yes/no questions which are to be supported by information provided by the SSQ Response form. If we take Q6.01a and look at it more closely, it can be seen that there are three elements to the question:

### **Box 6.01a:**

‘State the effects on the Safety Case, the required changes and associated actions’

It asks the aviation engineer answering the question to consider three conditions:

- The effects on the Safety Case that the new system may cause.
- The required changes to the safety case.
- Associated actions.

Before the aviation engineer can answer these conditions accurately and concisely it is important for him to understand exactly what this question is asking. To be able to do this, the aviation engineer must be versed in safety engineering terms and understand what they mean. The safety engineering world is made up of many terms, meanings and acronyms which are probably completely alien to the average aviation engineer who is required to populate Q6.01a and to a greater extent, the SSQ. It may be that for many aviation engineers who are answering this question, it may be the first time they have encountered safety terminology and it is possible that they have no idea as to what the terms used mean.

Remembering back to the SSQ Response form reviewed in Chapter 2 and which supports the SSQ question sheet, it was identified that there is no specific guidance given as to:

- What Safety terms mean in the context of the SSQ.
- What the engineer should be considering as to what affects the proposed design has on the existing SC.
- What are the required changes i.e. changes to the hazard log, changes to the SMS mean, is there a requirement for a new SC etc.
- Any associated actions i.e. changes to the RTS, any other supporting airworthiness documentation etc.

In the following sections of this chapter, the author attempts to identify what are perceived to be the most common safety engineering terms used, which relate to the activities detailed in Q6.01a of the SSQ and which the aviation engineer will need to be aware of and understand. It is noted, that safety engineering is a specialised topic and it will be unfair to assume, that without appropriate training, the average aviation engineer will understand and know about all safety engineering terms. However, this is taken into consideration when identifying these terms and will be evaluated in the evaluation phase. The terms chosen will be used in the evaluation phase through a questionnaire which will be used to assess what knowledge of safety terms and meanings the aviation engineer has. From the findings of the evaluation it will be decided and to what extent the level of guidance is required to assist the aviation engineer in understanding these terms.

## 3.1 Identification of Terms Used in Support of Q6.01a of the SSQ

Each of the terms explained in the next sub sections are perceived to be those terms that the aviation engineer should be familiar with and understand when completing the safety element of Q6.01a of the SSQ. On a larger scale, many of the terms chosen are also used in other areas of the SSQ so it is important for the aviation engineer to know them.

Most terms or definitions chosen are identified and then a small narrative is supplied describing what each means and where possible where it fits in the safety life cycle of the SM process.

### 3.1.1 Airworthiness

Airworthiness has been used consistently throughout this project so far and although considered to be a separate entity with respect to safety, the term Airworthiness is often used to mean and include airworthiness (safe to fly) and safety issues. This can be seen in the following definition:

...‘the ability of an aircraft or other airborne equipment or system to operate without significant hazard to aircrew, ground crew, passengers (where relevant), or to the general public over which such airborne systems are flown’.

The above definition talks about the safe to fly element of the aircraft being in a condition (safe) that when it is flown and it’s systems operated it will not cause any hazard (safety) to any persons that are in direct contact with the aircraft or may be those that be vulnerable as to when the aircraft is flown over there position.

### 3.1.2 Aircraft Release and Flight Trials

Although the following paragraph does define a term or describe a definition, it is important that when Service modifications are being considered the need for flight trials will be assessed by the aviation engineer. This is dealt with during an ‘Initiation’ meeting for the SM. Following acceptance of the SM proposal, an Initiation meeting will be held where all interested stakeholders will attend to consider the outline design. Safety, airworthiness and operational, engineering and support risks and issues are addressed. If specialised support is required this will be discussed and normally will be tasked by the appropriate IPT. This may include an experienced and appropriately designated safety organisation to compile the safety case. The RTSA will inform the meeting of what documented evidence is required in support of the SM so that it can be put in the RTS. Following trials (including Flight trials) the build standard and associated restrictions or limitations stated in the Aircraft Release shall be, amended where necessary. In this case the RTS.

### 3.1.3 Certificate of Design

A COD is described in DS 05-123 [15] as being evidence for the extent of how the design meets the requirements of the specifications and is required when materiel is delivered for evaluation trials, when the first production equipment is delivered or when required by the IPTL. A COD provides evidence that; the product has been manufactured to an approved drawing set, the methods used of checking design calculations including the procedure for verifying computer outputs. It also defines specific evidence of structural integrity and any testing that may have been carried out. It will also include any other COD’s that have been agreed by the DO for materials designed and developed by other DO and incorporated in the design. Safety requirements will be included. Much of the evidence provided for the COD can be used as supporting evidence in the production of the SC and can be used strengthen the argument that the system that has been modified is safe for its intended purpose. It will also be used and included in the RTS for the ‘as flown’ configuration.

### 3.1.4 Hazard

It is important that the engineer can identify as to what constitutes a hazard and an accident. These terms are often confused with each other and their states are incorrectly identified. It is also important that the aviation engineer designing the SM can identify the hazards associated with the SM design. This will involve the aviation engineer carrying out systematic analysis of the hazards which the system may encounter in operation. He will need to decide what control measures can be used to eliminate or reduce the hazard, identify the points in the system where the control measures are required to ensure system safety and then monitor and review that the controls are working.

A hazard is a situation in which there is a potential for human injury. Roland *et al* [37] suggests that the Safety person sees a hazard as an implied threat or danger, of possible harm. This is a potential condition waiting to become a loss. For the hazard to become a loss, the hazard must transfer through a change of state from the potential condition. An example would be component failure. They also suggest that a more technical definition of a hazard is:

‘A potential condition, or set of conditions, either internal or external to a system, product, facility, or operation, which, when activated transforms the hazard into a series of events that culminate in a loss (accident).

An example of a hazard for a system such as trials equipment mounted inside an aircraft would be:

Condition	Hazard	Risk Reduction Measures	Probability	Severity	Risk
Trials equipment mounted inside the aircraft.	Equipment breaking free and causing an obstruction	Trials equipment is mounted on the inside of the aircraft.	Improbable	Marginal	B(9)

**Table 1. Example of a Hazard Analysis Table**

A simpler and more fundamental definition of a hazard is, ‘a condition that can cause injury or death, damage to or loss of equipment or property, or environmental harm’.

### 3.1.5 Hazard Log

The Hazard Log will be affected by the SM design and should be reviewed for updating to include what the effects are. The aviation engineer may not have access to the SC and the Hazard Log but he must be aware that by introducing change through an SM there will be an impact on the Hazards already listed in the SC Hazard log. The Hazard Log should contain recorded information of the safety justification, or Safety case, and should provide a summary of all safety activities throughout the system life cycle. It will also contain details of each hazard and accident and should make reference to the following:

- Severity categories
- Probability categories
- Equivalent numerical probabilities
- Accident risk classification scheme
- Design rules and techniques
- Partitioning of random and systematic elements of the hazard probability targets between system functions

### 3.1.6 Risk

The risk associated with a hazard is determined by two factors:

- The potential consequences of any accident that might result from the hazard (severity)
- The frequency (probability) of such an accident occurring

Risk is a function of probability and severity and is associated with the possibility of harm. Just as the activation of a hazard can result in an accident, so the risk is related to that probability, intensity, and duration of the stimulus will be sufficient to transfer the hazard from a potential state to a loss. This is not an area that will be strongly considered by the aviation engineer and it is not the norm at the level where SM designs are carried out for Risk analysis to be considered. However, it is important that aviation engineers are aware of the Risks associated with their SM design and they are made aware of classification tables. Classification tables are an essential tool in defining the acceptability of safety risk and identify the priority and nature of action to be taken. The Safety Risk Classification table shown below in Table 2 [12] is the baseline standard for all DLO (Strike) projects. Should IPTL's choose to use a numbering system to prioritise safety risks, the historic numbering convention as shown in the table is used.

		Accident Severity Categories			
		Catastrophic	Critical	Marginal	Negligible
Accident Probability Categories	Frequent	A (1)	A(3)	A(7)	B(13)
	Probable	A(2)	A(5)	B(9)	C(16)
	Occasional	A(4)	B(6)	C(11)	C(18)
	Remote	B(8)	C(10)	C(14)	D(19)
	Improbable	C(12)	C(15)	D(17)	D(20)
	Incredible	C(21)	D(22)	D(23)	D(24)

**Table 2. Example Of A Risk Classification Table**  
(Annex A to BP1201) [12]

The risk classification table shown in Tables 2 and 3, when used with the As Low As Reasonably Practicable (ALARP) carrot in Figure 8 describes the acceptable and unacceptable levels of risk and the required actions to minimise or mitigate that risk. Each classification is shown as a region and is used to determine when a safety risk has been reduced to ALARP. A Statement of Risk Classification should be included to provide a brief statement of the current System Risk Class. It should contain sufficient information to enable it to be a stand alone statement, and it should contain the Hazard Log reference to enable traceability to its supporting documentation.

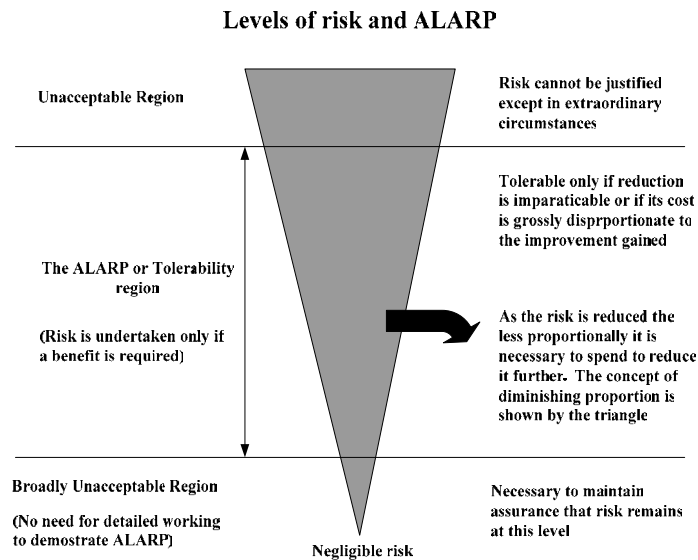
Risk Classification	
<b>A</b>	Unacceptable – Urgent management action required since such risk can not be justified save in extraordinary circumstances.
<b>B</b>	Undesirable – Requires management action to introduce control measures to reduce risk and shall only be accepted when risk has been reduced to ALARP.
<b>C</b>	Tolerable – The residual risk is tolerable only if further risk reduction is impracticable or requires action that is grossly disproportionate in time, trouble and effort to the reduction in risk achieved.
<b>D</b>	Broadly Acceptable – The level of residual risk is regarded as insignificant and further effort to reduce risk not likely to be required as resources to reduce risks likely to be grossly disproportionate to the risk reduction achieved.

**Table 3. Example of Risk Classifications**  
(Annex A to BP1201 [12])

When assessing risk it is important for the aviation engineer completing the SSQ and in particular Q6.01a, to consider the following:

- The value of the assets that are threatened.
- The probability that a threat to these assets will arise (the hazard probability).
- The probability that the threat will develop into an incident (the accident probability).
- The probable extent of the damage to the assets.
- The costs of repairing or replacing the assets or compensating the asset owners.
- The circumstances of use. Our view of what is an acceptable risk depends on the circumstances where that risk is being evaluated.

### 3.1.7 The ALARP Principle



**Figure 8. The ALARP Principle**

This is a common and frequently used term in the safety engineering world. The evaluation will assess the engineers understanding of the acronym and how it is used in relation to risk reduction. It is the requirement of the Health and Safety Work Act (HSWA) [9] to reduce risks so far as is reasonably practicable. This is implemented by the adoption of the ALARP principle (Figure 8), which states that safety should be improved beyond the baseline criteria when reasonably practicable. To achieve ALARP will require some evaluation be it qualitative or quantitative, of the reduction in risk associated with adopting some particular measure, and a clear view of the costs. In some circumstances, both safety risk and the marginal cost or efforts to improve safety can be realistically assessed in numerical terms; in others, risk reduction can only be judged qualitatively – for example, the simple addition of a further safety feature, which costs relatively little, may be obviously worthwhile. However, if the risk falls in the intolerable region the cost is irrelevant. It is felt that if the aviation engineer is to address risk appropriately within his SM design then it is important he understands the ALARP principle. The problem here is that ALARP is the start of the argument and not the end, and if the aviation engineer can not apply the ALARP principle to his design then there is little chance to justify that Risk will be mitigated appropriately.

### 3.1.8 Safety

Due to new safety legislation, the reductions in Crown Immunity and the ever-growing litigious society, the MOD and Armed Forces in recent years have had to assess and look at how they ensure their equipment is safe to operate and support. The MOD and Armed Forces are now required to demonstrate that safety is measurable, traceable and visible, therefore allowing the management and control of risks associated with their platforms or equipment.

Storey [35] defines Safety as:

... 'a property of a system that it will not endanger human life or the environment'

From this definition he goes on to define the term safety-related system as follows:

... 'a *safety-related system* is one by which the safety of equipment or plant is assured'.

This definition covers a widespread variety of equipment, from a micro switch that ensures a guard is closed before a machine may operate, to a nuclear shutdown system. It also encompasses systems whose primary role is to ensure safety and equipment that must provide safety while carrying out some other function. The example he uses to describe this is an aircraft autopilot.

### 3.1.9 Probability Matrix

The engineer should consider the probability category assessment for each safety risk with care and it should not only be the best estimate of the position the probability table, but include consideration of judgement as to whether the probability is likely to worsen or improve over time.

### 3.1.10 Safety Critical System

It is important for the aviation engineer to be able to differentiate between a safety critical and a safety related system when putting together his design for the SM. The reason for this is that each one is treated in a different manner and if safety techniques are not applied appropriately, especially to safety critical systems then the outcome may be catastrophic. Sub section 3.1.12 and 13 attempts to define the differences between the two systems. A Safety Critical system is described as:

'A computer, electronic or electromechanical system whose failure may cause injury or death to human beings. E.g. aircraft or nuclear power stations control system. Common tools used in the design of safety-critical systems are redundancy and formal methods'.

In the case of an Army Gazelle helicopter, the Radio Altimeter is considered Safety Critical. Other aircraft systems that may be considered (not on Army Gazelle) are Collision Avoidance Manoeuvres and Flight Management systems.

Safety critical systems combine the efficiency of computing with dangerous conditions to ensure human well-being. Safety Critical systems prevent human error in complex calculations, thereby performing important tasks better. However, the complexities of computer programming cause tragedies in Safety Critical systems. Failures in Safety Critical systems can have catastrophic effects, and due to the nature of the system, often lives are at stake when a failure occurs. Sometimes, the results of the failure can be dealt with in time to avoid an accident, but sometimes, we are not so lucky.

### 3.1.11 Safety Related System

Storey [35] defines safety related system as one by which the safety of equipment or plant is assured. This definition covers many things from a micro-switch on a machines guard to stop inadvertent operation to a nuclear shutdown system. He also suggests that it also encompasses systems whose primary role is to ensure

safety and equipment that must provide safety while carrying out some other function for example an aircraft autopilot.

Storey also suggests the term safety critical system is normally used as a synonym for a safety related system, although in some cases it may suggest a system of high criticality. Many systems within the military are treated as such and in some instances a system is defined as 'mission critical' rather than 'safety critical'.

### 3.1.12 Safety Case

This element is probably the most important focus of this project and is the area that raises most concern. The SSQ asks what the effects on the SC the proposed SM has. In the scope being considered for this project there is no definitive guidance for completing this question and it has been seen from the previous review of standards that there is nothing appertaining directly to the SSQ that provides this. This does not help the aviation engineer and before he can answer this question concisely and accurately, it is important he must first a) understand what a safety case is and b) what elements make up a SC. When the aviation engineer is conversant with the SC model he can make an accurate assessment of what within the SC is affected by the introduction of the proposed design he is dealing with. However, until that guidance is provided the aviation engineer will be constrained to making informed answers to Q6.01a. In many cases, it is not unusual for the aviation engineer to pass the requirements of Q6.01a on to the appropriate IPT who will task safety specialists to assess the affects on the SC impacted by the SM. The evaluation phase of this project will assess through a questionnaire what the aviation engineer understands by the term SC and what its contents are. SC contents are discussed in the next sub section.

Kelly [38] defines the safety case as follows:

..'A safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context'.

The SC is the documentation of the reasons why the system is believed to be safe to be deployed and it reflects the design and assessment work carried out in the development process. In most projects especially within the military world and the modification of aircraft, the SC is one of the major deliverables towards the certification process. Reflecting back to the RTS, the RTS for the 'as flown' configuration is based on the SC for the platform.

The definition of a SC given in DS 00-56 [11] is that:

'A Safety Case is 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 environment'.

The SC should contain all the evidence and arguments used to justify the safety of the system, so that a determination can be made as to the validity of the conclusions. The SC should be structured hierarchically in a logical manner and the safety justification should be summarised and catalogued in a Safety Case Report (SCR) prepared by the IPTL. The main elements of a SC are:

- System definition and description.
- Safety requirements, targets and objectives.
- Assumptions.
- Safety Assessment, which consists of:
  - Hazard Identification.
  - Hazard Analysis.
  - Risk Assessment.
  - Hazard Control.

- Safety Management System(s) – including the provisions for incident reporting and investigations.
- Emergency and Contingency Arrangements.
- Limitations for safe use.

The SC can be presented in many formats and in the past the popular method used was free text. However, one method that is gaining popularity for use today is Goal Structuring Notation (GSN). GSN is a graphical notation used to present system safety arguments. GSN is made up of ‘goals-strategies-solution’ where ‘Goals’ are (requirement, target or constraints) ‘Solutions’ are (sub-claims or evidence) and ‘Strategies are (individual pieces of analysis, evidence, results of audit reports). Guidance on the use of GSN can be found in Kelly [7].

Adelard [39] suggest that the main elements of a safety case are:

- *Claim* about a property of the system or some subsystem
- *Evidence* which is used as the basis of the safety argument. This can be facts, (e.g. based on established scientific principles and prior research), *assumptions*, or *sub-claims*, derived from a lower-level sub-argument.
- *Argument* linking the evidence to the claim, which can be deterministic, probabilistic or qualitative.
- *Inference* the mechanism that provides the transformational rules for the argument.

### 3.1.13 Safety Case Contents

It has already been identified in Chapter 2 (Literature review) that there is no definitive list of what elements make up a SC. In most cases these will depend upon the nature of the service modification to a specific platform. The *CONTESSE Test Handbook* (CONTESSE) [35] details a number of items that may be but are by no means definitive, included in a safety case and are as follows:

- A description of the safety related system
- Evidence of competence of personal involved in any safety activity
- A specification of safety requirements
- The results of hazard and risk analysis.
- Details of risk reduction techniques employed.
- The results of the design analysis showing that the design meets all the required safety targets.
- The verification and validation activities.
- Records of Safety reviews.
- Records of any incidents which occur throughout the life of the system.
- Records of all changes to the system and justification of its continued safety.

In addition to those items described above Graham [17] suggests that other areas that may be included are:

- Functional analysis
- Zonal analysis
- Component failure
- System safety analysis
- Human factors analysis.

### 3.1.14 Safety Management System

Another term the engineer will encounter is Safety Management System (SMS). A SMS is the organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet safety requirements and safety policy objectives. An SMS provides the framework for managing safety at all stages of acquisition i.e. from conception to completion of a project and then on to obsolescence or disposal of the system. The SMS is needed to show that all necessary safety activities have been, and will continue to be, undertaken to an adequate standard whatever the nature of the contract. It is important that the SMS is well documented and auditable so that it provides visibility that it is operating effectively. SMS provide a formal, organised process whereby people plan, perform, assess, and improve the safe conduct of work. The Safety Management System is institutionalised through the IPT's directives and contracts to establish the Department-wide safety management objective, guiding principles, and functions.

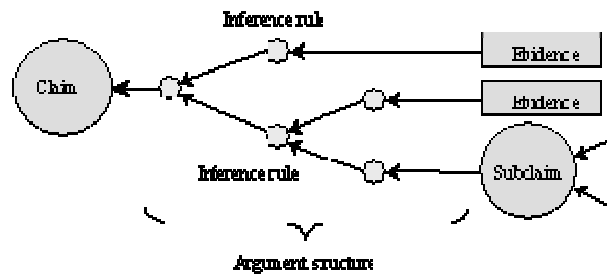
### 3.1.15 Goal Structuring Notation

GSN has been briefly discussed in previous paragraphs. This paragraph expands on that brief explanation and looks at GSN in more detail. The structure shown in the Aviation Safety Case example at Figure 2 uses a technique developed by Kelly [7] called Goal Structuring Notation (GSN). This method of graphical notation is one method that is used to present system safety arguments. Other methods that may be used are Free Text or Adelard Safety Case Development Manual (ASCAD). GSN is a graphical notation that can be used for presenting system safety arguments. Kelly and Weaver [40] describe GSN as:

*..... a graphical argumentation notation which explicitly represents the individual elements of any safety argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument).*

When the elements of the GSN are linked together in a network they are described as a 'goal structure'. The principal purpose of any goal structure is to show how goals (claims about the system) are successively broken down into sub-goals until a point is reached where claims can be supported by direct reference to available evidence (solutions). As part of this decomposition, using the GSN it is also possible to make clear the argument strategies adopted (e.g. adopting a quantitative or qualitative approach), the rationale for the approach and the context in which goals are stated (e.g. the system scope or the assumed operational role).

Adelard also use a graphical notation structure but is represented in a different form called Adelards Safety Case Development Methodology (ASCAD) [39] (see Adelard website for further information). ASCAD uses a "claims-arguments-evidence" motif for representing argument structure - see Figure 9 below.



**Figure 9. A Generic Graphical Argument Using a Claims-Arguments-Evidence Structuring [39]**

Another form of representing a SC is through free text. The following example of a safety argument used by Kelly describes clearly how a safety requirement (P65) has been interpreted and achieved in the system:

*The Defence in Depth principle (P65) has been addressed in this system through the provision of the following:*

- *Multiple physical barriers between hazard source and the environment (see Section X)*
- *A protection system to prevent breach of these barriers and to mitigate the effects of a barrier being breached (see Section Y)*

However, if the text is poorly constructed the safety argument will lose its effectiveness. If the person/s writing the safety argument use poorly constructed English, then it will be very difficult to understand the argument and it becomes ambiguous and unclear. This problem is further increased in large SC's where there will be lots of cross referencing to other evidence and assurances and it becomes a minefield to trace through the argument satisfactorily.

Aircraft and rotorcraft continue to become more complex as technology advances and operational needs dictate the use of more sophisticated weaponry and systems to outwit the enemy and enhance survivability. This coupled with the increased demands of more detailed SC's by certification standards are causing SC's to become extremely large and more concerning, difficult to manage. In many large SC's the large amount of low-level analysis evidence that supports the SC especially for large aircraft can blur the high level argument. As Kelly *et al* [38] point out, in many cases a SC is produced in a purely linear format which also makes it very difficult to structure the high level argument for a SC and to show the relationships with the supporting evidence. Safety should be a key driver in the design of systems. Early safety analysis (for example Preliminary Hazard Analysis) often leads to derived requirements and design decisions. Yet it is difficult to link the results of the early analysis to those requirements and decisions; usually only the hazard log records such information. Taking into account the problems identified in the above paragraphs, the unsafety skilled aviation engineer is going to find it extremely difficult to identify what the effects are on the SC unless the guidance provided is understandable and is also available.

### 3.1.16 Summary

Chapter 3 has looked at what is perceived to be the common safety terms that an aviation engineer may encounter when dealing with the safety question Q6.01a of the SSQ. There is no defined list of contents for a SC but armed with the knowledge of what may be presented, the aviation engineer will be able to investigate what effects the proposed SM design has on the SC. The aviation engineer will be required to make a judgement as to whether the SC is affected and whether any reviews or amendments are required. As a bare minimum the author feels that the following areas should be addressed as a minimum list when considering the requirements of Q6.01a:

- All claims in support of the argument within the SC that will be affected by the modification should be reviewed to ascertain that they still hold true in the current argument that is presented. This will mean reviewing the SC that may be presented in GSN or Free text or other tools

- A review of the Hazard log and whether there are additional new hazards that need to be added due to the affect of the modification. The addition of the new system may also remove some of the current hazards because it improves the system functionality. More importantly the hazards should be addressed to identify required control measures.
- Any maintenance activities that may be incurred that can lead to unsafe procedures and working practices.
- What operational impacts are introduced and how they impact safe operation and flight of the aircraft.
- Does the modification introduce any health and safety risks which must be addressed for operators (e.g. maintainers, cleaners, passengers, pilots and navigators) of the system?
- What are the environmental safety risks associated with the system's construction, operation and disposal?
- Records of all changes to the system and justification of its continued safety.
- Are there changes to the SMS?
- Any risk assessment.

Although not definitive, this list will focus the engineer in the important areas of the SC to be addressed. Each of the areas addressed above are considered to be key to the SC and are the ones that most emphasis should be placed on when reviewing. However, it is only possible for the aviation engineer to address the activities above when he feels he is safety competent, has adequate safety experience and undergone some formal training. The evaluation phase through a questionnaire will address these issues.

## Chapter 4 - Developing and Analysing a Questionnaire

The main aim and focus of this project is the completion of the safety element question Q6.01a within the SSQ. Areas that have been investigated so far have looked at what other guidance in addition to the provided 'Response form' is available to assist the aviation engineer in completing the question. This has looked at:

- Current Standards and what they offer.
- What guidance is required for the engineer to complete the question and how competent they should be?
- Safety terms that may be encountered by the engineer when answering the question.
- Reviews of the SSQ as questionnaires or checklists.
- What other forms of questionnaires are being used either within the military or within industry

The aim now is to develop or identify a guide or process that will aid the engineer in completing the question. Before this can be produced it is important to ascertain what the engineers understanding of safety engineering is. To be able to design the new guidance it is important to establish a baseline of the skills and competencies of the aviation engineers filling in Q6.01a. It was felt that this would be best achieved by developing and sending out a questionnaire to aviation engineers involved with completing SSQ's as part of their primary tasks.

### 4.1 Planning the Study

Planning case studies is not an easy task and having the correct and useable output from the study relies on getting the upfront planning correct. Five general characteristics to providing a case study are provided by Yin [41]. The case study must be:

- Significant.
- Complete.
- Consider alternative perspectives.
- Display sufficient evidence.
- Be composed in an engaging manner.

### 4.2 Basic Process of Survey Research

Burgess [42] suggests that the basic process of survey research can be outlined as follows:

- Define the research aims. What is trying to be achieved?
- Identify the population and sample. Who the intended target audience is.
- Decide how to distribute the questionnaire and collect the replies. By post or electronic services.
- Design the questionnaire.

- Run a pilot survey. Test out the questionnaire before it is sent to the target audience.
- Carry out the main survey.
- Analyse the data. Review the results and assess what the outcome of the questionnaire is.

#### 4.2.1 Define the Research Aims

A crucial part of good research design concerns making sure that the questionnaire design addresses the needs of the research – Burgess [42]. This means that it is important to ensure the questions being asked are the right one. Burgess also states that the move from research aims to deciding what are the right questions to put on a questionnaire are the key aspects to be addressed by the researcher.

In the case of this project the aim of producing this questionnaire was to collect data that could be analysed to ascertain what safety and safety assurance knowledge resides amongst aviation engineers. This is so that a guide or questionnaire with supporting guidance can be formulated to provide the correct information required to answer Q6.01a of the SSQ.

#### 4.2.2 Identify the Population and the Sample

This is probably one of the more difficult areas to satisfy. The successful output of a questionnaire is dependent on the chosen target audience (*population*). Furthermore it is important that the target audience would be willing to respond and complete the questionnaire and would be in the appropriate job positions where SSQ's are dealt with. Technical expertise (including knowledge of Safety engineering) is important but in the case of this report it was not crucial as a wide audience of aviation engineers would be considered.

The author works within the military aviation domain (Army at the time of writing this project) and although directly involved with Army aviation, to give the questionnaire some credibility it was considered that the audience would be as broad as possible. To that end, it was decided that the questionnaire would be surveyed by all three armed Services and by personnel with different responsibilities within the aviation world. These engineers (*sample*) mostly aviation need to be familiar with the SM procedure so the questionnaire will be addressed to engineers within the:

- Rotary world IPT's who review the SM processes.
- Service Modification Teams and Aircraft Trials and Evaluation of Tactics teams within the three armed Services who develop the SM's for both rotary and fast jet aircraft operations.
- Engineering, Development and Investigation Teams who review and write SM's for fleet installations.

This will provide a wide range of knowledge, experiences and competencies when gathering data for the questionnaire.

##### 4.2.2.1 Sample Sizes

Burgess [42] suggests that to determine the sample size it is usual to work back from how many responses (completed questionnaires) are required for the analysis. Due to the limited time of this project it was decided that 20-30 samples would be sent out with an expectation of 15-20 replies. This would allow enough time for the analysis and evaluation phase to be completed.

#### 4.2.3 Distributing and Collecting of the Questionnaire

Once the target audience had been chosen it was necessary to decide whether the survey was to be completed directly or through an interviewer and design the questionnaire and any other documents accordingly. E-mail was the chosen form of delivery and an introductory sheet would be attached to the questionnaire to explain the rationale behind the questions and why its completion was of value. The cover sheet would also

detail how the questionnaire was to be completed and finally details of how to return the completed questionnaire to the author i.e. by hard copy or e-mail – see Appendix A.

#### 4.2.3.1 Self-Administered Questionnaire

It was decided to use a self-administered questionnaire which would be distributed electronically by e-mail. However, using this method of questioning relies on the respondent to complete the questionnaire which has implications for ensuring the design is correct. If a questionnaire is interesting, respondents are more likely to commit to answering it and also if it is of value, where possible short, clearly thought through and well presented. Another implication is that of the questionnaire being too difficult to complete. If it is pitched too high above the perceived level of the knowledge of the respondent/s then uncompleted questionnaires will be returned. If it is pitched too low then a successful evaluation may not be possible. A poor quality questionnaire will yield poor quality data.

The questionnaires were sent to known individuals within military aviation engineering who hold different positions of responsibility when it comes to dealing with the SM documentation and in particular the SSQ. The range of respondents used was:

- Team leader of an Engineering and Development Investigation Team (EDIT).
- IPT desk officer's from within the Rotary world.
- An under training Safety engineer from ARC IPT.
- Aviation engineers within the DO domain responsible for compiling SM's for Rotorcraft both Army and Navy.
- Aviation engineers engaged in compiling SM's for trials purposes on fast jet aircraft.

A total of 30 questionnaires were distributed and 12 returns were received. Respondents had the option of anonymity by omitting their names from the questionnaire.

### 4.3 **Design of the Questionnaire**

Pitching the questions at the correct level of understanding for the given target audience is important. Burgess [42] proposes that the design of the questionnaire can be divided into three elements:

- Determine the questions to be asked
- Select the question type for each question and specify the wording.
- Design the question sequence and overall question layout.

#### 4.3.1 Determine the Questions to be Asked

At this stage it is worth reminding what a questionnaire is?

A questionnaire is a tool to obtain data for analysis purposes. It is:

- A set of specifically designed questions to which answers are written on a prepared form.
- It describes who the target audience may be in demographic terms.
- It is a way of finding out exactly what the target audience knows and needs to know about the topic.

- It contains up to date data which is not available from any other source.

Burgess [42] proposes that a key link needs to be established between the research aims and the individual questions via the research issues. Issues and questions can be determined through a combined process of exploring the literature and thinking creatively.

It has already been established in Chapter 2 – Literature Review that there is little useful published guidance for completing question 6.01a of the SSQ. Through the author’s personal experiences it is surmised that there is little safety knowledge amongst the aviation engineers who are involved with SM process and completing or reviewing the SSQ.

#### 4.3.1.1 Questionnaire Design

The questionnaire assumed that the respondent had little if no knowledge of safety and safety assurance and was designed in four sections:

- Section 1 – General questions.
- Section 2 – Safety Case and Safety Management System questions.
- Section 3 – Safety and Support Questionnaire (SSQ) questions
- Section 4 – Tools questions.

The questions have been directed towards the safety terms and definitions identified in Chapter 3. They were as follows:

- |                             |  |
|-----------------------------|--|
| • ALARP                     | • Risk                                 |
| • Aircraft Release          | • Safety                               |
| • Airworthiness             | • Safety Case and Safety Case Contents |
| • Aviation Safety           | • Safety Critical Systems              |
| • Certificate of Design     | • Safety Management System             |
| • Goal Structuring Notation | • Safety Related System                |
| • Hazards                   | • Severity                             |

It was also decided that questions would be asked specifically regarding; standards, the SSQ and Tools.

A mix of question types were chosen; open vs. closed, multiple responses and ranking. On the whole, closed-format questions were used although there are some open-ended ones. Spaces under the questions were supplied for the respondent to include additional comments as appropriate. These comments can be valuable and more often than not provide useful information towards the analysis that has not been considered in the question. These comment areas also allow for a respondent to extend the answer to the questions.

#### 4.3.1.2 Wording of the Questionnaire

Burgess [42] gives guidance on the decision on the question wording. He suggests that question wording should follow these general rules:

- Be concise and unambiguous.
- Avoid double questions.
- Avoid questions involving negatives.
- Ask for precise answers

- Avoid leading questions

Overall questions should be brief, clear, concise and unambiguous. The use of jargon words should be avoided as they may elicit an informed response.

Ratings were used for respondents to describe or indicate their levels of experience, confidence and knowledge. These areas were rated as follows:

- **Experience**
  - Experienced
  - Adequate experience
  - Little experience
  - No experience
- **Knowledge**
  - Excellent knowledge
  - Adequate knowledge
  - Little knowledge
  - No knowledge
- **Confidence**
  - Fully confident
  - Reasonably Confident
  - Not very confident
  - Not confident at all
  - Not sure

When producing the questions it was important to keep wording, standards and terminology consistent and as already discussed, clear.

It was decided that general questions regarding the respondent be used to open the question sequence in the questionnaire. This was deemed to be the most appropriate thing as it would settle the respondent in to answering the questions. It is easier to answer a question which is based on something you know. These questions also raise interest within the questionnaire and should ensure the respondent completes it. It was also important to logically set the questions grouping like and similar types together.

#### 4.3.1.3 Examples of Questions Used

Due to the number of questions asked within the questionnaire, sample questions will be discussed and like for like questions will be used.

##### ***Question 2***

<i>Do you write Service Modification(SM) leaflets?</i>		(✓)
Yes		
No		

It is intended that the respondent will treat these types of questions as a series of independent dichotomous yes/no questions.

**Question 3**

(✓)

<i>Which statement best describes the Service Modification experience you had before taking up your present position?</i>	
Experienced in service modifications	
Adequate service modification experience	
A little service modification experience	
No service modification experience before this role	

**Question 9**

(✓)

<i>Please indicate your level of confidence in your ability to identify hazards, assess likelihood and severities and allocate tolerabilities.</i>	
Very confident	
Reasonably confident	
Not fully confident	
Not confident at all	

The above closed-format style of questions Q3 and Q9 should elicit one response i.e. the answers form mutually exclusive categories. This type of question format was chosen mainly for areas that questioned the respondents experience, confidence and knowledge.

**Question 10**

<i>Please explain what you understand the following terms to mean?</i>	
Airworthiness –	
Safety Case –	
Human Machine Interface –	

This is an example of one of the open-ended format questions used. It was decided to use this format as it would elicit a range of replies of varying length and articulation. It would also allow for precise judgment of the respondents knowledge. However, that said, the answers to this question would vary; there would be text book answers where the respondent has used reference material to find the answers and there would be answers provided that would be the respondent’s personal knowledge of the topics. It was felt that identifying the two types of answers would be fairly evident.

**4.3.1.4 Questionnaire Format - Section 1 Questions**

In Section 1 of the questionnaire, respondents were asked to indicate their experience in dealing with the SM process, the SSQ and what their knowledge and understanding of safety and safety assurance was. It also attempted to elicit what knowledge of airworthiness and human factors they had and was achieved by asking questions in these areas. This section was used to set the basis for the questionnaire and question types were intended not to be too hard to complete.

Answers would allow the evaluator to assess the type of person answering the questionnaire and give an indication as to what their experiences, competencies and knowledge are. Questions 1 to 5 asked questions relating to the respondents experiences and responsibilities with regards to the SM process and the SSQ.

Questions 6 to 9 asked general questions on the respondent's knowledge of safety engineering and how confident and competent they are in answering questions on safety. Question 10 focused in on the knowledge of the respondent regarding airworthiness, safety case and human machine interface. These are three specific areas dealt with in the SSQ.

Question 11 asked the respondent to describe what they thought is the difference between a safety critical system and one that is safety related. This question was asked as it is important for the aviation engineer to differentiate between the two meanings so that they are able to identify as to nature of the system they are introducing as a modification and what type of other system the modification will affect. Dependant on the system introduced may have an impact on how reviewing the effects on the safety case are dealt with.

Question 12 was a question more directed at where safety responsibilities should be defined in the respondents' working environment and would define the safety culture within that department.

#### 4.3.1.5 Questionnaire Format - Section 2 Questions

Having investigated the respondent's responsibilities, knowledge, experiences and competencies in Section 1, this section is intended to elicit knowledge of the SC and SMS in order that an assessment can be made as to what information would need to be provided to the un-safety skilled engineer in order that they are able to answer Q6.01a of the SSQ. Many of the questions in this section are based on the prepositions of the discussions of Chapter 3. Although it was ascertained that there is no definitive list of exactly what the contents of the SC are because they are system and platform specific. The minimum lists of elements to be checked as the contents of a SC are detailed in Chapter 5 for evaluation.

Questions 13 to 16 asked the respondent specific questions regarding the SC, what its contents are, what is an SMS and what its contents are. Question 17 asks who the SCM is for the platform/s that the respondent deals with. Answers to these questions would derive the requirements for the amount of guidance that needs to be provided to steer the aviation engineer when considering what effects there are on the SC by the introduction of the modification.

It was deemed appropriate that questions regarding the RTS and RTSA were asked and this is catered for by questions 18 and 19. The reason for this is, is that the RTS is the regulatory certification to allow the aircraft to fly in the 'as flown' configuration (refer to Chapter 2) and without the RTSA addressing this, area the aircraft will not fly. The RTS is based on the platform SC and follows that as the aviation engineer has been questioned on the SC the next was to question knowledge of the RTS and the RTSA. Questions 20 and 21 questioned the respondent's knowledge of ALARP and the difference between a hazard and an accident.

#### 4.3.1.6 Questionnaire Format - Section 3 Questions

Section 3 covered the use and knowledge of Tools. Under the heading 'Tools' included the procedures, processes, methods and other aids the respondent uses to populate the SSQ. It also questions the use of check listing and the respondent's knowledge of hazard logs. The aim of this section was to elicit information from the respondents what 'Tools' if any, are used and to discover if any other means are used. GSN was included as a tool and the respondent was question as to whether they used anything similar to GSN or had used any other tools for SC work.

Questions 22 and 23 questioned the use of GSN and the respondent's familiarity with the term and whether they had encountered the use of any other similar methods i.e. ASCAD, Text based SC's. Questions 24 to 26 asked the respondents what procedures, processes, methods and other aids including check lists the respondent used to populate the SSQ and q6.01a. Information from this area would allow the evaluator to assess whether there was a chosen tool that was used and could be developed or whether one would need to be developed. It would also establish whether there were forms of procedures, processes and standards being used.

Question 27 was specific to the Hazard log and information supplied as an answer to this question would establish the respondents understanding of hazard logs and what they are used for.

#### 4.3.1.7 Questionnaire Format - Section 4 Questions

These questions were directed towards the Safety and Support Questionnaire. The intention of the questions was to elicit information on how the respondents approach the SSQ and complete question 6.01a. In particular the questions attempt to elicit information to build up the bigger picture on how the respondent/s approach the design of a new project, whether a feasibility study is carried out, scenarios are used to define any safety requirements and how they elicit information for safety requirements.

Questions 28 to 32 'requirements' gathering type questions covering feasibility studies, the use of scenarios to derive safety requirements, safety critical requirements settings and hazard analysis. These particular questions were asked because it is felt that as a minimum, with some clear guidance, the respondent could attempt some early PHA with respect to their design. It could be argued that without good training in Safety analysis and assurance techniques it may be difficult to define safety-critical requirements. This question may be outside the scope of the questionnaire and its worth will be commented on in the evaluation part to this project.

More general questions were asked in questions 33 to 36 relating to how helpful the respondent found the guidance supplied in the 'Response' form. It was anticipated that the answers would vary considerably here and would be dependant on the experiences and competencies of the aviation engineer. It is this area that this project is aiming to develop and expand.

Questions 37 and 38 questioned what the respondent thinks are the inputs and outputs of question 6.01a of the SSQ and 39 to 41 finishing the questionnaire by asking in an open format style question what assistance or guidance the respondent would like to help/aid in answering question 6.01a of the SSQ. The purpose of this question being that it was hoped that it would capture any other data that had not been covered in the questionnaire.

It was felt that the questionnaire covered all areas regarding safety analysis, completing the SSQ and what the respondent's responsibilities are to enable sufficient data to be gathered and formulate a new guidance following data evaluation. However, it was possible that there were too many questions in the questionnaire and this would also be assessed in the evaluation section of this report.

A small pilot survey was carried out using work colleagues of the author to ensure that all questions could be answered and the questionnaire was understandable. Following this successful mini-trial, the next step was to distribute the questionnaire. A four week period was given for completed questionnaires to be returned.

## Chapter 5 - Evaluation

The first aim of this chapter is the evaluation of twelve completed and returned questionnaires which are the resultant returns from thirty identical questionnaires that were distributed to a target audience of aviation engineers who are responsible for populating and reviewing a SSQ in support of a SM. The questionnaire was distributed to gather data from respondents on their knowledge of safety and safety assurance and to gain a measure of what additional support is required to assist the aviation engineer in completing Q6.01a of the SSQ. This problem of insufficient guidance/documentation being available to support the aviation engineer in answering fully the safety element question Q6.01a of the SSQ was identified as part of the literature study performed in Chapter 2. This has meant in the past, incomplete answers being provided for Q6.01a and in most cases the onus of addressing the requirement has been passed to the relevant IPT who as part of the SM process are required to review the SSQ. It was also identified that it is possible that the aviation engineers completing the SSQ and subsequently Q6.01a are not safety trained, do not have adequate safety skills and competencies and are not confident to answer the question. This is also evaluated in this chapter.

The second aim of this chapter is to evaluate from the findings in the above paragraph whether it is possible to produce a form of supporting tool, which provides the aviation engineer with the concise guidance he requires so as to be able to fully complete the requirements of Q6.01a. This tool may come in the form of; a checklist, flow chart, another questionnaire addressing just the requirement of Q6.01a or concise and accurate guidance and documentation on how to complete Q6.01a. This additional support is proposed to be used with the already supplied SSQ 'Response' form. It will also be assessed from the findings of the evaluation on how to better the aviation engineers safety competencies and how the necessary skills and knowledge to be able to complete Q6.01a fully can be delivered.

Due to the number of questions in the questionnaires, only a sample of completed question's are evaluated for each question asked in the twelve returned and completed questionnaires. For anonymity reasons, all the respondent's names have been omitted from the answers shown.

### 5.1 Summary of Completed Questionnaires

As was discussed in Chapter 4, thirty questionnaires were sent out to known respondents and twelve completed questionnaires were returned. The following table shows the number of questions answered by each respondent.

	RESPONDENTS											
	1	2	3	4	5	6	7	8	9	10	11	12
Q1	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Q2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q5		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Q6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q15	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Q16		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Q17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q20		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q22		✓	✓		✓	✓	✓		✓	✓	✓	✓
Q23	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Q24	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Q25			✓	✓	✓	✓		✓		✓	✓	✓
Q26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q27	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Q28	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Q29	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Q30	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Q31	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Q32	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q33	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q34		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Q35	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Q36		✓	✓	✓	✓	✓	✓				✓	✓
Q37	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
Q38		✓	✓	✓		✓	✓	✓		✓	✓	✓
Q39	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Q40	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Q41	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

**Table 4. Questions Answered By Each Respondent**

Although the returns on the questionnaires were disappointing, less than 50% of those sent out, answers to the questions were very frank, concise and extremely informative. An early observation on the questionnaire which may be due to a bit of short-sightedness in the questionnaire design was the lack of apportioning a ranking to the rating type questions, for example; question 6 asks the respondent to indicate what Safety Engineering experience they had before taking up their current position. The answers to this question were given in the following rating format:

- Experienced in safety engineering
- Adequate safety engineering experience
- A little safety engineering experience
- No safety engineering experience before this role

This therefore meant a quantitative assessment of the data could not be made. A few respondents also chose to add comments to this type of question so a qualitative approach to analysis has been made to evaluate the answers. A quantitative analysis would have meant it would have been possible to derive summary statistics that would potentially measure an overall experience level of the respondents. Also by using quantitative analysis, summary scores could be obtained by pooling across different questions related to the same issue.

### 5.1.1 Initial Observations

In the Questionnaires that were returned answers were supplied to a total of 458 questions from a possible 492 representing 93% of the questions asked in 12 questionnaires. These answers represent a very high proportion of the questions asked and can be seen in Table 4. It was also felt that this number of answers for this many questionnaires were very comprehensive and indicated a high degree of engagement by the respondents. Respondent 9 answered the least questions as the job position he fulfils is to review safety cases rather than write SM's and complete the SSQ.

### 5.1.2 Evaluation of Section 1 – Questions 1 To 12

In this section and the subsequent evaluation sections a number of questions from each section of the questionnaire are considered. The implications of the responses for each question are evaluated against the problems indicated in the introductory paragraphs of this chapter. Observations at the Section level are presented in section 5.2 and a summary of the overall implications of the survey on the proposals put forward in this project are presented in Section 5.3.

#### 5.1.2.1 Question 3 Respondents were asked in question 3:

*'Which statement best describes the Service Modification experience you had before taking up your present position?'*

From the twelve replies the following details were indicated:

	<b>Number of Respondents</b>
Experienced in service modifications	4 (Note 1)
Adequate service modification experience	2
A little service modification experience	4
No service modification experience before this role	2 (Note 2)
Note 1 – Resp 2. 17 years of writing SRIMS and SEMS	
Note 2 – Resp 5. All my experience was picked up from reading the JAP, whilst producing a draft SM leaflet for the IPT's	

A third of respondents indicated they were experienced in SM's with the most experienced respondent indicating 17 years of experience gained writing SRIMs and SEMs. At the other end of the rankings, a sixth of respondents indicated they had no previous SM experience with Resp 5 stating that they had gained all their experience through reading the JAP whilst compiling draft SM leaflets. Half of all respondents indicated they had little or no experience and half had adequate or were experienced in SM's. In general these answers conformed to expectations when considering the target audience and are a proportional spread of the anticipated experiences.

#### 5.1.2.2 Question 4 Respondents were asked in question 4 whether they were required to populate the SSQ as part of their responsibilities. If they answered 'yes', question 5 asked the respondent:

*'If you answered 'yes' to the previous question, how confident are you that you are sufficiently competent to populate the SSQ?'*

	<b>Number of Respondents</b>
Fully confident	1 (Note 1)
Reasonably confident	5 (Note 2)
Not very confident	2
Not sure	
Note 1 – Resp 7. Do not populate SSQ, but however, am involved in review of content	
Note 2 – Resp 5. I feel competent through experience to populate some of the areas, but not qualified.  Resp 10. As you will be aware the SM 2 is a live document and changes throughout the course of the SM as more evidence, F100's, manufacturers Safety cases, Design Authority comments and QinetiQ advice becomes available.	

It can be seen that for those that answered this question, the majority indicated they were reasonably confident in their competencies to populate the SSQ. This number represents just under half of those questioned. It was interesting to see that Resp 2 who had indicated the most experience with regards to service modifications in question 3, indicated he was only 'reasonably confident' in populating the SSQ. This is difficult to understand as the expected answer here would be to assume this person is fully confident because of their experiences. However, experiences do not necessary dictate the person's competencies and without appropriate training these competencies may not be achieved or retained. Alternatively, the respondent may be erring on the side of caution and may feel that there are areas in the SSQ where they are able to answer questions confidently and other areas where they are not so confident. This is reflected in the answer provided by Resp 5 (note 2) who in their answer identifies that they feel confident due to their experiences but do not feel qualified (adequate training). Resp 2 may also believe the SSQ is ambiguous and therefore he is unable to complete it fully. It may be possible to establish which of the authors thinking on Resp 2 answers is true by assessing other answers provided by the same respondent and assess their content. However, this reiterates the findings of the literature survey and that there is not enough guidance provided in the SSQ to enable the respondent to form a concise and accurate answer for the question. It also identifies that those completing this element of the SSQ are not adequately trained in safety.

Resp 10 provided a totally obscure answer which appears to indicate that the question was not read properly. What is interesting though about his answer and although not related to this question is that Resp 10 has also indicated that he sees the SSQ as a living document. This was identified during the Literature Review in Chapter 2 and further demonstrates that much like the SC which is a living document so potentially is the SSQ.

### 5.1.2.3 Question 7 Question 7 asked respondents:

*'How confident are you that you are sufficiently competent to answer questions on Safety Engineering?'*

	<b>Number of Respondents</b>
Fully confident	1 (Note 1)
Reasonably confident	6
Not very confident	5 (Note 2)
Not sure	
Note 1 – Resp 1. This respondent is employed in a position where he reviews SSQ's and authorises the release of draft SM's compiled by his engineering team.	
Note 2 – Resp 2. Courses to give paper qualifications would be required to enhance the detailed aspects of Safety Engineering over that gained from experience of working on the subject.	

This was considered to be a key question in the questionnaire as the level of confidence an engineer has in his/her competency will influence the quality and depth of the answers provided to safety engineering questions within the SSQ. 50% of the respondents indicated they were reasonably confident, with 44% indicating that they were not very confident. Resp 1 has previously worked in IPT's that reviewed SEM's and STF's and would have come in to contact with safety engineering matters a lot more than most of the respondents who answered this questionnaire. That said, he does make comment in an accompanying e-mail that he thought he knew all the answers but would go away and review exactly what he does know. Resp 2 indicates that experience alone is not enough to provide the necessary competence and some form of formal training (paper qualification) is required to support this. It must be remembered at this point that none of the respondents are employed in safety specific roles.

#### 5.1.2.4 Question 8 In question 8 the respondent was asked:

*Do you consider that other persons without an explicitly defined safety role are competent to populate the SSQ?*

The purpose of this question was to invite the respondent to indicate whether they felt that any person who does not have specific safety roles could complete the SSQ. This question refers out to comments made by Graham [17] (Chapter 2) where he suggests that a person with an engineering background should be able to complete the SQ for an SEM although the author argues that this is not the case for the SSQ. In the context of this question 'competent' is used to describe a person's experience (platform), skill or ability to populate the SSQ based on aviation engineering experiences and knowledge alone. It questions whether to be competent to populate the SSQ, the person must be safety trained, have safety experience (preferably aviation), have platform experience and knowledge, and whether they need to be system conversant.

	<b>Number of Respondents</b>
Yes	3 (Note 1)
No	3 (Note 2)
Not sure	6 (Note 3)
<p>Note 1 - Resp 2. Provided they are aircraft engineered trained and that in the format of the SSQ is at present. Any uncertainties they have should be indicated as further investigation required during the SM process. This would be for those subjects they are inexperienced at i.e. Mechanical person commenting on Electrical aspects and vice versa.</p> <p>Resp 11. If that person is deemed competent on the main system / platform that the system that the SSQ pertains to is to be fitted, then I feel that they should have sufficient knowledge to adequately populate the SSQ.</p>	
<p>Note 2 - Resp 4. I think personnel making these decisions should be fully qualified to populate the SSQ</p> <p>Resp 5. The person should be suitably qualified or attained</p>	
<p>Note 3 - Resp 8. Would depend on the individual and their previous experience.</p> <p>Resp 9. A lot depends on their capabilities, background and understanding of Military procedures and understanding how an aircraft operates.</p>	

A third of respondents support Grahams theory and in particular both respondents 2 and 11 propose that as long as the engineer is well versed and experienced on his platform, then there should not be a problem. This is further supported by Resp 8 and 9 in the 'not sures' who make similar comment to Resp 2 and 11. However, Resp 2 does go on to indicate that although he feels an engineer with appropriate platform training

can answer these questions they are trade specific, it would therefore be difficult for someone with a mechanical engineering background to answer electrical/avionic type questions satisfactorily.

**5.1.2.5 Question 10** The purpose of this question was to elicit the respondents interpretation of the following three engineering terms; Airworthiness, Safety Case and Human Machine Interface. These are three of the main categories of the SSQ and form the heading for many sub-topics. Airworthiness and safety are often treated in the same light and it was considered that the engineer should be able to differentiate between the different terms. These terms are explained in Chapter 3 and an attempt is made to define what they mean in the context of the SSQ. A sample of answers is shown below:

*'Please explain what you understand the following terms to mean?'*

- Airworthiness
- Safety Case
- Human Machine Interface

Resp 1

Airworthiness – The fitness for flight of an aircraft so that it does not endanger its crew, passengers or anybody on the ground (the only exception being the enemy we may be *****).
Safety Case – The document that justifies the airworthiness of the aircraft based upon qualification evidence.
Human Machine Interface – The interaction between the user and a piece of equipment.

Resp 3

Airworthiness – A statement that the item in question is deemed to have as low a risk as practicable to the aircraft or user.
Safety Case – An in depth study on the impact of a proposed piece of equipment on to a platform. Providing risk assessments and documented evidence
Human Machine Interface – Something that is directly operated by, or requires input from a person or persons. I.E. frequency selector knobs on a radio.

Resp 9

Airworthiness – The state or condition where an aircraft is deemed serviceable to fly within its design criteria or Military Aircraft Release to Service. The ac must be 'fit to fly' or maintained in a 'serviceable' condition to be able to undertake the tasking placed on it.
Safety Case – A robust report detailing all the aspects, and if applicable underpinned by a number of assumptions, to state that an aircraft meets its System safety Criteria.
Human Machine Interface – A Pilot/Co-Pilot. A person in control of an aircraft.

## Resp 11

Airworthiness – Ensuring the ability of an airborne platform to fly with the minimum of risk to its occupants or any person underneath its flight-path.
Safety Case – A body of evidence which forms the basis of a structured argument that a system is safe to maintain and operate with any identified risks being reduced to ALARP.
Human Machine Interface – Those parts of a system which require input from an operator to ensure satisfactory operation.

Most respondents provided similar answers to this question with some offering near text book solutions (these have not been included) to the definition given in Chapter 3. Resp 3 provided an interesting answer which appears slightly confused with the meaning of ALARP. Resp 9 appears to have misunderstood the question and talks about the serviceability and maintenance of an aircraft and its fitness for flight within the design criteria. This is directed more towards the RTS and he talks about a ‘state’ or ‘condition’ of the aircraft. Of the examples used, two respondents indicated that airworthiness should also consider the general public and the other two respondents did not. This was a similar split in all the answers provided.

Comparing all twelve respondents’ answers to the definition provided in Chapter 3, most indicated some knowledge of what a SC is. Resp 1 also recognises that a SC is part of the supporting evidence that is provided as part of the RTS.

A varied amount of answers were provided for the meaning of HFI and again most had some knowledge as to what was meant by this term. This highlights a lack of understanding of the meaning and it would be appropriate to consider the aviation engineer undertaking some form of safety training course such as Safety System Engineering (York University). This would better arm the respondent with the knowledge to answer this question more fully and accurately. This further supports the argument that the aviation engineer should have received some formal safety training to make him more competent in answering Q6.01a of the SSQ.

**5.1.2.6 Question 11** It is felt that the aviation engineer should be able to differentiate between a safety critical system and a safety related system as they are treated differently when providing safety analysis and assurance assessment. If the status of the system or the system/s affected by the new design is not identified early in the design process then there is potential for this scenario not be addressed at all or until the SM is passed to an independent agency for safety analysis. Question 11 asked:

*‘Please explain what you think the difference is between a safety critical system and a safety related system?’*

The following answers were provided:

## Resp 2

Answer: Safety Critical if it failed would cause a disaster. Safety related system, if it fails would produce problems. i.e. failure of AFCS is Safety Critical, failure of a radio is loss of facility. But loss of an Air Traffic Control radio at a particular time could be construed as Safety Critical. Therefore not only the system needs to be considered but how and when it is used.
---

## Resp 3

Answer: A safety critical system is something that if it fails will have catastrophic effects on either the larger system or persons operating it. A safety related system is something that operates to maintain the safety of the system it is attached to or monitoring.
--

#### Resp 4

Answer: If the system is Safety Critical, any fault in the system could have catastrophic and/or fatal consequences. If the system is safety related a failure could result in an incident but not necessarily a catastrophic and/or fatal accident.

#### Resp 8

Answer: Safety Critical System – A system where human lives may be put at risk  
Safety Related System – A system whose failure to function in a safe manner may result in human injury or fatality.

#### Resp 9

Answer: Having had no formal safety training as yet for my post, my answer is based purely on in-service knowledge gathered over 29 year's service.

Safety critical system: An aircraft system ie;Hyd's/Ejector Seat/Transmission/Lubrication etc, that if lost can seriously affect the way in which an aircraft is flown.

Safety related system: Safety related system are there as a back up or can be used alongside the prime or critical system. NB This answer is a 'best guess' - not wholly sure.

The former part of the answer supplied by Resp 9 is typical of the situation aviation engineers find themselves in an MOD environment, and is more so for military persons. This is a good example of where the requirement for appropriate training to be able to perform the job responsibilities is required. Although Resp 9 indicates he has 29 years of in-service knowledge, much of that knowledge is now irrelevant for the platform and systems he is expected to deal with. This is because of the advances in technology and the environment he now finds himself within the military are completely different to the ones in which he has been trained previously. In general the respondents have been able to define some of the differences between the two forms of systems. However, Resp 3 is more specific in his identification of those affected unlike the definition given in Chapter 3 which encompasses all human beings. The two definitions provided by Resp 8 are very similar in their intent and it appears that there is some confusion between what each of the questions asked.

#### 5.1.2.7 Question 12 Question 12 asked;

*'Are responsibilities for system safety well identified within your organisation?'*

	Number of Respondents
Yes	7 (Note 1)
No	5

Note 1 – Resp 11. Although I have answered Yes to the above question, it is actually not that clear cut. The reason being is that responsibilities are detailed within the JAP but they are not expanded upon and cited within the Job Spec of individuals. Therefore, this could lead to scenarios where someone understands the responsibilities but may not fully realise that they are their responsibilities.

Those that answered 'yes' to this question are mainly employed in departments such as IPT's where there is a requirement for system safety responsibilities to be detailed in the SMS. However, those that answered 'no' have a tendency to work in DO's where system safety is treated very much as a bolt on. Resp 1 notes that even though employed in a DO and conforming to the requirements of the JAP, the responsibilities are not clear. It is not uncommon that much emphasis on detailing responsibilities for system safety is directed at DLO and DPA departments and the fringe DO's tend to be left out.

### 5.1.3 Evaluation of Section 2 – Questions 13 To 21

This section of the questionnaire looked at Safety Case and Safety Management System Questions. The following answers were provided.

#### 5.1.3.1 Question 13 Question 13 asked:

*‘What is your knowledge of Safety Cases and what they are used for?’*

	Number of Respondents
An excellent knowledge of Safety Cases	
Adequate knowledge of Safety Cases	4
A little knowledge of Safety Cases	8
No knowledge of Safety Cases	
<i>Safety cases are used: (Sample of answers provided)</i>	
Resp 2 - To assess a system with a view to clear its use taking into account all risks and hazards are deemed to be as low as possible.	
Resp 4 - To provide safety advice for the Military Aircraft Release (MAR) or Release To Service (RTS) document which is required when any new aircraft or system is brought into Service.	
Resp 6 - To produce evidence that a system is safe for a given application in a given operational environment	
Resp 9 - To document or show evidence that the aircraft/platform is operation safely within its intended aim/envelope.	

Two answers were required for this question which probably questioned the design of the questionnaire (discussed later). However, it was felt that concise information was received here as this is the key element of the SSQ. There are several definitions of what a SC is provided in the literature but minimal literature is provided on dealing with the contents. 66% of respondents indicated they had little knowledge of SC's. This came as no surprise as most DO's especially within the military do not come into contact on a day to day basis with SC's and until recently there has been little emphasis on the requirement to do so.

The SSQ asks; State the effects on the Safety Case, the required changes and associated actions. In Chapters 2 and 3 it was established that there was no exact defined contents of a SC and an attempt was made in the context of this project to define what elements the engineer should address. Question 14 attempted to elicit from the respondent what they thought the contents of a SC are.

#### 5.1.3.2 Question 14 Question 14 asked respondents to:

*‘Please explain what you think are the contents of a Safety Case?’*

- To be able to evaluate this answer the example SC contents described in Chapter 3 section 3.1.15 were used.

The following answers were provided:

##### Resp 1

Answer: Safety critical and safety related information with reference to the qualification data and mitigating maintenance activities.
--

Resp 2

Answer:  
Design requirement criteria.  
Risk analysis  
Hazard analysis  
Test reports/results

Resp 3

Answer:  
What the intended use for the item is.  
What systems will it interact with?  
What impact will it have on those systems?  
What the impact of catastrophic failures will be on the systems it interacts with.  
What the impact of partial failures will be on the systems it interacts with.  
Does the item meet current safety regulations for the situation it is intended for?  
Recommendations.

Resp 4

Answer: Effects on airworthiness i.e. EMC, Armament, Structural, Stress, C of G, Changes to Electrical Systems, TEMPEST, operation and handling.

Resp 6

Answer: Documentation providing evidence that a system is safe. It will include:  
All applicable legislation, regulations and standards to be applied.  
Hazard analysis.  
Risk management processes  
Safety arguments.  
Safety case reports and Safety statement.

Resp 7

Answer: The contents of the safety case is the documentation set which proves the safety of a system, as an example such documentation could include:-  
  
Hazard log.  
Statement of Operating Intent and usage.  
Test reports.  
Configuration management plan.  
Modification Record Index – Equipment build standard.  
Technical Documentation.  
Operating manual - limitations as to use etc.  
History of incidents – Air Incident Signals etc.  
History of Technical Instructions.  
Etc, etc.

It was difficult to define the exact contents of a SC when carrying out the literature review in Chapters 2 and 3 - the answers above highlight that difficulty even more. However, for this evaluation the example provided in Chapter 3 section 3.1.15 was used as the measurable quantity. On the whole most respondents indicated some knowledge of the SC contents measured against the given example. It is important for the aviation engineer to understand what elements they may have to deal with in a SC accepting that these elements are platform specific and may also have a dependency on who wrote the SC in the first instance. The presentation of the SC may also contribute to this factor and understanding GSN or similar Goal, Claims, Argument, Evidence type presentations will also determine how the aviation engineer deals with the SC.

It is evident from the respondent's answers there are varied understandings as to what constitutes the exact SC contents. It is felt that although the answers are varied it may not necessarily mean an inadequate understanding on the part of the respondent. There are many definitions and versions given in available literature as to what constitutes the SC contents and which are most definitely not prescriptive by any means. With so many variants provided it is possible to see why it can be so confusing for the respondent to decide which one is correct.

**5.1.3.3 Question 18** The RTS was described and discussed in Chapter 2 – Literature Review and was shown to be the final phase before the platform was given assurance that it was safe to fly in the 'as flown' configuration, following the changes brought about by the addition of the SM. The RTS was shown as being the release document which gives authority for Service regulated flying. The RTS is derived from the initial Release To Service Recommendation (RTSR) or MA Release but includes a safety justification of subsequent changes. The RTS is required to be supported by a SC and this uses as its baseline the SC supporting the MAR with additional documented safety justifications for Service changes to the design or changes to the limitations promulgated in the MAR.

As this was an important output of the SM process and which is an input regarding the SC, it was deemed necessary to illicit whether the engineer was familiar with the RTS and what it stands for. Question 18 provided the following answers:

*'Please explain what you think the Release To Service document is?'*

Resp 3

Answer: A statement that all evaluations and independent testing has been carried out. It provides documented evidence to that effect. Concluding that this item is of little or no risk to the user and is therefore cleared for use on this platform.

Resp 6

Answer: A document authorising the use of an aircraft in a defined configuration for a defined operational usage and including any limitations imposed.

Resp 7

Answer: The Release to service document is the main body of evidence forming the basis of the safety case for an airborne platform. The RTS comprises two main elements:-  
MAR – Which identifies the build standard and limitations as cleared by the Design Authority.  
Service Deviations which authorise the use of additional equipments which are not cleared/recognised by the DA.

Resp 9

Answer: Those elements of trial or changes to the design of the aircraft which affect the way in which it is operated. The R to S is written for both the Engineers and aircrew directly, as it makes those people that need to know the capability and changes of the original 'base-line' ac.  
The R to S is a controlled document, containing signals on any deviations their operating parameters and limits to the platform.

Resp 7 provides an answer that is confused and suggests the RTS is the main body of evidence forming the basis for the SC.

**5.1.3.4 Question 20** Another term that is consistently used in system safety engineering is that of 'As Low As Reasonably Practicable' (ALARP). Respondents were asked in question 20 to indicate what they understood the term to mean.

*'Please explain what you think the acronym ALARP stands for and how is it used?'*

The responses expected were:

- As Low As Reasonably Possible
- Not sure
- Do not know
- As Low As Reasonably Practicable
- As Low A Risk As Possible

Resp 2

Answer: As Low As Reasonably Possible.  
Assessing the requirement of the new system against the known possible problems/hazards.

Resp 3

Answer: As Low AS Reasonably Practicable.  
It is used as a justification for the safety of an item. Some items have an inherent risk and to reduce that risk to nothing would expend too much money or time top make the item practical. In this case the statement is that the risk is ALARP.

Resp 7

Answer: ALARP – As Low As Reasonably Practicable. ALARP is a term used in risk management which applies when all necessary actions have been taken to ensure an identified hazard has been mitigated as far as possible. Decision as to whether a hazard has been reduced to ALARP is usually taken through analysis of the residual risk balanced against the costs associated with reduce that risk any further.

Resp 10

Answer: As low A Risk As Reasonably Possible

Two respondents did not answer this question as they did know what the acronym ALARP meant and of the remaining ten respondents, four described the acronym correctly and the other six did not. Resp 10 provided an answer that had not been anticipated. Although a frequently used term in safety fraternity, it is not a term that the average aviation engineer may have to deal with. However, it does raise some concerns that if the engineer who is proposing the design for the SM does not correctly understand this term then how is it possible for him to assess the Risk associated with his design and provide mitigation as appropriate. If he does not know what ALARP means then how does he provide any justification that his system is ALARP.

**5.1.3.5 Question 21** Following on from the ALARP question, question 21 asked the respondents to explain what they understand a hazard to be and how it is different to an accident. A hazard is often confused with an accident and when analysing SM proposals and designs it is important that the engineer is able to identify the hazards associated with his design. This is necessary so that the engineer can provide sufficient mitigation to reduce the level of risk to an acceptable level (ALARP) and hence prevent the hazard changing state and becoming an accident.

*'Please explain what you think a hazard is and how does it differ to an accident?'*

The following answers were provided:

Resp 1

Answer: A hazard is a risk that could result in an accident. An accident is the realisation of a hazard.

Resp 2

Answer: A Hazard is a potential problem. An accident is the result of a hazard.

Resp 3

Answer: A hazard is something that if ignored or used incorrectly may cause catastrophic failure of an item or harm to the user.  
An Accident is what happens if a Hazard is ignored or incorrectly used.

Resp 6

Answer: A hazard is a physical situation or state of a system that may lead to an accident  
An accident is an unintended event or sequence of events that causes harm.

Most respondents identified the differences between an accident and a hazard and demonstrated they had some knowledge of what each state is. This means that when designing or evaluating the proposed design for the SM they should be able identify the associated hazards of the design and mitigate against them.

### 5.1.4 Evaluation of Section 3 – Questions 22 To 27

In this section of the questionnaire the respondents were asked questions on what tools were being used to assist in populating the SSQ and in particular Q6.01a and what knowledge of other tools they had. The following answers were provided.

5.1.4.1 Question 25 In Chapter 2 the literature review investigated what tools were available to assist in the completion of question 6.01a. It was established that the with the exception of the SSQ ‘Response’ sheet which provides guidance there was no other direct guidance or support to assist in completing the question. Question 25 asked the following:

*‘Please explain what procedures, processes, methods and other aids you use to help populate question 6.0.1a of the SSQ?’*

Resp 2

Answer: Discussion with users, operators, engineers and experience.

Resp 3

Answer: None

Resp 6

Answer: Experience and a detailed knowledge of the purpose and working of the proposed equipment or systems.

### Resp 8

Answer: Every system will need to be looked at and judged on its individual merits. All those concerned with the system will sit down and discuss the safety implications of the system on the safety case and whether it can be sufficiently mitigated to allow acceptance of the system. If a system is obviously unfit for flight then this will be evident relatively early on and the system/Modification will be scrapped.

### Resp 11

Answer:

I populate this question with a standard answer which is as follows:

“If the proposed [system] is fitted to the aircraft, the existing Aircraft Safety Case (ASC) will require amendment. Consultation will be required between the [relevant] IPT and the ASC manager, to agree an amendment to the ASC to include this modification.”

It can be seen, the answers range from none through using personal experiences to using a standard format answer (Resp 11) as was identified in Chapter 2. These answers support the findings that in most cases the answers provided by aviation engineers when answering the SSQ can be somewhat vague. It is a concern when an answer like that of Resp 3 is provided to Q6.01a. However, an answer like that provided by Resp 11 would be a chosen response when populating the SSQ. This would imply that in most cases the aviation engineer populating the SSQ and in particular Q6.01a is not trained in safety and has no safety responsibilities attached to his role and basically does not understand how to answer this question. He therefore errs on the side of caution and the onus is passed to the IPT to provide specialist advice to assess the safety implications and provided assurance that the SM is safe. This will be contracted out to specialist safety consultant organisations and on most occasions at cost. It could be argued by the aviation engineer that if this is the normal procedure then why does he need to know about the effects on the SC?

What is evident though is that in all the answers received, not one respondent mentions the use of an appropriate Standard i.e. DS 00-56, DOI 178B or SC tool such as GSN or ASCAD.

**5.1.4.2 Question 27** If the engineer is to be able to assess areas of Q6.01a, then it is important that they are aware of other tools used in support of the SC. Question 27 asks:

*‘Please explain what you think a Hazard log is and how it is used?’*

The following answers were provided:

### Resp 2

Answer: Part of the development process to identify and record possible Hazards identified during outline design through to completion of the detailed design stage.

### Resp 5

Answer: A log of hazards....a document that lists the hazards that may affect a system or aircraft. It is probably used in the safety case.

### Resp 7

Answer: The hazard log is used to record and manage all identified system risks and provides an audit trail as to the actions taken to mitigate and reduce a hazard to ALARP.

Resp 8

Answer: When a hazard has been identified it will enter this log. The log provides an audit trail and proof that comprehensive risk assessments have been carried out.

Resp 12

Answer: A hazard log is a list of potential hazards that have been identified and documents what process has been put in place to reduce or remove that hazard.

Most respondents identified that the hazard log is a document where identified system hazards are recorded and is used as part of the SC. However, none mentioned any of the other elements that are to be found in a Hazard log such as; severity categories, probability categories and accident risk classification scheme. Respondents 7 and 12 identified risk mitigation or processes to reduce the risk that are used in resolving the risks associated with the identified hazards.

### 5.1.5 Evaluation of Section 4 – Questions 28 To 41

In this section of the questionnaire the respondents were asked questions on the SSQ. In particular the questions attempted to illicit whether respondents felt there was enough supporting documentation to help them complete the SSQ and Q6.01a. The following answers were provided to a sample of the questions asked.

5.1.5.1 Questions 35 and 36 Questions 35 and 36 formed a two part question. Completion of question 36 was dependent on the answer that was provided by question 35. Question 35 asked:

*‘Does the guidance provided by the SSQ response form help in answering question 6.0.1a on safety?’*

The following sample answers were provided

Yes	2
No	9
Note 1 – Resp 9 did not provide an answer for this question	

An overwhelming response of ‘no’ was provided by the respondents to this question equating to 75% of those who answered. The following answers to question 36 demonstrate why respondents answered no. Question 36 asked:

*‘If you answered ‘no’ to the previous question please explain why?’*

Resp 2

Answer: Very vague.  
Any change to a cleared aircraft will in some way affect the aircraft Safety case.  
It is the responsibility of the IPT and RTSA to amend as required.

Resp 3

Answer: The explanation of what they are actually asking is insufficient to make a fully informed answer.

Resp 5

Answer: “State the effects” appears to be quite open ended and should be broken down into other categories.

Resp 6

Answer: Simple statement only with no guidance on specific info required

Resp 7

Answer: Guidance is insufficient to ensure a qualified decision as to impact of the SM on the overall safety case. In addition I consider that the question as to impact on safety case can only be addressed when all other elements of the SSQ have been considered, suggest the question at 6.1.a should be moved to end of questionnaire.

Resp 12

Answer:  
It asks for three things - the effect, the required changes and the actions required to update the Safety Case. Without detailed knowledge of how a safety case is compiled and current risks within an area / system it is probably outside the scope of the system designer to fully answer this question at this stage.  
I feel that this question is more directed at the Safety Case Manager who would be better placed to determine the effects on the Platform Safety Case by the implementation of the SM albeit in consultation with the system designer.

It is quite clear from these answers that there is a strong feeling that there is not enough supporting documentation to help complete the SSQ. Resp 7 feels that the guidance is insufficient to ensure a qualified decision as to impact of the SM on the overall safety case and also indicates that for completeness, he would like to see Q6.01a moved to the end of the questionnaire so that it is answered after all other questions have been answered.

It is assumed that Resp 7 means a competent decision when he refers to ‘qualified decision’ as to the impact of the SM on the overall SC. For his decision to be of sound judgement based on fully supported facts and evidence the guidance in the SSQ needs to be more concise as to what he needs to consider when making his decision. He possibly feels that because of this his answers are informed. Resp 12 also highlighted that there are three elements to Q6.01a as was highlighted in Chapter 2 of the literature review and felt it was not possible to completely answer this question without consultation between the SCM and system designer.

5.1.5.2 Question 37 To be able to answer Q6.01a completely it was felt that the engineer should have some idea as to what the inputs to Q6.01a were. Question 37 asked:

*‘Please explain what you think are the inputs to question 6.0.1a of the SSQ?’*

The following sample answers were provided:

Resp 3

Answer:  
Hazard Log  
Risk Assessment  
Current RTS  
Form 100 Certification

Resp 4

Answer: Hazards and safety critical issues as stated before.

### Resp 6

Answer: Details of equipment to be modified or fitted.  
What testing and clearance of the modified or new equipment has been carried out with proof (Forms 100, DDPs etc.)  
How modification of existing or inclusion of new equipment/system could affect the safety of the aircraft and how this risk could be removed or mitigated.  
Any limitations imposed due to the modification/inclusion of the equipment/system.

### Resp 7

Answer: All other questions on the SSQ.

### Resp 12

Answer: The inputs are the positioning of LRU's, their methods of attachment, associated cables and their routing, the SM's weight and balance, how the system is used - fully automated or human controlled, coupled with the interaction / effects that it may have on other systems. A number of which have not yet been decided upon.

Again, this question produced a large spread of responses. None found it easy or very easy to detail what the inputs are to Q6.01a as can be seen from the answers. This is an area which is problematic to be specific on actual inputs. Resp 7 suggests that all other questions of the SSQ are the inputs. This holds true in the sense that all changes brought about by the introduction of the SM are addressed in the SSQ and form a fundamental part to the input of the SC. This would also support Resp 7 reasoning on wishing to put Q6.01a at the end of the SSQ. Resp 6 identified more formal type airworthiness elements i.e. F100, DDP. Again these are important elements to consider when reviewing the SC and they form some of the inputs to the RTS.

5.1.5.3 Question 38 Having established what the respondent thought were the inputs to Q6.01a, Question 38 asked respondents what they thought were the outputs of the question. Question 38 asked:

*'Please explain what you think are the outputs to question 6.0.1a of the SSQ?'*

### Resp 2

Answer: Tasking to be arranged at Initiation meeting to review installation, ground testing, flight testing, EMC, Tempest and other testing that may be required to enable RTSA to issue an amendment to the aircraft SD.

### Resp 3

Answer: What actions need to be taken to provide evidence to support the safety case.  
The safety case for that item on a specific platform.

### Resp 4

Answer: Hazards and safety critical issues as stated before.

### Resp 6

Answer: Identification of any hazards introduced by the modification/inclusion of the equipment/system.

Resp7

Answer: Outputs should be all required actions required to identify and mitigate hazards plus also requirement to update overarching platform safety case. Primary purpose of SSQ is to inform the IPT of the potential risks that may be introduced by a service mod so that this risks can be assessed to confirm that they can be reduced to ALARP and hence the SSQ informs the decision as to whether a SM may be progressed, i.e. if an unacceptable risk cannot be reduced to ALARP then the SM will not be progressed.

Most respondents referred out to the identification of hazards as being one of the outputs of Q6.01a. Resp 3 provided an answer that would reflect the actions of the inputs on Q6.01a and identified that the outputs would be the actions required to provide evidence in support of the SC. Resp 7 provided the most thorough answer indicating that the outputs should be *all* the required actions to identify and mitigate hazards but also he identified there would be a requirement to update the overarching platform SC.

5.1.5.4 Question 41 To complete the questionnaire and provide a catch all type question to sweep up any issues that had not already been covered. Question 41 asked:

*'Please detail what assistance/guidance **you** would like to help/aid in answering question 6.0.1a of the SSQ'.*

The following sample answers were provided:

Resp 1

Answer: The current SSQ is adequate.

Resp 2

Answer: To know what the IPT and Aircraft Safety Manager are after.

A more in depth guidance to what the above are after.

Resp 3

Answer: A more in depth explanation of what is required by the question.

A list of publications/leaflets that could assist me in answering the question.

Resp 4

Answer: None, it is not our job and we are not properly qualified to make these safety critical decisions, there are people who are paid a lot more than ourselves to put their neck on the line.

Resp 6

Answer: Course on Safety Management.

Resp 7

Answer:

1. Check list of areas to be assessed.
  2. Preliminary hazard analysis.
- Input from platform SM.

### Resp 8

Answer: Greater experience with Safety Cases should naturally lead to making this question easier to answer. Having only done one SSQ I don't feel I have adequate knowledge to know what would aid me and what would not as I am still awaiting feedback on my first attempt.

### Resp 9

Answer: From past experience of writing SEMs any guidance like that shown in AP100B-04 (Service Engineering Modifications) -Proposal and Safety Questionnaire would help. A lot of knowledge was always passed by word of mouth between engineers tasked to draft the SEM. How this ever was checked against a Safety Case I don't know. The SEMs were always written in house and checked internally by IPT Engineering. Once the SEM TI was undertaken evaluation by QinetiQ was tasked prior to SEM Approval.

### Resp 10

Answer:  
I regularly use, specialist advice from the following agencies:  
  
Support Helicopter Engineering Development Investigation Team (SHEDIT)  
QinetiQ  
Equipment Design Authority  
Aircraft Design Authority.  
Release to Service Authority.

### Resp 12

Answer: Greater guidance on what information is required, the depth and format of that information and where possible adequate training on Safety Case to ensure the information presented is pertinent and succinct.

Only one respondent felt that the guidance provided in support of Q6.01a was adequate and one respondent did not answer the question. In general most respondents indicate that they feel there is insufficient guidance to assist in completing Q6.01a accurately which supports the findings of the literature review in Chapter 2. Lists of publications, leaflets or checklists which would guide the engineer through the completion of Q6.01a, featured in two of the answers provided. Three respondents indicated that they would require more in-depth information regarding what information is required by the question and one respondent indicated that he would like to know exactly what the IPT and Safety Case Manager require. Other answers range from gaining the guidance necessary through developing experience, being provided with the appropriate training i.e. a Safety Management course and using specialist advice from specialist departments and finally on a cultural issue the respondent who felt it was not his job as there are people paid more money than him to take that risk!

As with many of the questions respondents did not answer exactly what was being asked of them and the information supplied by the respondents particularly to this question lacks completeness and accuracy. This may be for the following reasons:

- The question is open-ended and the respondent has misinterpreted and hence misclassifies his response.
- The respondents did not have sufficient time to complete the question and it was completed hurriedly
- The respondent does not know what additional guidance/information he requires to answer the question.

- The respondent was bored with completing the questionnaire as it was possibly too long and uninteresting.
- A matter of a culture issue in that the respondent does not see the benefit of completing the answer completely and accurately because he can not see the long term prospects. These prospects would be a much improved set of guidance documentation to assist in being able to complete fully and accurately Q6.01a and on a larger scale the SSQ.

## 5.2 Summary and Observations

The means of deciding whether a guide or questionnaire with supporting guidance is required to assist the aviation engineer in correctly answering Q6.01a of the SSQ was carried out using a questionnaire. This investigated what safety and safety assurance knowledge resides amongst aviation engineers. The questionnaire was sent out to a known target audience which covered domain knowledge from SM designers (fast jet and rotary) to IPT's who support rotary and large aircraft platforms. Overall it is felt that the 40% feedback received of completed questionnaires was good when then respondents only had four weeks to complete it. However, the amount of data received in those questionnaires was excellent and provided a rather large amount of analysis.

Overall the questionnaire has done well at addressing the issues and problems identified in Chapters 2 and 3 and further supports that these problems and issues do exist. The following sections discuss in detail the findings in the evaluation phase addressing each area separately.

### 5.2.1 Questionnaire Design

There was some criticism received regarding the design and size of the questionnaire. On reflection it was possible there were too many questions asked which made the questionnaire laborious and time consuming to answer. This may have been a contributing factor in the poor response of completed questionnaires. Whatever the intent, questionnaires rely on their ability to interest respondents, strike a relevant chord and motivate a thoughtful response. While attention to design and a conceptual understanding are important, it was not taken into consideration how busy the respondent may be and finding time to complete the questionnaire was difficult.

However, at the time of design it was decided that Safety covered a wide ranging spectrum of engineering attributes and to gain an appreciation to form a complete picture of the respondents needs; many questions would need to be asked. It was also decided not to use rankings as the choice for answering relatively simple questions but to use a ratings system instead. This would enable the respondent to indicate at what level they placed themselves in the rankings based on the assessment of their own abilities, knowledge and competencies – again giving a more complete picture. Most rating type questions were found in Sections 1 and 2.

The comments blocks were relatively well used although adding comments in these areas was not mandatory but allowed the respondent to extend their answer. This also provided the extra benefit of more data on which to base the analysis. Much like the open-ended questions that were used in section 4 of the questionnaire the comments blocks did allow the respondent to expand on their answer or add to the already constrained closed-ended question that the comments blocks were attached to.

Use of open-ended questions allowed the respondents to supply a variety of answers of varying length and articulation. It also presented some very precise judgements of individual respondents which can be seen in some of the answers provided in Section 4 of the questionnaire.

The understandability of the questions is paramount and in some of the completed questionnaires this is obvious. Pitching the question at the correct level for the respondent to understand is very difficult especially when considering the wide target audience that the questionnaire was distributed to.

## 5.2.2 Section 1 of Questionnaire

### 5.2.2.1 Competencies and Qualities

What is interesting in this section of the questionnaire is that 50% of respondents indicated they felt they were reasonably confident and competent to answer questions on Safety engineering but only 44% indicated they were reasonably confident to populate questions on the SSQ. All respondents who answered these questions are not employed in safety specific posts and tend to be platform/domain experienced aviation engineers with no safety engineering training. When asked whether a non-safety role person was competent to answer questions on the SSQ most respondents were not sure although many additional comments supplied to this question suggested that as long as the engineer was competent on the platform and had the correct experience to be able to answer the question then it would be possible. It is felt however, that to be able to provide completeness of the answer to Q6.01a the aviation engineer must be safety competent, confident in his abilities, appropriately trained and with the necessary platform/domain skills, experience and knowledge. These competencies may be based on the model guidelines presented in Chapter 2 section 2.5.4. This will be put forward as a proposal in Chapter 6 - Further Work.

### 5.2.2.2 Engineering Terms

Most respondents provided some understanding of the meaning of Airworthiness, Safety Case and Human Machine Interface. The answers that were near word perfect and suggest reference to some form of textual source i.e. JSP553 were not included in the examples used for the evaluation as it is felt that this defeats the objective of what the question is attempting to elicit. This question was to ascertain what the respondent understood by each term however, the question may have been better set to elicit the respondents understanding of Safety rather than Safety Case. The reason why SC was used as this term is one of the key areas in the SSQ and to answer Q6.01a which asks about the affects on the SC it was deemed to be the better choice. However, the literature review in Chapter 2 and 3 identified that the two terms Airworthiness and Safety are often confused or incorrectly defined and it may have been more appropriate to compare these two terms.

### 5.2.2.3 Safety Critical and Safety Related

It was judged that the engineer should be able to differentiate between a safety critical system and a safety related system as both are treated different when providing safety analysis and assurance. If the status of the system or the system/s affected by the new design is not identified early in the design process then there is potential for this scenario not be addressed at all or until the SM is passed to an independent agency for safety analysis. At this point the assessment phase becomes expensive and may mean cancellation of the project. Answers were not exceptionally strong to this question and it highlights that although the aviation engineer may have years of platform experience and system knowledge, it does not necessarily hold that he will be able to identify whether the system he is modifying is safety related or safety critical.

### 5.2.2.4 Safety Responsibilities

Most respondents targeted with answering the questionnaire do not work in departments where safety engineers are employed and as was previously highlighted, there is no requirement to define system safety responsibilities. This is further supported by Resp 1 who notes; that even in the JAP which is his governing document, system safety responsibilities are not clearly defined for SM's. It is not uncommon that much emphasis on detailing responsibilities for system safety is directed at DLO and DPA departments and the fringe DO's tend to be left out. For many DO's there is currently no requirement to put in place an SMS.

### 5.2.2.5 Other Questions Asked

All though several questions were evaluated in this section, not all were covered. Others were asked regarding the respondents experience of Safety Engineering to which the majority answered No safety engineering experience before their previous role but most indicated they felt reasonably confident to answer questions on safety engineering. Respondents were also asked to rank their experiences regarding their level

of confidence to identify hazards, assess likelihood and severities and allocate tolerabilities. Most answered not fully confident and again if the respondent is to populate a question which is concerned with the effects to the SC then it is felt that these are areas the aviation engineer should be conversant in.

### 5.2.3 Section 2 of Questionnaire

#### 5.2.3.1 Knowledge of Safety Case and the Contents of the Safety Case

The main thrust of the safety element of the SSQ is Q6.01a which asks:

‘State the effects on the Safety Case, the required changes and associated actions’

For the engineer to provide completeness of his answers to this question it is important he understands what a SC is, how it is used and what are the contents of the SC. There are several definitions of what a SC is but minimal literature is provided on dealing with the contents and the results from the answers to questions in these areas were not unsurprising. Two thirds of respondents had little knowledge of SC’s but some had some idea as to what their purpose is. However, for the engineer to be able to answer this question extensively may/will require access to the SC to determine exactly what has been the effect caused by the change due to the introduction of the SM. For most engineers this will not be the case as most platforms SC’s are held by the IPTL and managed by the RTSA. Varied answers were supplied and as with the literature review in Chapter 2, nothing conclusive was derived as to the exact contents of the SC. Guidance is needed here and a starter for ten list is required. This list has not been generated due to lack of time and will form one of the proposals for the further work chapter.

#### 5.2.3.2 The Release To Service

It was not clear from all the answers provided for this question that all respondents were familiar and understood the term RTS. It was also clear that respondents did not understand that the SC was a major input into the RTS. This was illustrated by the answer provided by one respondent who thought the RTS was the main body of evidence forming the basis of the SC.

#### 5.2.3.3 ALARP, Hazards and Accidents

Respondents were asked to describe what they thought the acronym ALARP meant and how it was used. Although most had heard of the term, only 42% described what the acronym stood for. Less than 40% were able to describe how it is used and only two respondents were able to give detailed and accurate answers to this question. Although a commonly known term in the safety engineering world, ALARP is not necessarily as well known within the aviation engineering fraternity.

Safety Hazard and Risk analysis involves responsibilities for identifying all foreseeable hazards and assessing the risk of an accident. Hazard analysis has a large influence on the design of a system. However, much discussion goes on as to whether it is an accident or a hazard and on many occasions accident and hazard are used in the wrong context. In question 21 respondents were asked to explain; what they understood a hazard to be and how it is different to an accident. Most respondents had some idea as to what a hazard and an accident are and would be able to identify top level hazards associated with the design of their SM. Being able to perform this action will enable the engineer in assisting with the identification of mitigation to eliminate hazards or reduce the risk of accidents.

### 5.2.4 Section 3 of Questionnaire

#### 5.2.4.1 Establishing Other Guidance Used in Completing Q6.01a

This section of the questionnaire looked at the use of tools in support of completing the questionnaire and although it asked questions in other areas of the SSQ, it focused in on what procedures, processes, methods and other aids the engineer uses to populate Q6.01a. The responses were disappointing in this area and did

not yield many sources of information used. Many respondents indicated they use their experiences but at no time was an appropriate Standard i.e. DS 00-56, DOI 178B or SC tool such as GSN or ASCAD mentioned – of the 12 respondents 83% indicated they had not heard of the term/tool GSN in the GSN question.

#### 5.2.4.2 Hazard Logs

Most respondents had heard of the tool Hazard Log, but none had used it. Many answers stated the obvious statement of a hazard log being somewhere where hazards are recorded, but no mention was made to its other contents i.e. severity categories, probability categories and accident risk schemes. Neither was it indicated that the hazard log should be reviewed to assess the impact on already documented hazards that the new SM may have. A SM could change the level of risk of an existing hazard and clearly has the potential to introduce additional hazards.

#### 5.2.4.3 Other Questions Asked

Others questions were asked in this section on whether respondents used other tools such as checklists, GSN and other tools such as ASCAD. Responses to most of these questions were no. A high percentage of respondents had not seen or used GSN or any other Graphical Notation type tool. However evaluation on these questions was not carried and the most pertinent questions in this section were chosen for evaluation.

### 5.2.5 Section 4 of Questionnaire

#### 5.2.5.1 Determining the Support Provided by the SSQ Response Form

Answers provided to questions asked in this area regarding the support provided by the SSQ Response form used in answering Q6.01a, consistently indicated that the support and guidance provided is inadequate. These questions resoundingly recorded the most amount of ‘no’ answers which was more than any of the previous questions asked. A general theme emerges from the answers and is one where the respondent requires more guidance/ support to be able to make a qualified answer to Q6.01a. Resp 7 indicated in his answers to this question, that he would like to see Q6.01a moved to the end of the SSQ so that it is populated after all other SSQ had been answered. This feeds in to the next area that was discussed – that of what the respondents consider to be the inputs to Q6.01a.

#### 5.2.5.2 Inputs to Q6.01a

This proved a difficult area for respondents to answer and like many of the other answers supplied by respondents they were varied and incomplete. There is not a defined answer for the inputs to Q6.01a of the SSQ, much like there are no defined contents of a SC. This makes this question difficult to evaluate as there is no criteria to evaluate against. Probably the answer that provides what is perceived to be the input to Q6.01a is all the answers to all other questions on the SSQ – this was identified by Resp 7. In most answers supplied, respondents identified some of these inputs.

#### 5.2.5.3 Outputs of Q6.01a

Again respondents supplied varied answers to the question posed in this area. Much like the comments above regarding the inputs to Q6.01a, there are no defined outputs. Most respondents took the hazard identification route whilst others included the requirement to update the overarching platform safety case

#### 5.2.5.4 Final Catch All Question

Having researched the respondents; qualities, competencies, knowledge’s of safety engineering, experiences of SC’s and safety engineering tools and thoughts and views of the SSQ, question 41 provided a sweeping up open-ended type question. This was used to ascertain exactly what additional assistance/guidance the respondent would like to help/aid in answering all questions on the SSQ and in particular Q6.01a. The answers provided were not as detailed as was expected and the cause of this may have been that by this stage

of the questionnaire, respondents interests were starting to wane. However, what was evident was that all respondents indicated there was a requirement for additional guidance, training and support required for:

- Completing all other SSQ questions
- Completing Q6.01a of the SSQ.

## 5.3 Conclusions

The aim of this project was to establish what safety and safety assurance knowledge exists within the military aviation engineering world of those completing a SSQ as part of a tri-service Service Modification (SM) process. It would also investigate whether there is a requirement to provide some form of guidance tool in this area and to indicate what form this guidance should take. In particular, the study looked closely at the completion of a question (Q6.01a) which involves asking the person/s completing the SSQ whether there is an effect on the Safety Case (SC), the required changes to the SC and associated actions, which are caused by the introduction of a SM design.

The SSQ is normally completed and reviewed by non safety specific aviation engineers, this one small question presents a plethora of areas within the safety engineering world that the aviation engineer should be aware of. A questionnaire was developed in four sections covering the role, competencies and experiences of the engineer, through knowledge of safety terms, tools used in support of completing the questionnaire and what guidance the engineer feels is necessary to complete Q6.01 fully. Twelve completed questionnaires were received back from a total of thirty that were sent out and on the whole provided excellent data for analysis.

From the findings in the evaluation sections and the answers provided to the questionnaire, it is evident there is a requirement for any one or possibly more of the tools listed below to be provided to assist the engineer in completing Q6.01a of the SSQ. However, it is proposed that this tool could take any of the following forms:

- A checklist detailing what activities are required for the completion of answering Q6.01a.
- Another questionnaire which is designed to specifically asks questions relating to the activities in Q6.01a.
- Concise and accurate guidance and documentation on how to complete the activities of Q6.01a.
- Improve the safety competency levels of the aviation engineer by providing the appropriate safety training and skills needed to be able to confidently answer Q6.01a.
- A flow chart which directs the aviation engineer through the activities of addressing the requirements of Q6.01a.

More details are provided in the further work section in Chapter 6.

### 5.3.1 Strengths and Weaknesses of the Questionnaire

Overall the use of a questionnaire to assess what knowledge of safety and safety assurance the aviation engineers who are completing and addressing SM's and SSQ's have, was the correct choice for this project. The questionnaire has provided an effective method for efficient collection of information. The strengths and weaknesses of the questionnaire are provided in the following bullet points.

#### 5.3.1.1 Strengths

- Questionnaires permit respondents time to consider their responses carefully without interference from, for example, an interviewer. However, in the case of the questionnaire used for the case study,

respondents were only given four weeks in which to complete and return the questionnaire to the author – this may have been a weakness (see below).

- It was possible to provide questionnaires to large numbers of people simultaneously especially as electronic distribution by e-mail was chosen. However, there is a down side to this form of distribution and that is there is a possibility that the response rate would be lowered.
- Uniformity. Each respondent received an identical set of questions. With closed-form questions, responses are standardised, which can assist in interpreting from large numbers of respondents.
- Closed questions are less time consuming for respondents to complete, and this allows the questionnaire to ask more questions. However, this questionnaire also comprised open-ended questions. The advantage of an open-ended question is that it allowed respondents to answer the question in the way they wished and therefore allowed true opinions/attitudes to be elicited. It is felt by the author that by mixing both open and closed questions was the best approach, avoiding an overly restrictive questionnaire and one that is too open and difficult to analyse.
- Questionnaires can address a large number of issues and questions of concern in a relatively efficient way, with the possibility of a high response rate.
- Often, questionnaires are designed so that answers to questions are scored and scores summed to obtain an overall measure of the attitudes and opinions of the respondent. Rankings were not used in the case study questionnaire but ratings used instead. This approach was employed to give the author an accurate assessment of the experience, competencies and knowledge of the respondents.
- Questionnaires permit anonymity. The respondents were given the choice of whether to complete the Name block on the questionnaire or not. It was hoped that anonymity would increase the rate of response.
- Respondents appeared to be honest in most questions asked and the information supplied appears a true reflection of their safety and safety assurance knowledge.

### 5.3.1.2 Weaknesses

- The response rate was disappointing and a much higher return of more than twelve questionnaires had been expected. There may have been many factors for this and the following details some of those:
  - The questionnaire was too long and respondents lost interest in completing it.
  - Respondents were too busy to attempt it in light that only four weeks were given for respondents to reply.
  - The questions were too difficult to answer and hence the respondent would not attempt them.
  - The respondents did not feel it appropriate to answer the questions as they were not concerned of the outcome of the study.
- The use of open-ended questions may have invited respondents to supply unhelpful and misleading data.
- The quality of data in some areas i.e. Section 4 was probably not as high as expected and interviewing respondents may have been more appropriate.
- Completeness and thoroughness of the answers supplied often made the analysis of the answer inconclusive.

- The inability on the part of the respondent to correctly read the question and answer it properly also presents a problem – if the answer is misrepresented then the analysis becomes flawed.
- Cultural issues. As was pointed out in one respondents answer, he felt that answering and dealing with Q6.01a was not his responsibility as there are persons who are paid much more than him to deal with the risk of safety and to quote ‘put their neck on the line’.

## 5.4 Other Observations

Many observations have been made in the ‘Evaluation’ and ‘Summary and Observation’ phases regarding the data supplied in the completed questionnaires. However, it has also been observed that:

- There is some misunderstanding of safety terms and how they are used and interpreted by non safety trained engineers.
- SC knowledge of respondents was relatively weak and this is further compounded by the fact that there are no concise details listed in relevant literature as to what the exact contents of the SC are so as to assist the aviation engineer.
- It was clear that not all respondents understood the questions and without appropriate training in safety and safety assurance it is unlikely that this situation will change.
- With the exception of one, all other respondents agree that there is a need to provide more and proper guidance in support of completing Q6.01a of the SSQ.
- Most respondents agree that there is also a requirement for more guidance and support documentation in support of completing the SSQ as a whole.
- Appropriate training in safety engineering should be employed for those engineers in DO’s or roles where dealing with the SM’s and SSQ’s is involved.

Having read much literature regarding what is perceived to be an acceptable response rate to respondents completing questionnaires, it was deduced that there is no acceptable response rate but returns of between 45% and 60% are deemed good. This is supported in an article written by Dr J Briggs – Portsmouth University [43] who suggests that:

‘The issue of response rates, or completion rates, is very much one of the old chestnuts.

What constitutes an acceptable response rate?

The recommendations that accompany the University's policy on feedback state a threshold for satisfactory completion rate for both course and unit feedback should be at least 50%, and that 75% would be "good". Action should be taken where this is not met. The standard work on student feedback in the UK is the report by Brennan and Williams setting out good practice (Brennan 2004). They suggest that 60% is something to aim for and that below 30% the results would need to be treated with care’

It is therefore fair to say that response rate achieved in this project was acceptable and 44% of returned questionnaires is a very reasonable figure and a good achievement.

## Chapter 6 – Further Work

This project has assessed, using a questionnaire, the safety and assurance knowledge of aviation engineers who complete or review a Safety and Support Questionnaire (SSQ) used in support of a tri-Service, Service Modification process. It has also evaluated that the findings of the literature review (Chapter 2) and the observations of the author show that there is insufficient guidance provided in the SSQ to assist the aviation engineer in completing the safety question (Q6.01a) fully. The next stage in this project is to propose some further work that the author sees as beneficial to the identified issues. The following further work is suggested to extend this case study towards providing sound and complete guidance for completing Q6.01a of the SSQ.

### 6.1 Provision of a Flow Chart

Given the nature of the issues dealt with in the evaluation phase (Chapter 5), it has been established and conclusively confirmed that the specific guidance provided by the SSQ Response form does not provide the aviation engineer with sufficient information to assist in confidently addressing the issues related to answering Q6.01a. Searching around for appropriate supporting/guiding documentation to help the aviation engineer has also established that there is no specific guidance to address this gap. The author therefore proposes that a flowchart be developed, which guides the aviation engineer through the elements of Q6.01a.

#### 6.1.1 Development of a Guidance Flowchart

The use of a flow chart will provide the aviation engineer with an easy to understand diagram/s showing how steps in the process fit together. This makes it the ideal tool to communicate to the aviation engineer how to answer the requirements of Q6.01a and on, a wider scale, other questions in the SSQ. It will also provide clear documentation on how this particular job is done. Furthermore, the act of mapping a process out in flow chart format will help the aviation engineer to clarify his understanding of the process, and will also help to make the aviation engineer think about where the process can be further improved.

#### 6.1.2 Designing the Flowchart

Q6.01a asks the person completing question to ‘State the effects on the Safety Case, the required changes and associated actions’ which are brought about by the introduction of the Service Modification (SM). These are considered to be the key starting points for the flow chart. To address these three elements it may require more than one flow chart, and it could be possible that there is a flow chart for each element. It is therefore proposed that the first flow chart deals with ‘effects on the safety case’, the second with the ‘required changes’ and the third with the ‘associated actions’. It is possible that at some level of decomposition, the output of one of the flow charts may feed into one of the others. Due to the nature of the SSQ, the approach to the flow chart will probably be a hierarchical ‘bottom up’ type chart in that, for example, local effects of a proposed modification on elements of the safety case will be considered first, and then the effect of these at the overall safety case level will be addressed.

Understanding the activities within the flowchart is important and the aviation engineer will need to be versed in the safety engineering terms discussed in Chapter 3 (discussed more in further work). However, if the aviation engineer does not understand the question being posed, or does not have the relevant guidance to answer the question, he will be directed within the flow chart where to find the relevant answers or guidance from the no output of that particular level. For example, ‘do you have access to the platform safety case?’ If the answer is ‘yes’ then the aviation engineer will be directed to continue. However, if the answer is ‘no’ then guidelines in the flow chart will describe the required activities to address this question. In this particular case the chart may well state something like: ‘Contact relevant IPT for access to the safety case’. If the issue is perhaps how to deal with a hazard introduced by the SM and the compiler does not know how to deal with it, he would be prompted to source appropriate documentation in the form of safety literature or a defence standard or other source of information where the solutions can be found.

It is intended that the flow chart addresses and includes the safety and airworthiness terms described in Chapter 3, which have been evaluated in the questionnaire at Chapter 5. It will also include what the author feels is a bare minimum of areas that should be addressed when considering the requirements of Q6.01a. This list was described in Section 3.1.6

Due to limiting timescales it has not been possible to produce and evaluate the proposed flow chart. It is therefore proposed that the flow chart is produced and evaluated as part of a case study to assess its suitability as a tool to provide the necessary guidance to the aviation engineer. It would be beneficial for the case study to be carried out using the respondents who supplied answers and comments to the original questionnaire so that a true evaluation can be made.

## 6.2 Competencies Framework

It is recognised that for the aviation engineer to confidently use the flow chart proposed above, he will need to be safety competent. The aviation engineer can only achieve this level of competency if he has been appropriately trained in safety engineering and has appropriate domain knowledge and experience. As was identified in the literature review (Chapter 2) and the evaluation phase (Chapter 5), there is not a specific competency model for the aviation engineer who completes and reviews the SSQ and in particular Q6.01a. The author therefore feels that there is a need to develop a competencies framework/model which is specific to the aviation engineers completing the SSQ to address this issue.

It is proposed that the competency framework be developed using elements from the Airworthiness Competencies Set or from the IEE competency guidelines or even both as discussed in Chapter 2. It should also be considered that both competency sets are guidelines and that they can be tailored suit the role being performed. Further information that could be used to develop the competency framework is that of a set of competency guidelines entitled 'Managing Competence For Safety-Related Systems' [44]. At the time of writing this project the document is currently in draft format. The guidelines have been produced by a partnership of HSE, the Institution of Electrical Engineers (IEE) and the British Computer Society (BCS), and details how to manage competence for safety-related systems.

The focus of the draft guidance is the functional safety of safety-related systems. However, the IEE/BCS/HSE suggest that it is written with a view to broader application, and it is compatible with competence management systems (CMS) with more general scope and with career development and professional development schemes [44]. To quote the draft guidance it aims to:

- Explain the main features of a competence management system (CMS) for all staff at all levels of responsibility within an organisation that works on safety-related systems, to enable the organisation to meet the UK legal requirements for competence for safety-related systems in general (i.e. without going into detail for any one particular industry sector)
- Describe the purpose of each of these features and give guidance on how to set up and operate a CMS in a way that achieves these and is efficient, effective, minimises administrative overhead, and can be audited efficiently.

The key objectives of a competence management system in this guidance are represented in the form of 15 'principles' unlike the 12 functions described in Chapter 2. Specific guidance is then provided on practical ways to realise those principles.

## 6.3 Checklist to Consider the Contents of the Safety Case

Although it is not possible to exactly define the contents of the platform safety case as they will be specific to that platform, it may be possible to derive a generic checklist, based on the author's ideas in Chapter 3, of what elements the aviation engineer needs to consider when addressing the effects on the SC. This document could be used as stand-alone document/checklist, or integrated into the flow chart process described in section 6.1.

## **Abbreviations**

---

<b>ACS</b>	Airworthiness Competencies Set
<b>ADS</b>	Aircraft Document Set
<b>ALARP</b>	As Low As Reasonably Practicable
<b>AMS</b>	Acquisition Management System
<b>ASEMS</b>	Acquisition Safety and Environmental Management Systems
<b>COD</b>	Certificate of Design
<b>CFT</b>	Certificate of Flight Trials
<b>DA</b>	Design Authority
<b>DAOS</b>	Design Approved Organisation Scheme
<b>DASM</b>	Defence Aviation Safety Management
<b>DASB</b>	Defence Aviation Safety Board
<b>DPA</b>	Defence Procurement Agency
<b>DLO</b>	Defence Logistic Organisation
<b>DLS</b>	Directorate of Logistic Support
<b>DM</b>	Designer Modification
<b>DMC</b>	Direct Ministry Control
<b>DMSL</b>	Draft Service Modification Leaflet
<b>DO</b>	Design Organisation
<b>Eng Pol Reg</b>	Engineering Policy Regulator
<b>ES (Air)</b>	Equipment Support (Air)
<b>FAA</b>	Federal Aviation Authority
<b>FLC</b>	Front Line Command
<b>GARP</b>	Generic Aircraft Release Process
<b>IPT</b>	Integrated Project Team
<b>IPTL</b>	Integrated Project Team Leader
<b>JAP</b>	Joint Air Publication
<b>MAE</b>	Military Air Environment
<b>MAR</b>	Military Aircraft Release
<b>MOD</b>	Ministry of Defence
<b>PI</b>	Proof Installation
<b>RTS</b>	Release To Service
<b>RTSA</b>	Release To Service Authority
<b>SC</b>	Safety Case
<b>SCR</b>	Safety Case Report
<b>SM</b>	Service Modification
<b>SMS</b>	Safety Management System
<b>S&amp;SE</b>	Safety and System Engineering
<b>SofS</b>	Secretary of State
<b>SSQ</b>	Safety and Support Questionnaire
<b>TI</b>	Trial Installation
<b>UOR</b>	Urgent Operational Requirement

## References

---

- [1] Service Engineered Modifications - AP100B-04
- [2] Special Trial Fits - AP101B-01
- [3] Service Engineering Aircraft Radio Installation Modification - AP100C-40
- [4] Naval Aircraft Maintenance Manual - AP100N-0140
- [5] Joint Air Publication (JAP) 100A-01. Military Aviation Engineering Policy and Regulations
- [6] An Introduction To System Safety Management & Assurance – Issue 1 February 2002.  
Rhys David MA CEng -Advantage Technical Consulting
- [7] Managing Safety During Design Change – A Vaughan. Project Dissertation MSc – Safety Critical Systems Engineering. University of York Department of Computer Science. September 2004.
- [8] DASMS Implementation Within The Fixed Wing Environment of The DLO. Report – July 2003
- [9] Health and Safety at Work etc. Act 1974
- [10] Joint Service Publication (JSP) 553. Military Airworthiness Regulations
- [11] Defence Standard 00-56 – Issue 3 (Interim) Safety Management Requirements for Defence Systems
- [12] ES(Air) Business Procedure 1201 – Equipment Safety Management.
- [13] Acquisition Management System  
[www.ams.mod.uk/ams/default.htm](http://www.ams.mod.uk/ams/default.htm)
- [14] Managing Complex Safety Cases. Dr T P Kelly. Department of Computer Science University of York - [www-users.cs.york.ac.uk/~tpk/pubs.html](http://www-users.cs.york.ac.uk/~tpk/pubs.html)
- [15] Defence Standard 05-123 - Technical Procedures for the Procurement of Aircraft, Weapons and Electronic Systems
- [16] Federal Aviation Authority  
[www.faa.gov/avr/iasa/PART05.doc](http://www.faa.gov/avr/iasa/PART05.doc)
- [17] Heavy Mods. A Three Stage Process For The Modification Of Undocumented Legacy Systems. KB Graham. Project Dissertation MSc – Safety Critical Systems Engineering. University of York Department of Computer Science. 2002
- [18] A Systematic Approach to Safety Case Maintenance - Kelly and McDermid.  
[www-users.cs.york.ac.uk/~tpk/scomp99.pdf](http://www-users.cs.york.ac.uk/~tpk/scomp99.pdf)
- [19] The Airworthiness Competencies Set - ALTG/06/22/02 25 May 05.
- [20] Safety, Competency & Commitment. Competency Guidelines for Safety-Related System Practitioners. The Institution of Electrical Engineers. 1999. ISBN 0 85296 787 X

- [21] Concise Oxford English Dictionary.  
[www.askoxford.com/worldofwords/wordfrom/concise11/](http://www.askoxford.com/worldofwords/wordfrom/concise11/)
- [22] Data Gathering Methodologies to Identify Impact Variables in Aviation Maintenance  
[www.hf.faa.gov/docs/508/docs/maintIERC2004WebSAT2.pdf](http://www.hf.faa.gov/docs/508/docs/maintIERC2004WebSAT2.pdf)
- [23] Questionnaires in Usability Engineering A List of Frequently Asked Questions (3rd Ed)  
 Jurek Kirakowski  
[www.ucc.ie/hfrg/resources/qfaq1.html#whatisaquestionnaire](http://www.ucc.ie/hfrg/resources/qfaq1.html#whatisaquestionnaire).
- [24] Questionable Practices - The Use of Questionnaires in PoP Research. A Blackwell.  
[www.kmi.open.ac.uk/people/paulm/summer98/question.html](http://www.kmi.open.ac.uk/people/paulm/summer98/question.html)
- [25] Acquisition Safety and Environmental Management System  
[www.asems.dii.r.mil.uk/asems\\_home\\_page.htm](http://www.asems.dii.r.mil.uk/asems_home_page.htm)
- [26] Evaluation of the Railways (Safety Critical Work) Regulations 1994.  
[www.hse.gov.uk/railways/scwreport.pdf](http://www.hse.gov.uk/railways/scwreport.pdf)
- [27] Perception of Procedures By Operators and Supervisors.  
[www.energyinst.org.uk/heartsandminds/docs/percept.pdf](http://www.energyinst.org.uk/heartsandminds/docs/percept.pdf)
- [28] System Safety Engineering – Software System Safety  
[www.monmouth.army.mil/cecom/safety/sys\\_service/software\\_handbook.htm#definition](http://www.monmouth.army.mil/cecom/safety/sys_service/software_handbook.htm#definition)
- [29] Logic and Methodology of Checklists. Michael Scriven - Claremont Graduate University  
 June 2000. [www.wmich.edu/evalctr/checklists/papers/logic\\_methodology.htm](http://www.wmich.edu/evalctr/checklists/papers/logic_methodology.htm)
- [30] The Hutchinson Encyclopaedia.  
[www.xreferplus.com/entry.jsp](http://www.xreferplus.com/entry.jsp)
- [31] Data and Computing Guidelines/ Standards Definitions  
[www.massachusetts.edu/administration/policy/data/itcdefad.html](http://www.massachusetts.edu/administration/policy/data/itcdefad.html)
- [32] Defence Standard 00-54. Requirements for Safety Related Electronic Hardware in Defence Equipment.
- [33] Defence Standard 00-55. Requirements for Safety Related Software in Defence Equipment
- [34] Defence Standard 00-58. HAZOP Studies on Systems Containing Programmable Electronics
- [35] Safety Critical Computer Systems. Neil Storey. Prentice Hall, Addison Wesley Longman  
 1996
- [36] Safety-Critical Software: Status Report and Annotated Bibliography. Patrick R.H. Place  
 Kyo C. Kang. June 1993.  
[www.sei.cmu.edu/pub/documents/93.reports/pdf/tr05.93.pdf](http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr05.93.pdf)
- [37] System Safety Engineering and Management. Harold E. Roland and Brian Moriarty 2<sup>nd</sup> Edition  
 Wiley Interscience
- [38] Arguing Safety – A Systematic Approach to Managing Safety Cases. Dr T P Kelly.  
 Department of Computer Science, University of York.  
[www.cs.york.ac.uk/ftpdireports/YCST-99-05.pdf](http://www.cs.york.ac.uk/ftpdireports/YCST-99-05.pdf)
- [39] Developing Safety Cases. Adelard  
[www.adelard.co.uk/iee\\_pn/safety\\_case\\_approach.htm](http://www.adelard.co.uk/iee_pn/safety_case_approach.htm)

- [40] The Goal Structuring Notation – A Safety Argument Notation. Kelly and Weaver  
[www-users.cs.york.ac.uk/~rob/papers/DSN04.pdf](http://www-users.cs.york.ac.uk/~rob/papers/DSN04.pdf)
- [41] Yin, R.K – Case Study Research, Design and Methods – Sage. 1994
- [42] A General Introduction to The Design of Questionnaires for Survey Research. Dr T Burgess.  
May 2001. Edition 1.1.  
[www.leeds.ac.uk/iss/documentation/top/top2.pdf](http://www.leeds.ac.uk/iss/documentation/top/top2.pdf)
- [43] Issues in the Collection of Student Feedback Online - Dr J Briggs, School of Computing, Faculty of  
Technology. Portsmouth University.  
[www.tech.port.ac.uk/staffweb/briggsj/feedback/papers/Viewpoint2005.doc](http://www.tech.port.ac.uk/staffweb/briggsj/feedback/papers/Viewpoint2005.doc)
- [44] Managing Competence for Safety-Related Systems. Consultation for Guidance Published by HSE,  
the IEE and BCS  
[www.hse.gov.uk/consult/condocs/competence.htm](http://www.hse.gov.uk/consult/condocs/competence.htm)

## Appendix A.

# Questionnaire on Engineering Knowledge of the Safety and Support Questionnaire MOD Format 755(SM2)

### ***ENGINEERING KNOWLEDGE OF THE SAFETY AND SUPPORT QUESTIONNAIRE – MOD FORMAT 755(SM2)***

I am a third year MSc student studying Safety Critical System Engineering. As part of my Dissertation I need to determine the current level of safety knowledge amongst engineering personnel who are required to populate/understand/use the MOD Format 755(SM2) Safety and Support Questionnaire (SSQ) (JAP 100A-01 Chapter 10.4 – 10.4.1). In particular I am interested in how the following statement in box 6.0.1a of the questionnaire is answered:

***‘State the effects on the Safety Case, the required changes and associated actions’.***

The MOD Format 755(SM2) –SSQ is used as part of the Service Modification (SM) process. The answers that are provided to the questions in the SSQ are used to assist in producing the SM Safety Case. The SM Safety Case is used to assess the effects of the SM on the whole aircraft Safety Case and enable the IPT to make a balanced decision on whether, or how, to proceed with the SM.

The aim of the questionnaire is to gather information on the level of safety knowledge that currently exists. From the data gathered it is my intention to devise and provide some form of tool, which will help in completing the requirements of the above question.

### ***Completing the Questionnaire***

The questionnaire contains a number of different question formats, each being self-explanatory. Where applicable, there is some extra space provided after the question for any additional comments you may wish to make. Your comments are valuable and are likely to provide some of the most useful information. Please answer the questions provided as fully as possible.

***ALL COMPLETED QUESTIONNAIRES WILL BE TREATED IN STRICTEST  
CONFIDENCE***

***I WOULD BE GRATEFUL IF YOU COULD COMPLETE AND RETURN YOUR  
QUESTIONNAIRE BY 14 DEC 05.***

***Completed Questionnaires can be e-mailed to:***

***[tony.gower@rws.mod.uk](mailto:tony.gower@rws.mod.uk)***

***Or returned by post to:***

***Tony Gower  
Desk Officer  
FS(MASU) Middle Wallop  
Middle Wallop  
STOCKBRIDGE  
SO20 8DY***

**QUESTIONNAIRE ON ENGINEERING KNOWLEDGE OF THE SAFETY AND SUPPORT QUESTIONNAIRE – MOD FORMAT 755(SM2)**

<b>Name</b> <i>(Completion of this box is optional)</i>	
<b>Position/Job Title</b>	
<b>Organisation</b>	
<b>Telephone</b>	GPTN:  CIV:

**GENERAL QUESTIONS**

***Question 1***

<i>What is your role within your department?</i>

***Question 2***

*(✓)*

<i>Do you write Service Modification(SM) leaflets?</i>	
Yes	
No	

*Comments:*

***Question 3***

*(✓)*

<i>Which statement best describes the Service Modification experience you had before taking up your present position?</i>	
Experienced in service modifications	
Adequate service modification experience	
A little service modification experience	
No service modification experience before this role	

*Comments:*

***Question 4***

*(✓)*

<i>Are you required to populate the Safety and Support Questionnaire (SSQ) (MOD F755(SM2))?</i>	
Yes	
No	

*Comments:*

**Question 5**

(✓)

<i>If you answered 'yes' to the previous question, how confident are you that you are sufficiently competent to populate the SSQ?</i>	
Fully confident	
Reasonably confident	
Not very confident	
Not sure	

Comments:

**Question 6**

(✓)

<i>Which statement best describes the Safety Engineering experience you had before taking up your present position?</i>	
Experienced in safety engineering	
Adequate safety engineering experience	
A little safety engineering experience	
No safety engineering experience before this role	

Comments:

**Question 7**

(✓)

<i>How confident are you that you are sufficiently competent to answer questions on Safety Engineering?</i>	
Fully confident	
Reasonably confident	
Not very confident	
Not sure	

Comments:

**Question 8**

(✓)

<i>Do you consider that other persons without an explicitly defined safety role are competent to populate the SSQ?</i>	
Yes	
No	
Not sure	

Comments:

**Question 9**

(✓)

<i>Please indicate your level of confidence in your ability to identify hazards, assess likelihood and severities and allocate tolerabilities.</i>	
Very confident	
Reasonably confident	
Not fully confident	
Not confident at all	

**Question 10**

<i>Please explain what you understand the following terms to mean?</i>	
Airworthiness –	
Safety Case –	
Human Machine Interface –	

**Question 11**

<i>Please explain what you think the difference is between a safety critical system and a safety related system?</i>	
Answer:	

**Question 12**

(✓)

<i>Are responsibilities for system safety well identified within your organisation?</i>	
Yes	
No	

Comments:

**SAFETY CASE AND SAFETY MANAGEMENT SYSTEM QUESTIONS**

**Question 13**

(✓)

<i>What is your knowledge of Safety Cases and what they are used for?</i>	
An excellent knowledge of Safety Cases	
Adequate knowledge of Safety Cases	
A little knowledge of Safety Cases	
No knowledge of Safety Cases	
<i>Safety cases are used</i>	

**Question 14**

<i>Please explain what you think are the contents of a Safety Case?</i>	
Answer:	

**Question 15**

(✓)

<i>What is your knowledge of Safety Management Systems and what are they used for?</i>	
An excellent knowledge of Safety Management Systems	
Adequate knowledge of Safety Management Systems	
A little knowledge of Safety Management Systems	
No knowledge of Safety Management Systems	
<i>Safety Management Systems are used:</i>	

**Question 16**

<i>Please explain what you think are the elements of a Safety Management System?</i>	
Answer:	

**Question 17**

(✓)

<i>Do you know who the Safety Case Manager is for the platform/s that you deal with?</i>	
Yes	
No	

**Question 18**

<i>Please explain what you think the Release To Service document is?</i>	
Answer:	

**Question 19**

<i>Please explain what you think the Release To Service Authority does?</i>	
Answer:	

**Question 20**

<i>Please explain what you think the acronym ALARP stands for and how is it used?</i>	
Answer:	

**Question 21**

<i>Please explain what you think a hazard is and how does it differ to an accident?</i>	
Answer:	

**TOOLS**

**Question 22**

<i>Please explain what you think the term Goal Structuring Notation (GSN) means and what it is used for?</i>	
Answer:	

**Question 23**

(✓)

<i>Have you used Goal Structuring Notation or a similar method before? If you used a method other than GSN what method(s) did you use?</i>	
Yes	
No	
<i>Other methods used:</i>	

**Question 24**

<i>Please explain what procedures, processes, methods and other aids you use to help populate the SSQ?</i>	
Answer:	

**Question 25**

<i>Please explain what procedures, processes, methods and other aids you use to help populate question 6.0.1a of the SSQ?</i>	
Answer:	

**Question 26**

<i>Do you use checklists for analysis?</i> (✓)	
Yes	
No	

Comments:

**Question 27**

<i>Please explain what you think a Hazard log is and how it is used?</i>	
Answer:	

**SAFETY AND SUPPORT QUESTIONNAIRE (SM2) QUESTIONS**

**Question 28**

<i>Do you carry out a feasibility study before starting a new project?</i> (✓)	
Yes	
No	

Comments:

**Question 29**

<i>Do you use scenarios to elicit safety requirements?</i> (✓)	
Yes	
No	

Comments:

**Question 30**

(✓)

<i>Do you perform any risk analysis on your proposed design?</i>	
Yes	
No	

Comments:

**Question 31**

(✓)

<i>Do you define safety-critical requirements?</i>	
Yes	
No	

Comments:

**Question 32**

(✓)

<i>Do you identify and analyse hazards?</i>	
Yes	
No	

Comments:

**Question 33**

(✓)

<i>Do you feel there is sufficient guidance provided to help in answering the SSQ questions?</i>	
Yes	
No	

Comments:

**Question 34**

<i>If you answered 'no' to the previous question please explain why?</i>
Answer:

**Question 35**

(✓)

<i>Does the guidance provided by the SSQ response form help in answering question 6.0.1a on safety?</i>	
Yes	
No	

**Question 36**

<i>If you answered 'no' to the previous question please explain why?</i>
Answer:

**Question 37**

<i>Please explain what you think are the inputs to question 6.0.1a of the SSQ?</i>
Answer:

**Question 38**

<i>Please explain what you think are the outputs to question 6.0.1a of the SSQ?</i>
Answer:

**Question 39**

(✓)

<i>Do you use a glossary of specialised terms when populating the SSQ?</i>	
Yes	
No	

Comments:

**Question 40**

(✓)

<i>Do you have a special lay out for the SSQ document to improve readability?</i>	
Yes	
No	

Comments:

**Question 41**

<i>Please detail what assistance/guidance <b>you</b> would like to help/aid in answering question 6.0.1a of the SSQ.</i>
Answer:

Thank you for taking the time to complete this questionnaire.