Defence Safety Authority

# Manual of Air System Safety Cases (MASSC)

Military Aviation Authority

Military Aviation Authority
MAA

## FOREWORD

1. The purpose of this Manual of Air System Safety Cases (MASSC) is to provide guidance to those organizations required to establish and maintain an Air System Safety Case (ASSC) in accordance with MAA Regulatory Article (RA) 1205[1].

2. The Safety Case regime is widely employed by organizations required to manage operating Risk and is regarded as good practice. The Safety Case regime places the onus on the operator, who understands the system, to identify and manage the Risks associated with their activity, rather than simply relying on prescriptive Regulation alone. To that end, the MASSC initially provides a background on Safety Case theory to highlight the underlying principles behind the implementation of a good Safety Case regime, and to demonstrate that the MAA's Regulation and guidance on ASSCs is based on good practice. However, those organizations and / or individuals responsible for the development of an ASSC who are well versed in Safety Case theory and / or application may wish to proceed directly to Chapter 3 which focuses on the application of this Safety Case theory to military Air Systems.

3. **Chapter 1** provides the context and background as to why the MAA commissioned research into the implementation and effectiveness of ASSCs within the Defence Air Environment (DAE).

4. **Chapter 2** draws on academic views to explore the theory behind Safety Cases, providing the reader with some historical context and how the Safety Case regime applies to the DAE from a regulatorily perspective. This Chapter also highlights the benefits of a Safety Case regime and provides guidance on aspects such as the primacy of the Safety Case argument, through life considerations and the differentiation between the Safety Case and a Safety Case report.

5. **Chapter 3** looks at the application of Safety Case theory to a UK military-registered Air System within the DAE, along with some of the tools and techniques available for developing the ASSC. Annex A to Chapter 3 provides an example of how a structured argument can be constructed following the principles of claim-argument-evidence.

6. **Chapter 4** introduces the Defence ASSC Model and the five key facets[2]; Annex A to Chapter 4 provides an ASSC Operating Context Checklist, whilst Annex B provides an ASSC Assurance framework.

7. **Chapter 5** provides awareness of the common pitfalls associated with Safety Cases, drawing on both the specific example of the Nimrod Safety Case and some of the more generic 'traps' highlighted by Haddon-Cave in the Nimrod Review and by Dr Tim Kelly in his article *'Are Safety Cases Working?'*.

8. The MASSC does not include a separate glossary; any terms or abbreviations not contained within the MAA Master Glossary (MAA02) are explained in full.

[1] Refer to RA 1205 – Air System Safety Cases.
[2] Context, Hazards Managed, Regulatory Compliance, Confidence in the ASSC and Effective Air Safety Management System (ASMS).

**TABLE OF CONTENTS**

**TABLE OF FIGURES**

Intentionally Blank for Print Pagination

# Chapter 1: INTRODUCTION

## REGULATORY CROSS-REFERENCES

1. This chapter must be read in conjunction with the following:

►◄

**RA 1020** – Aviation Duty Holder and Aviation Duty Holder-Facing Organizations - Roles and Responsibilities

**RA 1024** – Accountable Manager (Military Flying)

►**RA 1205** – Air System Safety Cases◄

## CONTEXT

2. The MAA is empowered through the Defence Safety Authority (DSA) Charter from the Secretary of State for Defence to regulate all Air Systems on the UK Military Aircraft Register (MAR). Its vision is *'A world class military Air Safety regulatory and assurance model that is proactive, innovative, modern, efficient and effective'*. It sets out its requirements in the MAA Regulatory Publications (MRP) which apply to all within the DAE, whether military or civilian. This requires those accountable for the Risk to Life (RtL) incurred through the operation of Military Air Systems to use a Safety Case to demonstrate how that Risk is managed. However, within the air domain the term Safety Case has, over time, been applied liberally, inconsistently and with a variety of prefixes, potentially leading to confused, incoherent and thus ineffective Safety Management. Moreover, the practical management of ASSCs has often been an equipment-centric, Defence Equipment & Support (DE&S) Delivery Team (DT) led activity. In the Nimrod Review, the Rt Hon Mr Justice Charles Haddon-Cave QC criticized the length, language and lack of operator involvement with Safety Cases within the MOD. The MAA also recognized that all too often, although through good intentions, ASSCs are simply a repository for the Safety evidence with no coherent thread to link the evidence to the overall Safety argument or claim being made. This is unfortunately consistent with Haddon-Cave's scepticism regarding "warehouses of inaccessible and impenetrable paper". MAA Audits found that the development and utility of a robust ASSC is poorly defined and, consequently, poorly understood, especially during the Acquisition and introduction of new capability into service[3]. The subsequent mitigations required to manage Safety once In-Service often result in limitations or constraints on the operational employment of the capability. Furthermore, the current MRP were largely written to reflect the legacy arrangements under which contractors predominantly operated military registered Air Systems during development, then handed them to the military Front Line Commands (FLCs) to operate them once 'In-Service'. The Regulated Community (RC) and mechanisms used by Defence to deliver capability within the DAE have since evolved and these distinctions no longer correlate reliably with exposure to Risk.

3. Against this context, and in line with its vision, the MAA contracted Niteworks[4] to investigate the links between the MOD's capability development process and the establishment of effective ASSCs, and the development of a new process for governance of activities conducted by Air Systems destined for, or already on, the UK MAR. The Niteworks report[5] concludes that more effective ASSCs and governance of activities for Air Systems on the UK MAR can be delivered through:

a. Clearly defining the development of an argument-based, context-driven, through-life and pan-Defence Lines of Development (DLoD)[6] ASSC in MAA regulatory instruments;

[3] Throughout the MASSC the term 'service', when used in the context of an Air System being 'In-Service' or 'introduced into service', refers to the phase where the Air System has completed development and is now being used to deliver the capability for which it was intended, be that training or operations. It does not refer to use of the Air System by one of the branches of HM Armed Forces (ie the Services – Navy, Land or Air).

[4] Niteworks was established by the MOD to provide a commercially neutral environment in which to address complex Defence challenges through a partnership between MOD, industry and academia.

[5] Niteworks Report NW / PR / 0820 / 014 MAA Regulatory Research Project Final Report dated 21 October 2016.

[6] Defence Lines of Development: Training, Equipment, Personnel, Information, Concepts & Doctrine, Organization, Infrastructure, and Logistics (with Interoperability as an overarching theme).

b. Introducing Regulation to ensure that Air System Safety requirements influence capability Acquisition and direct project sponsors to establish that a capability has the potential to be managed safely across all DLoDs through its life cycle;

c. Broadening regulatory scope to include capability staffs;

d. Adopting a common, Risk-based process for Aircraft classification and registration across the DAE;

e. Enabling MAA provision of an endorsement function at key programme milestones and prior to an Air System registration on the UK MAR;

f. Aligning other Defence policy and guidance to be coherent.

4. The Niteworks recommendations were accepted by the MAA and, where appropriate, have been incorporated into RA 1205 and the MASSC.

5. **Changes to MRP**. As Guidance Material for the production of an ASSC, the MASSC supports RA 1205. Commensurate with revisions to RA 1205, terminology coherency throughout the MRP is captured through business as usual Regulatory amendments. The authority for ASSC terminology is founded within RA 1205 and the MASSC.

## DEFINITIONS

6. MAA02 provides a master glossary of terms and definitions; the following definitions are reproduced here to aid understanding of this Manual:

a. **Air System**. Fixed and Rotary Wing Aircraft, piloted or remotely piloted, and the ground-based systems vital to their safe operation.

b. ►◄

c. ►◄

d. **Air System Safety Case**. A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that an Air System is safe for a given application in a given ►◄ environment. It is through-life, pan-DLoD, and addresses a combination of the physical components, procedures and human resources organized to deliver the capability.

e. ►**Senior Responsible Owner (SRO)**. The single individual with overall accountability for ensuring that a programme meets its objectives and delivers the projected benefits[7] (Cabinet Office Efficiency and Reform Group (ERG) 4 programme management methodology derived).

7. The following definitions are applicable to the MASSC but are not detailed in the MAA02: MAA Master Glossary:

a. **Safety Case**. A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment[8].

b. **Safety Case Argument**. A demonstration of how a system can be deemed acceptably safe from the evidence available.

c. **Safety Case Report**. A document which captures the key components of the ASSC at a particular point in time; it will articulate the Safety Case argument and summarize the supporting evidence in a clear and concise format.◄

8. **Safety Case vs ASSC**. From the definitions above, it can be seen that a Safety Case and an ASSC are essentially the same; an ASSC is simply the Safety Case for a UK Military-Registered Air

[7] ►Where a programme is initially the responsibility of a Capability Development Sponsor, the Sponsor is responsible for discharging the duties of the SRO detailed within RA 1205 and this manual until such time as the SRO is appointed. For clarity, both RA 1205 and this manual refer to the SRO throughout, so as to distinguish the role from that of the Crown Servant Sponsor of a Civilian Owned / Civilian Operated Air System as detailed in RA 1019 - Sponsor of Military Registered Civilian-Owned and Civilian Operated Air Systems - Air Safety Responsibilities.

[8] Refer to DefStan 00-056 - Safety Management Requirements for Defence Systems.◄

System. Within this Manual, the term Safety Case is used when referring to the academic theory of Safety Cases and the generic Safety Case regime as applied to any industry, predominantly throughout Chapter 2. Thereafter, the focus switches to the application of this theory to the DAE, hence the term ASSC is used.

9. ►◄

10. **MOD Acquisition and Investment Approval**

a. **The CADMID Process** ►◄. The MOD Acquisition system utilizes the Concept, Assessment, Demonstration, Manufacture, In-Service and Disposal (CADMID) cycle for through-life project management. ►◄

b. **MOD's Approach to Investment Decisions (MAID)**. Project MAID ►was◄ introduced by the MOD to deliver a more Risk-based and proportionate approach to investment approvals. The MAID process ►introduced◄ a 3-stage approval process consisting of the Strategic Outline Case (SOC), the Outline Business Case (OBC) and the Full Business Case (FBC). ►◄

Intentionally Blank for Print Pagination

# Chapter 2: SAFETY CASE THEORY

## ACADEMIC CROSS-REFERENCES

1. This chapter has been written with reference to the following academic papers; those responsible for the development and maintenance of an ASSC may wish to refer to these documents for further guidance:

b. Charles Haddon-Cave QC. *"The Nimrod Review – An independent review into the broader causes surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006."* The London Stationary Office, 28 October 2009.

c. Inge. *"The Safety Case, its Development and Use in the United Kingdom." Open Source,* 15 November 2007.

d. Tim Kelly. "*Arguing Safety – A Systematic Approach to Managing Safety Cases."* York University, September 1998.

e. MOD. *"An Introduction to System Safety Management in the MOD – Part 2, System Safety in MOD Acquisition."* Issue 4, 2018. (Note: this is widely referred to as *"The White Book"*)

f. MOD. *"Safety Management Requirements for Defence Systems."* Defence Standard 00-56 Part 1, Issue 7, 28 February 2017.

g. Niteworks. "*0820 Military Aviation Authority Regulatory Research Project Final Report."* Report NW / PR / 0820 / 014, 21 October 2016.

## BACKGROUND

### Historical Context

2. Until the Health and Safety at Work Act was introduced into UK legislation in 1974, Safety in the workplace was largely governed by piecemeal Regulations particular to each industry, technology or activity. These Regulations were developed reactively as lessons were learned following Accidents and they detailed specific, mandatory, solutions on how known workplace Risks were to be managed – commonly referred to as 'prescription'. However, ensuring Regulation kept pace with advances in technology and processes was recognized as impractical from a resource perspective. In 1970, Lord Robens was appointed to lead a committee to review the UK government's approach to Safety from which the 1974 Act was developed. This introduced a new legislative framework that took a more holistic view of Safety to ensure that the whole undertaking was addressed rather than only those elements subject to prescriptive legislation. Importantly, this meant it also recognized the Risk to those outside of the workplace who may be affected by its activities. This framework was goal based, setting principles rather than prescribing solutions and while it did not require the adoption of Safety Cases, their use as a means of managing Safety and demonstrating compliance with Regulation became widespread, particularly throughout high-Risk industries[9].

3. Consistent with this change in the regulatory landscape, industry moved away from a Safety approach based on prescription to a Safety Case regime, with the responsibility shifting back toward the operators in order for them to provide a sufficient and acceptable argument for Safety. This approach reflects key tenets of Lord Cullen's report into the *Piper Alpha* disaster[10]:

a. *"Safety has to be organized by those who are directly affected by the implications of failure"*;

b. Safety Cases are *"the means by which the operator demonstrates to itself the safety of its activities"*;

[9] Of note, the Nuclear Installations Act of 1965 had already introduced a licensing regime that required production of Safety Cases during all phases of production.

[10] *Piper Alpha* was an oil production platform in the North Sea which was destroyed on 6 July 1988 following an explosion and resulting oil and gas fires, killing 167 people. The recommendations from the subsequent Public Inquiry chaired by Lord Cullen led to the adoption of the Offshore Installations (Safety Case) Regulations 1992.

c. Safety Cases *"should not be seen as a one-off exercise but as part of a continuing dialogue between the operator and a regulatory body"*.

4. This Safety Case regime, whereby the onus is on the operator to identify and then manage the Risks associated with their activity, is widely employed by organizations to manage Risk, not only because in many areas it is required by Regulation, but because it is widely considered to be best practice. Where activities are considered to be particularly hazardous, a Safety regulator may be appointed to give society added Assurance that organizations creating Risks are managing them effectively[11].

5. It ►is to◄ be noted that whilst the principles of a Safety Case are employed within the commercial aviation industry, the Safety Case regime is implemented slightly differently; separate Safety arguments focusing on the design, Maintenance and operation of the Aircraft are made by the Aircraft manufacturer, Maintenance organization and operator (airline) for their respective areas of responsibility, rather than the single Safety Case owned by the operator as outlined at para 4 above. This approach works because all commercial aviation is conducted within a clearly defined, stable and well-understood context. Conversely, the operating context within which military Air Systems are employed varies significantly with each capability. Moreover, many of the tasks which are undertaken using UK Military-Registered Air Systems, either by the Armed Forces or by contractors, would be considered inherently dangerous, with increasingly complex systems employed in sometimes hostile environments. In order to ensure the Safety of all employees and other personnel affected by such activities, it is essential that Safety is robustly managed, and the most appropriate method to achieve this is via a Safety Case.

**Safety Cases within the Defence Air Environment (DAE)**

6. Applying this context to the DAE, the MOD is normally the 'creator of the Risk' but it is also the 'regulator'[11]; therefore, to ensure that one area is not responsible both for preparing the Safety argument and declaring it as acceptable, the regulator is organizationally distinct within the MOD and effected through the DSA to the MAA. The DSA directs that where a Defence activity presents a credible and reasonably foreseeable RtL, MOD Policy requires specified individuals to be designated as Duty Holders (DHs) to ensure these Risks are both As Low As Reasonably Practicable (ALARP) and Tolerable[12]. Within the DAE, the nominated DHs responsible for managing RtL will be Aviation Duty Holders (ADH)[13] for UK Military Aircraft Operating Authorities (AOA), or Accountable Manager (Military Flying) (AM(MF)) for those contractor organizations which, through the Contractor Flying Approved Organization Scheme (CFAOS)[14], are approved to operate UK Military-Registered Air Systems. The unique operating and operational contexts in the UK DAE, combined with the need (as described by Haddon-Cave in the Nimrod report) for individual accountability for Air System Safety within the military command structure (the DHs) requires the development, management and ownership of a collective and amalgamated Safety argument that integrates platform, people and environment together. The need for flexibility, adaptability, informed military judgment and operationally focused command authority makes this requirement for a collective Safety argument unique when compared with the civil aviation environment.

7. The DSA policy further directs that if the work-related Defence activity takes place on, or involves, a complex system (Aircraft, ship or other complex platform), a simple Risk Assessment will not be sufficient to assess the potential impact on the health and safety of the workforce or public, or impact on the environment. The use of a Safety Case provides the ability to understand the cumulative or interrelated Risks from the use of the complex system and for this to be captured in an argument and a supporting body of evidence[15].

8. But what is a Safety Case? The MOD defines a Safety Case as a *"structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a*

[11] MOD. *"An Introduction to System Safety Management in the MOD - Part 2, System Safety in MOD Acquisition"*.
[12] ►Refer to DSA 01.1 –◄ *"Defence Policy for Health, Safety and Environmental Protection"* ►◄.
[13] ADHs are to be nominated at three levels: Senior Duty Holder, Operating Duty Holder (ODH) and Delivery Duty Holder. In accordance with RA 1205, the responsibility to own and manage a Safety Case for an In-Service Air System rests with the appropriate ODH ►under◄ a military AOA, and the AM(MF) for Air Systems operated under CFAOS.
[14] Refer to RA 1028 - Contractor Flying Approved Organization Scheme.
[15] ►Refer to DSA 01.1◄ Chapter 4 - Risk Management, para 3.

*system is safe for a given application in a given environment"*[16]. This definition, or slight variations thereof, is in widespread use by organizations operating with a Safety Case regime. A simple way of understanding the Safety Case is to consider five basic questions►11◄:

a. What are we looking at? (system description and system operating context)

b. What could go wrong? (Hazard identification and analysis)

c. How bad could it be and what are the major threats? (Risk estimation)

d. What has been done, or can be done, about it? (Risk and ALARP evaluation, Risk mitigation / reduction and acceptance)

e. What if it happens? (emergency and contingency arrangements)

The Safety Case needs to answer these questions for the whole system under consideration for the uses defined.

## SAFETY CASES: AN ACADEMIC VIEW

### The Benefits of a Safety Case Regime

9. The benefits of a strong Safety Case regime, especially if implemented early in a product's life cycle, ensure that:

a. Safety arguments are considered early in capability design and development enabling Safety issues to be eliminated or mitigated through early design modification, thus avoiding difficult and costly re-design or Safety modifications being required once In-Service.

b. The rationale behind the selection or de-selection of certain design features is captured, providing an accountable audit trail and avoiding the potential for subsequent Safety Assessments and / or decisions to be based on incomplete data.

c. Design and test activities are focused on generating evidence originating from the context and Hazards identified.

d. The Safety Case can be used to inform and influence the daily management of the system and enable those responsible for operating the capability to make informed decisions. This includes being able to accept additional Risk in order to achieve an enhanced operational output, or to 'buy back' additional capability for the same level of Risk, because the Safety argument for the clearly-defined baseline context is clearly articulated and understood.

e. Those who are actually responsible for operating and maintaining the system, and therefore know how it really works, understand how their actions support the overall Safety argument, and are able to highlight weaknesses in the Safety argument and / or supporting evidence.

### Defining the Operating Context

10. Kelly contends that a properly constructed Safety Case ►will◄ demonstrate its Safety argument in relation to its particular operating context; indeed, he goes further to state that an argument of Safety is impossible to make without specific consideration of the context of use. This is especially true for systems which can be utilized for multiple activities or be operated in differing environments, as it is difficult to develop a single, convincing claim of Safety without any boundaries. Therefore, before any work is undertaken to develop an explicit argument, the intended or anticipated operating context of the system ►will◄ be defined. This enables likely Hazards from the operating context to be captured in a Hazard identification process. Moreover, it is essential that the intended operators of the system have sufficient influence over the definition of the context for the Safety Case, the identification of operating Hazards, and the development of the subsequent Safety argument. A further benefit of clearly defining the context for the Safety Case is that when a system is subsequently required to undertake new activities or operate in a new environment, ie a change to the context, it is much easier to assess the validity of the existing argument to the new context.

[16] MOD Defence Standard 00-56 *"Safety Management Requirements for Defence Systems"*; Part 1.

**Primacy of the Safety Case Argument**

11. In terms of Safety Case definition, a wide swathe of academic view revolves around the primacy of the explicit argument tied to explicit claims of Safety, relevant to the operating context. Kelly contends that a properly constructed Safety Case ►will◄ clearly demonstrate a comprehensive argument that a system is acceptably safe in its particular operating context. He further depicts the 'Safety argument' as one of three principal elements in a Safety Case with a keystone role in connecting the other two (Safety requirements and Safety evidence – see Figure 2), and offers two important observations:

a. The role of the Safety argument is often neglected, with the emphasis being placed on evidence, leaving the connection between the evidence and requirements unexplained and implicit.

b. An argument of Safety is impossible to make without consideration of the context of use.

12. The relationship between Safety claims, argument and evidence is critical. While the emphasis on an explicit argument is clear, supporting evidence that provides justification that the argument is valid remains important. There is commonality in the view that a Safety Case ►is◄ not ►to◄ be document-centric; indeed, Kelly highlights the danger that the mere existence of documents could provide a false sense of reassurance. This is consistent with Haddon-Cave's scepticism regarding *"warehouses of inaccessible and impenetrable paper"* and *"archaeological document trawl[s]".* Inge notes that *"for complex systems, the body of evidence [supporting the Safety Case] can be vast. For this reason, Safety Cases for reasonably complicated systems are not normally assembled as single physical documents; Instead, Safety Case reports are generated to summarise the argument for safety, and refer out to where the relevant evidence can be found."* Nevertheless, a body of evidence that is sufficiently comprehensive and supports the Safety argument remains a vital element in the overall Safety Case.

13. Kelly expands on the fundamental role of the argument and supporting evidence within the Safety Case, and their symbiotic relationship, as follows:

a. **The Argument**. The argument is the explanation of how the available evidence can be reasonably interpreted as indicating acceptable Safety within the clearly defined context, including demonstration of compliance with requirements and sufficient mitigation or avoidance of all associated Hazards. However, an argument without supporting evidence is unfounded.

b. **The Evidence**. The supporting evidence is the result of observing, analysing, testing, simulating and estimating the properties of a system that provide the fundamental information from which Safety can be inferred. However, evidence without argument is unexplained, regardless of the quality or quantity of that evidence.

14. Haddon-Cave identified that, like a case in law, the Safety Case is a body of evidence presented as a reasoned argument. However, unlike most areas of the law, the activities are not presumed innocent until proven guilty; the Safety Case ►will◄ prove that a system is safe. The legal analogy can be utilized to further illustrate the fundamental role of the argument and supporting evidence: a defence lawyer in court will aim to convince the jury that ►their◄ client is not guilty by presenting an argument which is constructed from, and summarises, the supporting evidence. However, if the evidence is not valid or does not robustly support the argument, then the defence's claim will be shown to be invalid through cross-examination. Equally, the jury will not be convinced simply by the existence of evidence; the argument ►will◄ still be presented to explain why the evidence supports the defence's claim that the defendant is not guilty.

**Safety Cases vs Safety Case Reports**

15. It is important that the difference between the Safety Case itself and a Safety Case Report is understood. Kelly articulates this as follows:

a. The **Safety Case** is the totality of the Safety argument and all of the supporting material, including Test and Evaluation (T&E) reports, validation reports, relevant design information etc.

b. A **Safety Case Report** is the documentation that summarises all the key components of the Safety Case and *references* all supporting documentation in a clear and concise format.

16. The MOD White Book[11] identifies that the purpose of the Safety Case Reports changes at different stages of the system's lifecycle. Early in the lifecycle, a Safety Case Report will aim to show that the Safety requirements and characteristics of the solution are properly understood and that a strategy is in place to manage Safety through the rest of the project. Later, a Safety Case Report will be used to show that planned trials can be conducted safely, and then that the system can be introduced safely into use or mid-life updates can occur. If an incident or accident happens, a Safety Case Report may be needed to show that adequate Safety can still be achieved, through design, upkeep or usage changes if necessary. Finally, a Safety Case Report may be used to show that safe disposal can be made at the end of a system's life. This through-life applicability of the Safety Case is discussed in more detail below.

**Through-Life Safety Cases**

17. Whilst a specific Safety Case Report may be used to articulate the argument that the Air System is safe to operate and being operated safely within the defined context at a particular point in time and maturity of the system, the Safety Case itself will require regular review and will evolve throughout the life of the system. Furthermore, much of the evidence supporting the Safety Case argument will refer to activity being conducted as part of the associated Safety Management System[17], rather than the mere existence of documentation at a point in time.

18. Haddon-Cave identified the purpose of the Safety Case as being *"to inform and influence daily management of a platform … and underpin the aircraft's RTS[18]"*. However, whilst noting such utility for *"use and maintenance during system operation (post commissioning)"*, Kelly observes that Safety Cases are often produced after system design has been finalised, meaning the opportunity for them to influence the design and subsequent operation of the system is missed. Indeed, ►Kelly◄ quotes: *"The Safety Case is to be prepared in outline at presentation of the Staff Requirement and is to be updated at each major procurement milestone up to and including handover … Ideally there should be a seamless development of the Safety Case from one phase to the next."* Straddling these positions, Inge notes the requirement for Safety Cases *"to show that the system is (or will be) designed to be safe, and that this safety is preserved through manufacture, operation, maintenance and eventual disposal".* Consequently, throughout the life of a system from concept to disposal the Safety Case will both demonstrate that a system is capable of being safe, and subsequently be used as a mechanism to support judgement that a system is actually safe.

19. Kelly highlights the utility of a phased Safety Case introduction, adapted to different stages of a project lifecycle as having the following three stages:

a. **Preliminary Safety Case**. Following project definition and initial requirements capture, the preliminary Safety Case will demonstrate the process by which Safety requirements will be met.

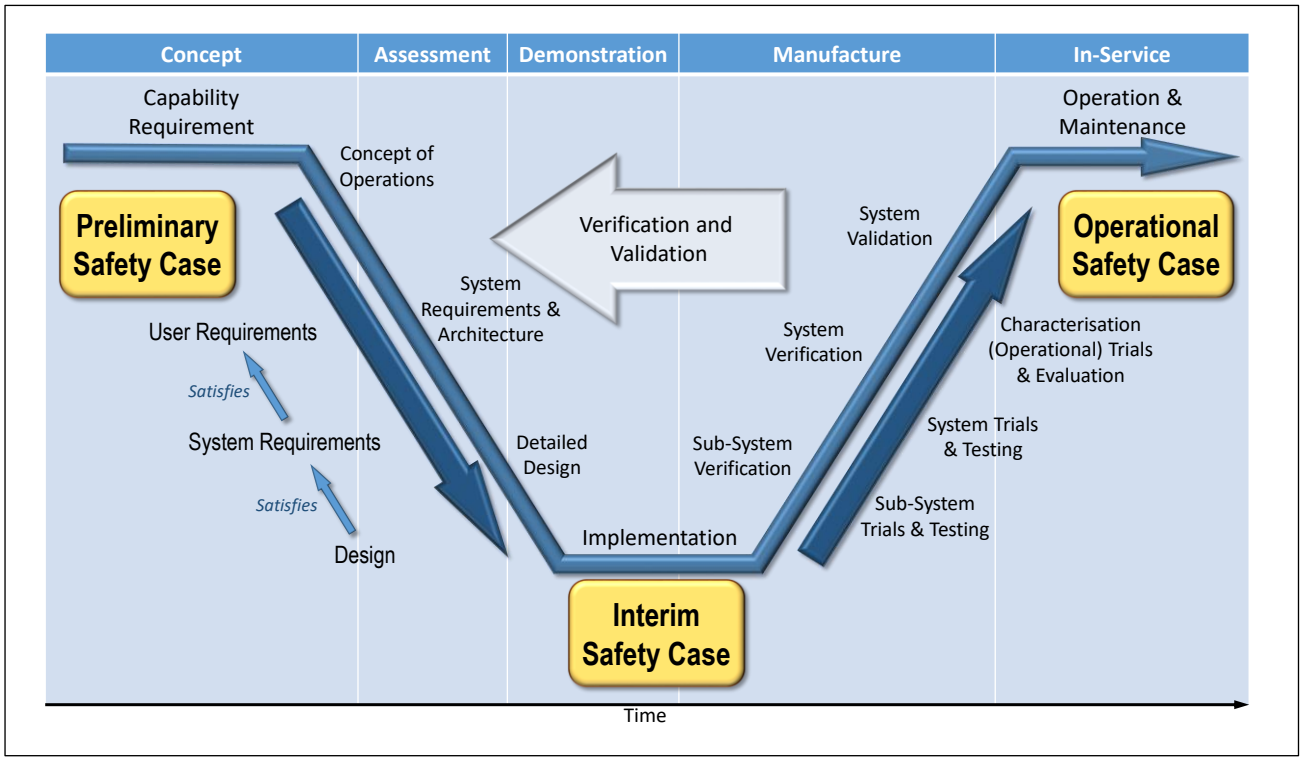
b. **Interim Safety Case**. Following initial design, the interim Safety Case will provide evidence that the Safety requirements are captured in the system specification and will meet the acceptable level of Safety.

c. **Operational Safety Case[19]**. Immediately prior to operation in intended role, the operational Safety Case will capture the full set of arguments and evidence that the Safety requirements have been met.

These stages of the Safety Case development are broadly aligned to the systems engineering 'V' diagram which is widely utilized for systems development and the Integrated Test, Evaluation and Acceptance (ITEA) process as shown in Figure 1 below:

[17] Normally articulated in an associated Safety Management Plan.
[18] Release To Service (See MAA02: MAA Master Glossary). Within the context of the MRP, this quote applies equally to a Military Permit to Fly or a Contractors Flight Limitations Document.
[19] In this context, the term 'Operational Safety Case' refers to the Safety Case for the System once In-Service and being used for its intended purpose, as opposed to the development of the system. This ►is◄ not ►to◄ be confused with the handover of a Military Air System from the ODH to an Operational Commander.

**Figure 1:** *Safety Case lifecycle aligned to a system's developmental lifecycle V-Model*



# Chapter 3: SAFETY CASE THEORY APPLIED TO UK MILITARY-REGISTERED AIR SYSTEMS

## Introduction

1. Having considered the academic view of the Safety Case regime in the previous chapter, this section will look at the application of Safety Case theory to a UK military-registered Air System, along with some of the tools and techniques available for developing the ASSC.

2. The Niteworks report concluded that there was a consistent view across industry that the ASSC should exist during Acquisition, that it should influence design / selection, and that (for MOD Acquisition) the SRO should be responsible for generating it[20]. The report also identified that the earliest sensible point that a (preliminary) ASSC could be understood well enough to inform design / selection was when a mature Concept of Employment for an air capability had been described and a Hazard identification process applicable to the Air System's intended application and operating environment had been undertaken, normally by Initial Gate (IG) ►(now OBC)◄; similarly, the Main Gate (MG) ►(now FBC)◄ and 'commencement of flying' milestones[21] would align with the "Interim" and "Operational" Safety Case points. These stages are synonymous with the Military Air System Certification Process (MACP) and the first two of these stages are broadly captured in the MOD White Book[11] which proposes Safety Case Reports at each key project decision point, with a Safety Case strategy early in the project lifecycle followed by a later report *"showing that planned trials can be conducted … and then that the system can be introduced safely into service."* These generic principles relating to the through-life applicability of a Safety Case have been adopted within the Defence ASSC Model presented in Chapter 4.

## Techniques and Tools - Creating the Argument

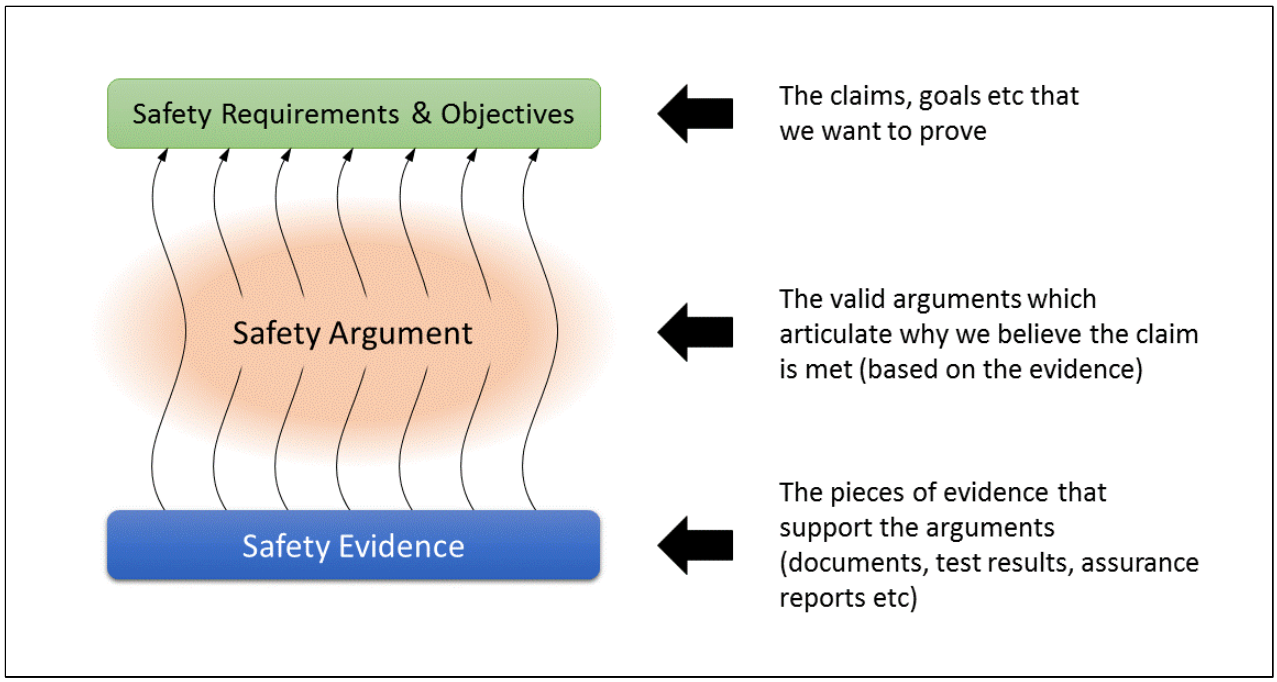
3. As previously articulated and emphasised throughout Safety Case theory, the objective of the Safety Case is to 'pull together' many forms of information and present a coherent, convincing and defensible argument that the system is safe within a clearly defined context, ie that the system is safe for a given application in a given environment. Considering the full spectrum of activity which is, or might be, conducted by military-registered Air Systems, and the need to ensure that the specific ASSC remains proportional to the specific context, there are numerous ways of constructing and subsequently articulating a Safety Case, each with clear benefits and potential pitfalls. As such, the MAA does not prescribe which technique to use when constructing an ASSC, nor provide an exemplar or template which can be 'filled in' with minimal critical analysis. Instead, the intent of the MASSC is to remain solution agnostic and provide guidance on the process and intellectual rigour which needs to be applied to construct a logical argument, and provide flexibility to those responsible for owning and managing the Safety Case with respect to how they achieve this.

4. **'Top-level Claim'**. Before being able to generate an explicit argument, there is a requirement to identify or define the overall Safety claim which will be argued for that Air System; this is often referred to as the overall Safety argument or 'top-level claim' and is likely to be based around the Air System being both safe to operate and operated safely within the clearly-defined context.

5. **Presenting Clear Arguments**. Fundamentally, the ASSC exists to articulate an argument; it is used to demonstrate how the ASSC owner[22] can reasonably conclude that the system is acceptably safe from the evidence presented. Kelly proposed a Safety Case structure consisting of three principle elements: Requirements, Arguments and Evidence[23]. The relationship between these three elements forms the basic argument structure for an ASSC, as depicted at Figure 2:

[20] Ownership of the ASSC is discussed further in Chapter 4, including for civil-initiated procurement of ►Civilian-Owned / Civilian Operated Air Systems destined for the UK Military Aircraft Register◄ which may not have a SRO.
[21] The 'commencement of flying' milestone would indicate that point from which RtL is incurred through the operation of the Air System.
[22] Depending on the stage of development, the ASSC will be owned by either the SRO or by the ADH / AM(MF); ASSC ownership is discussed in Chapter 4.
[23] ►Dr Tim◄ Kelly. "*Arguing Safety – A Systematic Approach to Managing Safety Cases.*" York University, September 1998.

**Figure 2:** *General Form of a Safety Case*




6. Clearly the overall structure of the ASSC will vary depending on the nature and complexity of the system being considered. However, in order to generate a compelling, comprehensible and valid overall Safety argument or top-level claim, it is likely that the top-level claim will be broken down into supporting claims which themselves need to be proven through evidence, or supported by further sub-claims. This approach therefore gives rise to a hierarchy of claim, argument, sub-claims, sub-arguments, and evidence; this structure represents a logical chain of reasoning, by which an overall Safety argument is established to underpin the top-level claim. An example of this hierarchical structure and logical way of thinking is provided at Annex A to this Chapter.

a. **Textual Arguments**. At the heart of the ASSC is the explicit articulation and documentation of this hierarchy of sub-claims which underpin the top-level claim. Whilst this can be achieved through a textural document, such an approach requires a disciplined document structure and clear signposting using section and sub-section numbering to enable the reader to follow the overall argument; furthermore, for large and / or complex ASSCs there is increasing potential for the reader to get lost in the document through multiple cross references, or be left asking ‘so what?’ or ‘how is this relevant to the overall claim?’.

b. **Tabular Structure**. A tabular structure - utilizing separate columns for claim, argument and evidence as depicted at Table 1 - provides clear differentiation between those elements of the argumentation, and shows how the evidence supports each claim or sub-claim through the respective argument; however, for complex systems it can be difficult to clearly articulate the hierarchical structure of the overall Safety argument.

***Table 1:*** *Example of how a Tabular Structure might be utilised to construct the Safety Case and articulate how evidence is linked to a claim though the argument.*

| Claim | Argument | Evidence |
|---|---|---|
| Aircrew are competent to undertake the required task(s) (which have been explicitly defined) | The Aircrew are competent to undertake the required task(s) because: (a) they have been trained, and are qualified, to undertake the required tasks; (b) they are maintaining the minimum level of currency required to safely perform those tasks; and, (c) their competency is being periodically assessed. | Evidence will consist of formal proof that the following sub-claims are valid:<br>• Sub-Claim (a): Aircrew are qualified for the task(s)<br>• Sub-Claim (b): Aircrew are current to undertake the task(s)<br>• Sub-Claim (c): Aircrew are periodically assessed as competent. |
| Sub-Claim (a): Aircrew are qualified for the task(s) | Aircrew are qualified for the task(s) because they have successfully completed an approved training course, which has been delivered by competent instructors using approved facilities, to the required standard. | • Documentation certifying that the training courses meet the Defence Systems Approach to Training (DSAT) Quality Standard.<br>• Documentation that the training courses have been formally endorsed by the Training Requirement Authority.<br>• Formal records that the Instructors are certified as competent to instruct.<br>• Formal Records of Aircrew Qualification (course reports, training folder, logbook). |
| Sub-Claim (b): Aircrew are current to undertake the task(s) | Aircrew are current to undertake the task(s) because the authorization process conducted prior to every flight checks the individual's actual flying currency records against the minimum currency requirements which have been clearly defined and confirmed as appropriate. Moreover, there is sufficient resource available for the maintenance of currency, which is actively managed on the Sqn. | • Flying Orders exist which detail the minimum currency requirements and have been confirmed as regulatory compliant.<br>• Endorsed Annual Flying Task demonstrates that there is sufficient allocation for continuation training.<br>• Aircraft serviceability records demonstrate that Aircraft availability is sufficient.<br>• Evidence that monthly flying logbook checks are being conducted, thus assuring supervisors that Aircrew are achieving minimum currency specified in orders.<br>• Evidence that the Sqn currency tracking tool accurately tracks currency and is being used as part of the sortie authorization process. |
| Sub-Claim (c): Aircrew are periodically assessed as competent. | Argument based on formal proof that the competence of Aircrew is being periodically assessed: | • Flying Orders exist which specify the requirements for periodic assessment of competence and have been confirmed as regulatory compliant.<br>• Evidence that the periodic assessment of Aircrew competence is being conducted in accordance with orders. |

c. **Graphical Notation**. In many situations, it may be easier for Safety Case owners to develop and show the overall Safety argument graphically, an example of which is at Figure 3

Graphical notations are particularly useful as a tool for the construction and articulation of the hierarchical structure for complex Safety Cases. There are a number of recognized techniques for this such as Goal Structured Notation (GSN)[24], and various software tools which may be utilized[25]. However, whilst the overall Safety argument needs to be captured and articulated, the priority is the application of intellectual rigour by appropriate Subject Matter Experts (SMEs) to the construction of a robust argument which will stand up to 'cross examination', rather than a focus on the graphical notation itself. A Safety Case argument constructed by one individual who is an expert at utilizing the full-functionality of a bespoke Safety Case software tool will never be as robust as an argument constructed by a team of SMEs - including operators and maintainers - who really understand how and where the capability is, or will be, employed. As an example, the graphical notation at Figure 3 employs the principles of GSN, but was constructed using nothing more than PowerPoint; equally, this could have been developed on a whiteboard and appropriately captured.

7. **Operator and Maintainer Input**. Regardless of the method employed to construct the structured argument, it is essential to include input not only from the designers, but also from the operators and maintainers who often have the most knowledge and experience about the system and how it is being, or is intended to be, used; moreover, not only will they have a personal interest in the overall level of Safety which has been accepted for the employment of the capability, but they will almost certainly have a role in implementing some of the mitigating factors and providing the evidence to support claims within the overall argument. Therefore, it must be demonstrated that in the development or revision of an ASSC there has been effective consultation with, and effective participation of, those who operate and maintain the Air System in order to facilitate informed opinions about the Risks and Hazards to which they may be exposed or be expected to mitigate[26]. The pitfalls associated with a lack of operator and maintainer input into the development of an ASSC are further discussed in Chapter 5.

**Utility of the Structured Argument**

8. Regardless of the method employed, the initial investment in developing and capturing a robust Safety argument will pay dividends throughout the life of the capability. Initially, the structured argument will be used to identify the evidence required to validate the top-level claim and articulate how and why that evidence supports the overall Safety argument. However, providing that the structured argument and hierarchy of claims is robust and has been captured appropriately, it can serve a number of purposes, including:

a. Requirements setting.

b. Generation and assessment of the Integrated Test, Evaluation and Acceptance Plan (ITEAP) criteria,

c. The structured argument will form the basis for the production of ASSC Reports at key milestones in the project, with references to the supporting evidence.

d. The structured argument can be retrospectively inspected during periodic review as part of the ASSC Assurance process, driving Air System Safety Working Groups (ASSWGs) and underpinning ODH / AM(MF) Safety statements.

e. The structured argument can be used to identify and assess the full impact of weaknesses and / or shortfalls in the evidence, and inform potential mitigating actions.

f. Providing the overriding context for the ASSC has been clearly defined, the structured argument can be used to assess the validity of the ASSC when the Air System is required to undertake a new type of operation or operate in a new environment. If the existing argument and supporting evidence supports the new activity, the overall context of the ASSC can be expanded; if it doesn't, then the ASSC argument can be adjusted and new evidence requirements identified to support the new expanded context. It is likely that the new ASSC argument and evidence for the expanded context would be captured through an ASSC Report.

[24] Further information is available from the GSN Working Group Online: http://www.goalstructuringnotation.info/about.
[25] For examples of GSN software tools see: http://www.goalstructuringnotation.info/archives/41.
[26] National Offshore Petroleum Safety and Environmental Management Authority. *"Safety Case content and level of detail."* N-04300-GN0106 Revision 9 dated October 2015. Available here: https://www.nopsema.gov.au/assets/Guidance-notes/A86485.pdf.

g. The structured argument can be used to assess the potential impact of changes within the pan-DLoD supporting structures on the ASSC; in effect, this would inform an Organizational Safety Assessment from the Air Safety perspective.

h. Perhaps most importantly, the ASSC structured argument can be used to actively manage the Safety of operations, providing it is easily accessible to those responsible for maintaining, operating, and managing the capability.

**The Supporting Evidence**

9. **Identifying the Required Evidence**. Once the structure of the argument has been endorsed by the Safety Case owner, the focus can switch to the generation and maintenance of the evidence that validates each sub-claim; this can be delegated as required to those best placed to manage it, for example the DLoD owners, Squadron Commanders, Instructors, STANEVAL[27], Continuing Airworthiness Manager etc. However, if this delegation is carried out too early - ie before the structured argument has been fully constructed - there is a danger that DLoD owners will operate in stovepipes without understanding what evidence is actually required and why. Exacerbated by the inevitable resource constraints, there is then a temptation for DLoD owners to just focus on the documentation and processes that they already have, anticipate and mitigate the impact of any shortfalls from within their DLoD stovepipe, and then present an argument to the Safety Case owner that their DLoD is fit-for-purpose. Consequently, any overall Safety argument is generated bottom-up, rather than the top-down structured argument that is fundamental to the Safety Case. This results in an 'apologetic' Safety Case built on 'the best argument we can create from the evidence we have', rather than one which proves the top-level claim; this pitfall is particularly relevant for an ASSC being developed retrospectively for an extant Air System, or an ASSC which is only considered as the development of the Air System nears completion.

10. **Repositories of Evidence**. Repositories of evidence, such as multi-tab excel spreadsheets full of hyperlinks to various documents, may be an appropriate way of accessing disparate elements of evidence; however, they are simply an unexplained collection of potentially irrelevant evidence without the clearly-articulated structured argument to demonstrate how and why they support the top-level claim.

11. **Documentation or Activity?** The structured argument needs to identify where multiple elements of evidence, potentially from un-related or cross DLoD sources, support a single claim, and also where a single element of evidence supports a number of claims; this is one of the benefits of a graphical notation such as that in Figure 3. In that example, Aircrew flying logbooks and formal training records (Evidence G) are used to support the claim that the Aircrew instructors are appropriately qualified, and also the claim that the Aircrew are achieving their minimum currency requirements. However, Aircrew logbooks are a living document, which need to be maintained and periodically reviewed in order to be used as evidence to support these claims; as such, another complimentary element of evidence is required to provide Assurance that monthly logbook checks are being conducted by the supervisory chain – hence Evidence I. This demonstrates an important aspect of ASSC evidence in that it includes verbs as well as nouns, ie it ►will◄ include those processes and procedures that are being conducted as well as the documentation that can be produced. This includes supervisory activity, as well as the processes required to review and update any documentation which is being used as supporting evidence; if the review process is broken, then it cannot be claimed that the documentation is up-to-date even if it had been previously endorsed as accurate. This is often referred to as a 'living body of evidence' or an 'up-to-date body of evidence'.

12. **Evidence Owners**. It is important that individuals understand when they are evidence owners, and that they are then responsible for managing the evidence or understanding how their routine activity contributes to the overall Safety argument; this can be achieved through orders, Terms of Reference and / or training, which empower those individuals to highlight when and where weaknesses or shortfalls are identified as part of routine business. Such activity needs to be at the core of the Air Safety Management System (ASMS) supporting the ASSC.

[27] Standardisation Evaluation; normally a unit which conducts oversight and Audit activity to provide Assurance to the chain of command that appropriate standards with respect to instruction, qualification, currency and adherence to orders are being maintained.

# Chapter 3: ANNEX A: CREATING THE STRUCTURED ARGUMENT - AN EXAMPLE

1. This Annex provides an example of how a structured argument can be constructed following the principles of claim-argument-evidence outlined previously. To facilitate this, Figure 3 provides a graphical representation of how a top-level claim has been deconstructed into supporting sub-claims and argument strategies which ultimately identify the evidence which needs to be gathered. However, this particular example follows just one thread from overall claim to supporting evidence; those sub-claims which have been identified but not developed further in this example are clearly annotated as such at Figure 3. The paragraphs below explain: the rationale behind the selection of sub-claims and the argument strategy; the importance of explicitly defining context to avoid ambiguity; and how the evidence validates the hierarchical argument. To aid this process, the column to the left of each paragraph signposts the corresponding element within Figure 3.

2. It ►is to◄ be noted that this Annex is not intended to be used as a template, nor does it attempt to strictly follow the conventions of GSN; indeed, Figure 3, which serves to explicitly articulate the hierarchical structure of the argument, was created graphically using PowerPoint alone. The important aspect to note is the thought process itself which has been employed to create the structured argument and identify the evidence which needs to be generated to substantiate the top-level claim; as useful as the graphical representation is for articulating the structured argument, it is the intellectual rigour that has been employed in its creation that is most important.

**Claim 1**

3. **Top-Level Claim**. The top-level claim being made by the ASSC owner is likely to be along the lines of *'the Air System is acceptably safe for a given operation in a given environment'*. Whilst such a claim may appear clear on first inspection, any attempt to develop the supporting argument is almost certainly destined to fail without further clarification of context. Potential pitfalls include missing certain aspects of capability, operation or operating environment, or by trying to create an argument that the Air System and all of its associated capabilities are acceptably safe for *all* methods of employment in *any* operating environment, which is simply unrealistic. Further objective assessment of this top-claim identifies four elements which need explicit definition – ie defining the context for the ASSC:

**Context 1a**

a. **Air System**. The first element is the Air System itself, which simply refers to the specific Aircraft type or Remotely Piloted Air Systems; or does it? Within many military Air System fleets some Aircraft have additional modifications and capabilities, and many operate with role equipment, weapons and / or Airborne Equipment[28]. Some of these additional capabilities are likely to require specific requirements within a number of the DLoDs and potentially additional or bespoke mitigations to ensure their employment remains acceptably safe; for example, certain capabilities (Night Vision Device (NVD) operations, air-to-air refuelling) might require crews to have additional training, qualifications and currency, or may only be employed on certain operations and / or in certain environments. Whilst such nuances can be accommodated in a single structured argument supporting the top-level claim, it may be more appropriate to sub-divide this claim for certain capabilities or environments which might otherwise distort or overburden the overall strategy. Either way, fundamental to the subsequent analysis is a clear explicit definition of what constitutes the Air System that is endorsed by the ODH / AM(MF) who is ultimately making the ASSC Safety argument.

**Context 1b**

b. **Acceptably Safe**. What constitutes acceptably safe? Essentially, this can only be decided by the ODH / AM(MF) who is required to confirm that all Risks have been reduced to ALARP and that the residual Risk is assessed as Tolerable, balancing the residual Risk against the reward. An understanding of the Risk owner's approach to this Risk-versus-reward balance will be key to developing the argument strategy and shaping the supporting claims. Some capabilities, operations or operating environments might attract a different Risk versus reward argument, and thus warrant a bespoke sub-claim and argument strategy.

[28] Including Airborne Forces Equipment (AFE) and Aerial Delivery Equipment (ADE).

Context 1c & Context 1d

c. **Nature of Operation** and **Operating Environment**. Rarely will an Air System be employed on a single type of operation, or be operated throughout its In-Service lifetime in the same operating environment for which it was originally procured; yet a single claim that the Air System is acceptably safe for all operations in all operating environments is likely to be unconvincing. As part of the ASSC context, it is therefore essential to clearly define the nature of operations and the operating environments for which the claim is made. A further benefit of doing this is that when the Air System is subsequently required to be employed on a new type of operation, or if the extant capability is required to be employed in a new operating environment, it is easier to identify that this falls outside of the scope of the existing argument. Appropriate objective analysis can then be conducted to 'cross-examine' the existing ASSC argument and supporting evidence to ensure that it adequately supports the top-level claim for the new, expanded context. If not, an additional argument strategy can be developed, focusing on the deltas that the new operation or operating environment has introduced.

Having clearly defined the context for the top-level claim, this can be deconstructed into supporting arguments or sub-claims; the two most common sub-claims for an ASSC (within the explicit context defined for the top-level claim) are that the *'Air System is safe to operate'* and that the *'Air System is being operated safely'*.

Claim 2

4. **Air System is Safe to Operate**. The strategy to support the 'safe to operate' claim is fundamentally an argument about Airworthiness and is likely to focus on the up-keep of type design to an acceptable standard. This claim is not developed further in this example.

Strategy 2

Claim 3

5. **Air System is being Operated Safely**. For this example, the sub-claim that the Air System is being operated safely is supported by a two-pronged argument strategy: the first concerns 'how' the Air System is operated and focuses on aspects such as governance, supervision, orders and the competence of operators; the second is concerned with 'where' the Air System is operated and focuses on aspects such as the airfield(s) and the airspace environments being acceptably safe for the operation of the Air System. Both of these argument strategies would encompass aspects from across the DLoDs; however, for the purposes of this example only the first argument strategy is developed further, with a focus on the training DLoD supporting 'how' the Air System is operated. Three further sub-claims have been chosen to support this argument:

Strategy 3a

Strategy 3b

Claim 6

a. **Orders and Procedures**. Orders and procedures are in place with clearly defined limitations which enable the required operations to be conducted safely (in line with the overall context previously defined). To support this claim, three further sub-claims have been chosen:

Claim 11

(1) "Orders are regulatory compliant and written to mitigate hazards". Clearly, to enable the orders to be written in such a way as to mitigate the Hazards, there is an assumption that all credible Hazards have been identified; this assumption would need to be justified elsewhere within the overall Safety Case, most likely through the ASMS supporting the ASSC. With this caveat accepted, it is now possible to generate the evidence to support this claim; this is likely to include evidence of:

Assumption 11

Evidence A

- The formal endorsement and publication of the orders by the respective AOA.

Evidence B

- An effective periodic review and amendment process for the orders.

Evidence C

- 1st / 2nd and 3rd party Assurance activity confirming that the orders comply with the regulations, and that the orders clearly articulate the limitations and / or procedures required to mitigate the identified Hazards.

Claim 12

(2) "All flying activity is conducted in accordance with the Orders". Clearly, having the appropriate orders as per Claim 6 above is only half of the equation; the orders need to be readily available and understood by those operating the Air System, and any flying activity also needs to be conducted in accordance with

Strategy 12

them. Consequently, an argument strategy based on evidence of active supervision and STANEVAL[27] Assurance activity has been chosen to support this sub-claim, but this is not expanded further in this example.

Claim 13

(3) ”Fully-substantiated Air System Document Set (ADS)”. The Air System can only be operated and maintained safely if there exists an ADS which describes the safe operating limitations, safe operating procedures and safe Maintenance procedures. This sub-claim therefore supports both the Safe to Operate and Operated Safely argument strategies. However, the subsequent argument strategy cannot just focus on the existence of the ADS itself; it also needs to provide evidence that the ADS is subject to periodic review, and is amended through-life to ensure that it continues to reflect the as-flown and as-maintained configuration of the Air System; this claim is not developed further in this example.

Claim 7

b. **Authorization and Supervision**. All operations are correctly authorized and supervised; assuming this claim is proven valid (through supporting evidence), this is a key argument that internal procedures are in place to ensure that each sortie is conducted in accordance with the published orders and procedures, and that the operating crew is meeting the prescribed competencies for the task; this claim is not developed further in this example.

Claim 8

c. **Aircrew Competence**. For any Air System, whether manned or unmanned, the claim that ‘All operating Aircrew are Competent (ie Suitably Qualified and Experienced ►Person◄ (SQEP))’ will almost certainly be a fundamental component supporting the argument that the Air System is being operated safely. However, the context for which this claim is being made ►is to◄ be defined. First, what are the Aircrew roles which constitute the basic and operating crew of the Air System, and is this the same for all tasks and / or operations? (links to Context 1c). Second, what competencies are required to deliver the necessary capabilities or operations with the acceptable level of Safety? Both aspects need to be clearly defined and understood to enable the subsequent strategy, which argues competency based on both qualification and currency, to be implemented. Fundamental to such a strategy is a clear definition of what constitutes the minimum level of qualification and currency for normal, emergency and role-specific tasks. Having defined the context for the claim that all Aircrew are competent, the supporting strategy based on qualification and currency can be further deconstructed into three further sub-claims: that all Aircrew are qualified, that they are maintaining the minimum level of currency, and that their overall level of competence is being periodically assessed.

Context 8a

Context 8b

Context 8c

Strategy 8

Claim 14

(1) **Aircrew Qualification**. Even with a clearly defined set of required qualifications, not all Aircrew will arrive on a unit fully-qualified to undertake all of the tasks which will be required of them during their tour; moreover, by their very nature training units will be required to fly un-qualified personnel as part of the crew. As such, validating the claim that all Aircrew are qualified is likely to prove unrealistic. Conversely, the claim that all aircrew are *either qualified or are undergoing instruction by qualified instructors* both reflects reality and has a realistic prospect of being supported by evidence. However, to do this, it is important to differentiate between that training which falls within the remit of the ASSC and those qualifications which are achieved through external training units; whilst the ASSC needs to include evidence of such a qualification having been awarded through external training units, it might be unrealistic to try and justify the award of the qualification itself. Instead, the ASSC can articulate the interface with these external training providers, the agreed course content and the required standard to be met for the award of the qualification. Where this approach is adopted, there also needs to be evidence of a robust plan for the external training unit to communicate any shortfalls in the training, such that the ASSC owner can assess the impact on the overall ASSC. It would also be reasonable to expect the receiving unit to conduct an arrival check on new arrivals, which can be documented as part of the evidence supporting this claim. For that training, which is delivered within the context of the ASSC, this claim has been deconstructed into two further sub-claims: that the *‘training facilities are appropriate’* and that the *‘training is delivered by qualified instructors’*:

Claim 17

Context 17a & Context 17b

Evidence D

Evidence E

Claim 18

Evidence F

Evidence G

Claim 15

Claim 19

Evidence G

Evidence H

Evidence I

(a) **Training Courses and Facilities**. Training courses, devices and facilities are appropriate and fit-for-purpose. In order to support this claim, it will be necessary to clearly define what the training objectives are, and what the acceptable output standard from the training course is. Having defined these, it is now possible to generate the evidence to support this claim; this is likely to include evidence that:

- The training courses are certified in accordance with the Defence Systems Approach to Training Quality Standard (ie that the content of the courses is being delivered appropriately).
- The training courses have been endorsed by the Training Requirements Authority (ie that the courses are delivering the right output).

(b) **Instructor Qualifications**. The claim that all training is provided by qualified instructors can be supported by the following evidence:

- Certificate of Competence to Instruct issued / endorsed by the appropriate examining body, an appropriate Instructor Rating issued by civilian regulator, or equivalent.
- Formal records of initial instructor qualification and periodic validation in aircrew training records, Form 5000, Logbook or equivalent.

(2) **Aircrew Currency**. Alongside qualification, the claim that all Aircrew are maintaining the minimum level of currency (as defined at Context 8c) is fundamental to the argument strategy based around operator competency. There are a number of ways to validate such a claim; for this example it has been decided to separate live and synthetic training, and to substantiate each sub-claim through evidence that the resources are being made available and that they are actually being utilized.

(a) **Live Flying Resource**. Having identified the amount of live flying required to maintain competency for the required flying tasks across the crews, this needs to be reflected in the Annual Flying Task (AFT) for the fleet. Clearly, if there are not enough hours allocated to enable the crews to maintain the minimum currency, then the claim cannot be justified, and the supported argument unravels. This is particularly important where specific competencies require crews to practice skill sets that they might not achieve on current or routine operations, even though such operations may be delivering sufficient live flying in terms of flying hours. The minimum currency (defined at Context 8c) needs to truly reflect the competencies required, not just a simplistic hours-based minimum. Furthermore, having sufficient capacity within the AFT to achieve the minimum currency ‘on paper’ is only half of the argument; the mechanisms also need to be in place to enable the crews to actually achieve this flying task. However, it ought to be relatively straightforward to generate the evidence to support this claim:

- Formal Aircrew training records, eg Logbook or equivalent which clearly show the amount and nature of the live flying completed.
- Formally endorsed AFT which demonstrates that sufficient live flying has been allocated, supported by actual Aircraft availability data and sortie records which shows that sufficient flying is being achieved.
- Periodic Flying Logbook Checks. Evidence that the supervisory chain is periodically reviewing each Aircrew member’s flying logbook,

with appropriate mechanisms in place for highlighting and mitigating any deficiencies.

Evidence J

- Squadron Currency Tracking Tool providing up-to-date data regarding the currency of each crewmember with regard to live flying requirements; evidence that this tracking tool has been periodically validated for accuracy and that it is being used as part of the flight authorization process.

Claim 20

(b) **Synthetic Training**. Synthetic training devices are appropriate, available, and being utilized to maintain the minimum level of currency. The synthetic training environment is an important element in the development and Maintenance of capability, providing a low-Risk training environment which can be used for ab-initio training, continuation training, tactics development and mission rehearsal. However, synthetic training encompasses a wide spectrum of activity utilizing numerous training devices, from the simple 'cardboard cockpit', through computer-based training, desk-top emulators, procedural trainers, rear-crew trainers and the 'zero flight hours' full-motion flight simulators. Consequently, the utility and employment of each device ►will◄ be clearly understood and articulated. It is essential that the synthetic training devices are suitable to deliver the required training output, that they represent the actual Air System and / or operating environment with sufficient accuracy, and that the limitations of any such devices are accepted and appropriately mitigated.

Context 20

Evidence J

- Squadron Currency Tracking Tool providing up-to-date data regarding the currency of each crewmember with regard to synthetic flying requirements; evidence that this tracking tool has been periodically validated for accuracy and that it is being used as part of the flight authorization process.

Evidence K

- Evidence of the certification / qualification of the synthetic training devices relative to the training which is required to be conducted; evidence of periodic assessment to confirm on-going suitability of the training devices.

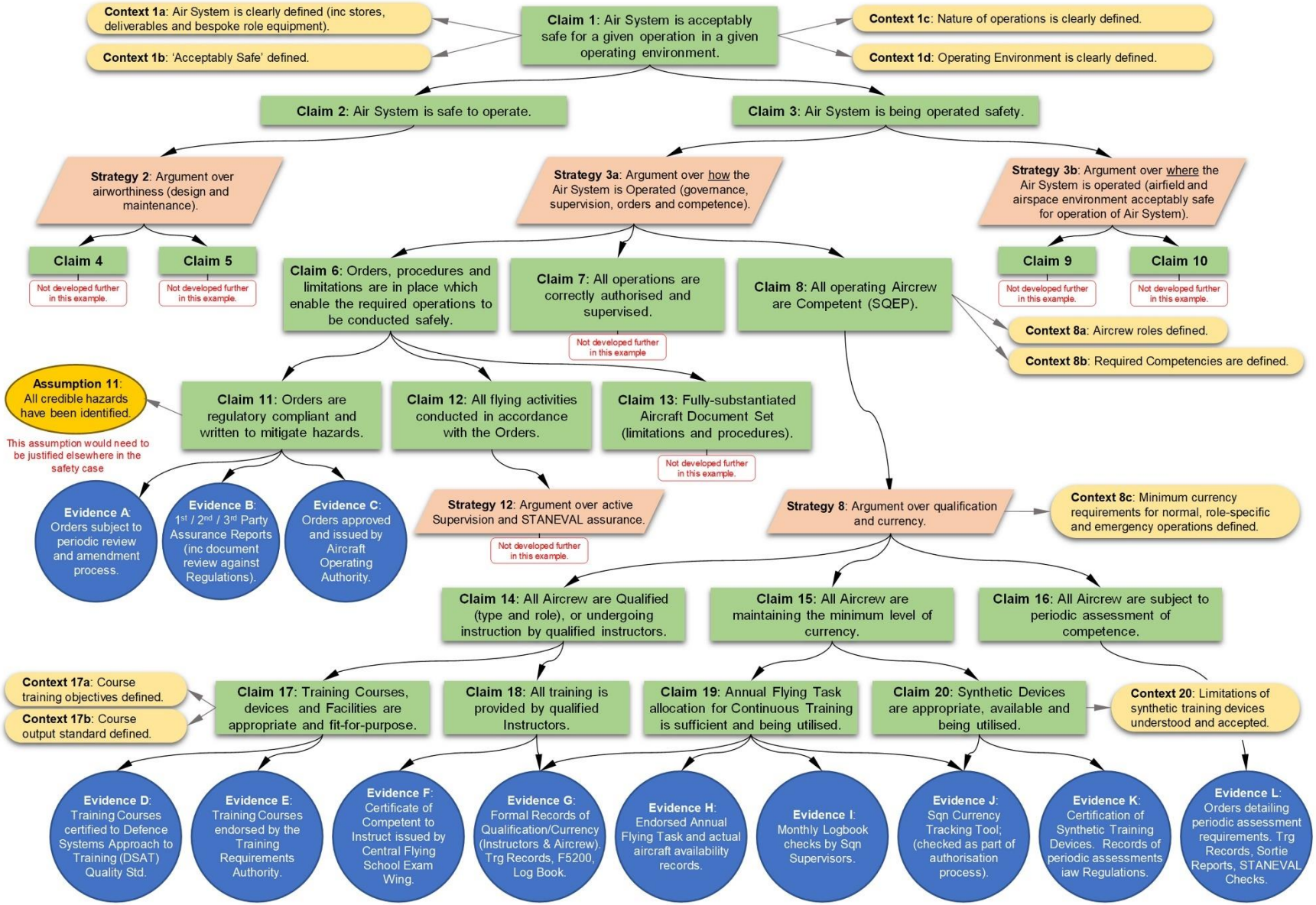
Claim 16

(3) **Periodic Assessment of Competency**. In addition to qualification and currency, the third element of the Aircrew Competency argument (Strategy 8) is the sub-claim that all Aircrew are subject to periodic assessment of their competence in role. Aircraft handling checks, Instrument Rating Tests, role checks and STANEVAL check flights are all examples of activity designed to assess Aircrew competence. The evidence that this activity is being conducted ought to be readily available:

Evidence L

- Evidence of the orders which specify the requirement to conduct periodic assessment of competency in role, and Aircrew training folders containing the sortie report forms from such checks.

**Figure 3:** *Graphical Example of the Structured Argument Thought Process (not intended as a template)*



# Chapter 4: THE DEFENCE AIR SYSTEM SAFETY CASE MODEL

## REGULATORY CROSS-REFERENCES

1. This chapter must be read in conjunction with the following:

**RA 1200** – ►◄ Air Safety Management.

**RA 1205** – Air System Safety Cases.

**RA 1210** – Ownership and Management of Operating Risk (Risk to Life).

## BACKGROUND

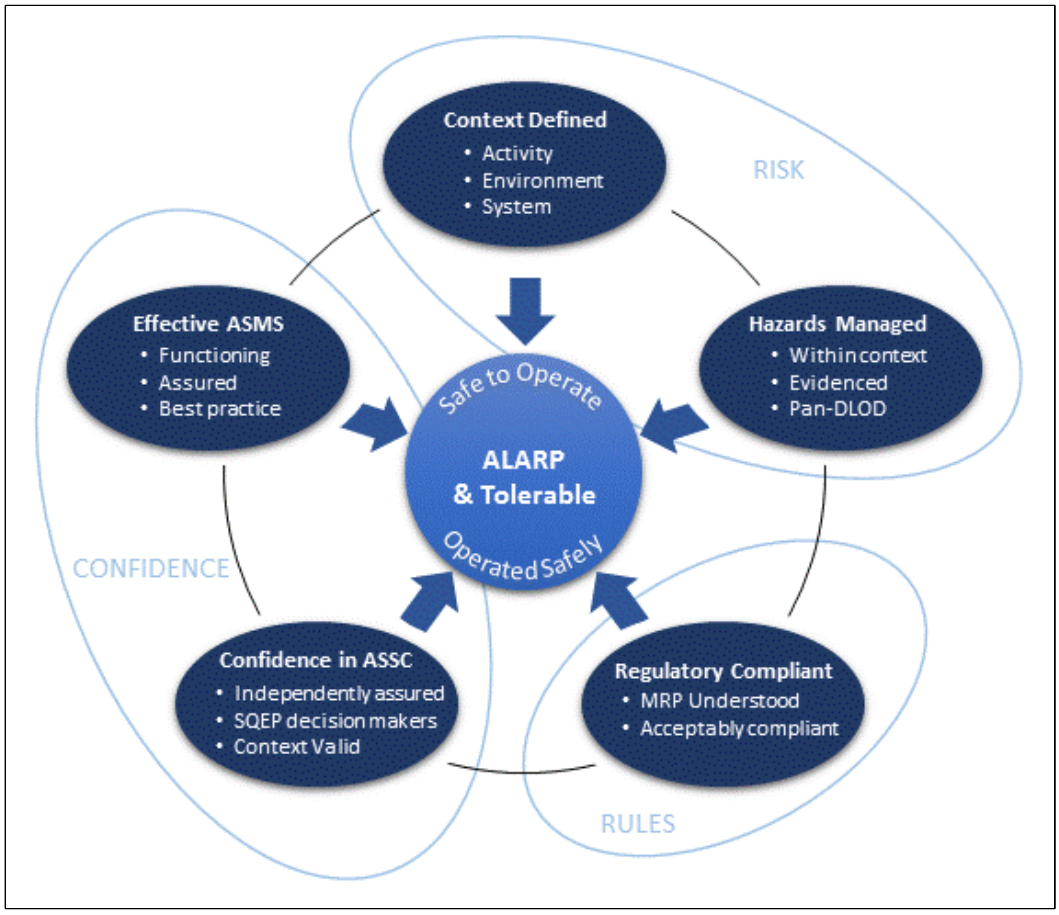
2. **ASSC Model**. In conjunction with Niteworks, a high-level ASSC Model has been developed by the MAA which recognizes:

a. The duality of the central hub's argument; both 'safe to operate' and 'operated safely'.

b. That operating context is critical to Hazard management.

c. That the overall Safety argument is dependent on three areas: the importance of Hazard / Risk Management (the overwhelming focus of Haddon-Cave's recommendations); compliance with Safety Regulation, and confidence in the Safety processes and governance which delivers the evidence to support it. Within these three domains of Risk, Rules and Confidence, 5 key facets were identified and developed. The resultant Defence ASSC Model is depicted at Figure 4 below:

***Figure 4:*** *The Defence ASSC Model*




3. **Central Hub - The Top-Level Claim**. At the core of the Defence ASSC Model is the Central Hub, which contains the two principle components of a top-level claim: that the Air System is Safe to Operate and being Operated Safely (within a clearly-defined context, as discussed in para 4a below). This top-level claim includes both the technical aspects of being safe to operate, ie an argument of the Air

System's Airworthiness - and the functional aspects that it is operated safely ie how and where the Air System is operated. The top-level claim is decomposed into supporting argument strategies and sub-claims, which ultimately identify the evidence which needs to be gathered. With a structured argument and supporting evidence which prove the top-level claim, the ASSC owner can declare that the Air System is both safe to operate and being operated Safety, and that the associated Risks are being managed to a level that is both ALARP and Tolerable in accordance with RA 1020 and RA 1024[29].

4. **The Subordinate Facets**. Surrounding the central hub of the Defence ASSC Model are five subordinate facets which are considered briefly in the following paragraphs. The intent is that each facet constitutes an area of focus for internal or external review / Audit of the ASSC, and the basis of an explicit Safety argument. In their totality, they ought to provide confidence that the overall ASSC argument is both valid and complete.

a. **Context**. The ability to make any effective argument depends on the existence and understanding of context; this includes the system itself, the capabilities and activities required to be delivered by the system, how they will be achieved, and the environment(s) in which the system will be required to operate. An ASSC Operating Context checklist is provided at Annex A, which allows a straightforward capture of the fundamental characteristics required of the future Air System based on its intended usage. The early definition of the Air System's characteristics and intended use will enable the core Safety requirements to be derived for integration into the User Requirements Document (URD)[30] and the operating Hazards to be identified. These can then be used to cross reference the System Requirements Document (SRD)[31] and / or Contracted System Requirements Document (CSRD)[31] in order to trace the Safety requirements through ITEA, and begin to manage the Hazards.

b. **Hazards Managed**. This reflects the criticality of Hazard identification, analysis and mitigation in the context of intended use, as so strongly emphasised by Haddon-Cave. Hazard Management does not deliver an argument in itself, but it is a critical facet in understanding Risk and therefore needs to be a vehicle for an argument surrounding gross disproportion, prioritisation of resources, operational imperative and the impact of shortfalls in other facets of the ASSC. Hazards ►will◄ be analyzed through a pan-DLoD process of identification, mitigation and review, right from the very earliest stages of an Air System's gestation and subsequently through-life, noting that threats to Air Safety that emanate from the Air System's design may ultimately rely to some (or even a great) degree upon operating procedures (and, therefore, operator training) for mitigation of the RtL. Equally, Hazards induced by the possibility of operator / maintainer human error may rely upon certain features of an Air System's design for mitigation of the associated RtL. Experience has shown that these inter-DLoD dependencies are often missed.

c. **Regulatory Compliance**. Compliance with Regulations is a critical step in making a Safety argument. To an extent, the same argument applies to Military Air Orders and Civil Ops Manuals. This facet requires explicit reference to *inter-alia* Alternative Acceptable Means of Compliance (AAMC), Waivers and Exemptions.

d. **Confidence in the ASSC**. This provides the justification that the Safety argument and supporting evidence can be relied upon. It requires Assurance that appropriate SQEP have been responsible for the evidence gathering and analysis of Safety related data during development through the ITEAP, and then for the ongoing periodic review of the argument and management of the supporting evidence. It also includes feedback from internal and external oversight and Assurance of the ASSC. It also needs to demonstrate that development of the ASSC has been informed by related best practice on other Air Systems.

e. **Effective ASMS**. An organization's ASMS is symbiotic to the ASSC for each Air System operated by that organization; indeed, it can be argued that the tangible output of an effective ASMS is evidence which supports the ASSC, whilst the intangible output is a safer system. The ASMS provides the management function for the Safety processes and artefacts that support the

[29] ADHs refer to RA 1020 – Aviation Duty Holder and Aviation Duty Holder-Facing Organizations – Roles and Responsibilities; AM(MF) refer to RA 1024 – Accountable Manager (Military Flying).
[30] The User Requirements Document defines what outcome or effect is needed, in what quantity, how effective and by when.
[31] The System Requirements Document / Contracted System Requirements Document defines what is needed, by how much, at what level of performance and when – taking all DLoDs into consideration.

overall Safety argument for each Air System. To achieve this, it needs to be functionally effective, rather than merely described on paper, and a learning system, continually improving in light of lessons identified. Just as the nature of the ASSC will change throughout the lifecycle of the Air System, so the ASMS will need to evolve to ensure that the supporting evidence remains valid; a key aspect to this is the clear articulation and maintenance of effective interfaces with the ASMS of supporting organizations such as Contractors, Coordinating Design Organizations, T&E Units, end-user etc. There will also be a requirement to revisit the ASMS requirements during major change programmes.

## APPLICABILITY OF THE ASSC

### Pan-DLoD Applicability of the ASSC

5. Historically, the Equipment DLoD has been subject to disproportionate emphasis in relation to other DLoDs, exacerbated by incorrect reference to the Equipment Safety Assessment (ESA) as the Equipment Safety Case and then conflating this with the overall ASSC. Moreover, as a consequence of resource constraints, efforts to satisfy one aspect of the ASSC argument and generate the supporting evidence can be detrimental to the development to other aspects of the argument, resulting in a significant degree of separation and / or incoherence within an ASSC. The Niteworks research concluded that the separation of single (equipment) Risks from unified Risk in many ASSCs reinforces the separateness of the Equipment-DLoD, making it difficult to connect an ESA to an explicit pan-DLoD Safety argument, masking the thread to the ALARP and Tolerable judgement and overall claim of Safety[32]. In order to develop and maintain a coherent, robust and effective ASSC which enables the operational capability to be delivered safely, the ASSC ►will◄ include pan-DLoD applicability.

### Through-Life Applicability and Development of the ASSC

6. Applying the through-life considerations of a Safety Case discussed in Chapter 2 to the CADMID[21] cycle of an Air System, the ASSC would be required to fulfil the following specific functions, with the argument for each captured through Safety Case Reports at key milestones[33]:

a. **ASSC Strategy**. At the Concept Phase, there will be an *ASSC Strategy* to establish that the capability has the potential to be managed safely across all DLoDs through its lifecycle. The associated ASSC Strategy Report (at ►OBC◄) must demonstrate that the proposed Air System and the associated processes and measures described are likely to be capable of supporting effective ALARP and Tolerable judgments. This ASSC Strategy Report will be subject to endorsement as per RA 1205.

b. **ASSC Acquisition Basis**. As the Air System matures through the Assessment Phase there will be an *ASSC Acquisition Basis* to establish how the pan-DLoD Safety requirements have been identified and how they will be substantiated. The associated ASSC Acquisition Basis Report (at ►FBC◄) will demonstrate that the operating Risk management processes and their artefacts have influenced capability design / selection. This ASSC Acquisition Basis Report will be subject to endorsement as per RA 1205.

c. **Live ASSC (► Development ◄)**. At the commencement of T&E flying, there will be a *Live ASSC (► Development ◄)* which demonstrates through claim, (explicit) argument and (appropriately cited) evidence by the T&E ODH / AM(MF) that the Air System is safe for the conduct of T&E flying and that the associated RtL is reduced to both ALARP and Tolerable. The associated ASSC Report(s) will demonstrate that the processes are actually supporting effective ALARP and Tolerable judgments. The Live ASSC (► Development ◄) Report will be subject to endorsement as per RA 1205.

d. **Live ASSC (In-Service)**. At the point that the Air System enters service, there will be a *Live ASSC (In-Service)* which demonstrates through claim, (explicit) argument and (appropriately cited) evidence by the ODH / AM(MF) that the Air System is safe for the conduct of operations and that the associated RtL is reduced to both ALARP and Tolerable. The associated ASSC Report (at In-Service Date (ISD) and periodically thereafter) will demonstrate that the processes

[32] Niteworks Report NW/PR/0820/014, Chapter 4 Para 4.4.2, page 38.
[33] Niteworks Report NW/PR/0820/014, Annex A, Para A.5, pages 94-95.

are actually supporting effective ALARP and Tolerable judgments. The Live ASSC (In-Service) Report associated with ISD will be subject to endorsement as per RA 1205.

7. This phased development of the ASSC through the CADMID cycle is presented at Figure 5, along with a graphical depiction of ASSC ownership, which is discussed in the following paragraphs.

**ASSC Ownership**

8. Having identified that the ASSC is required to fulfil a number of functions throughout the life of a capability, it follows that there needs to be a clearly identified owner of the ASSC at each stage of its development. However, due to the nature of Defence procurement and capability development, ASSC ownership is best conducted through a supported-supporting relationship, as depicted at Figure 5 and described in the following paragraphs.

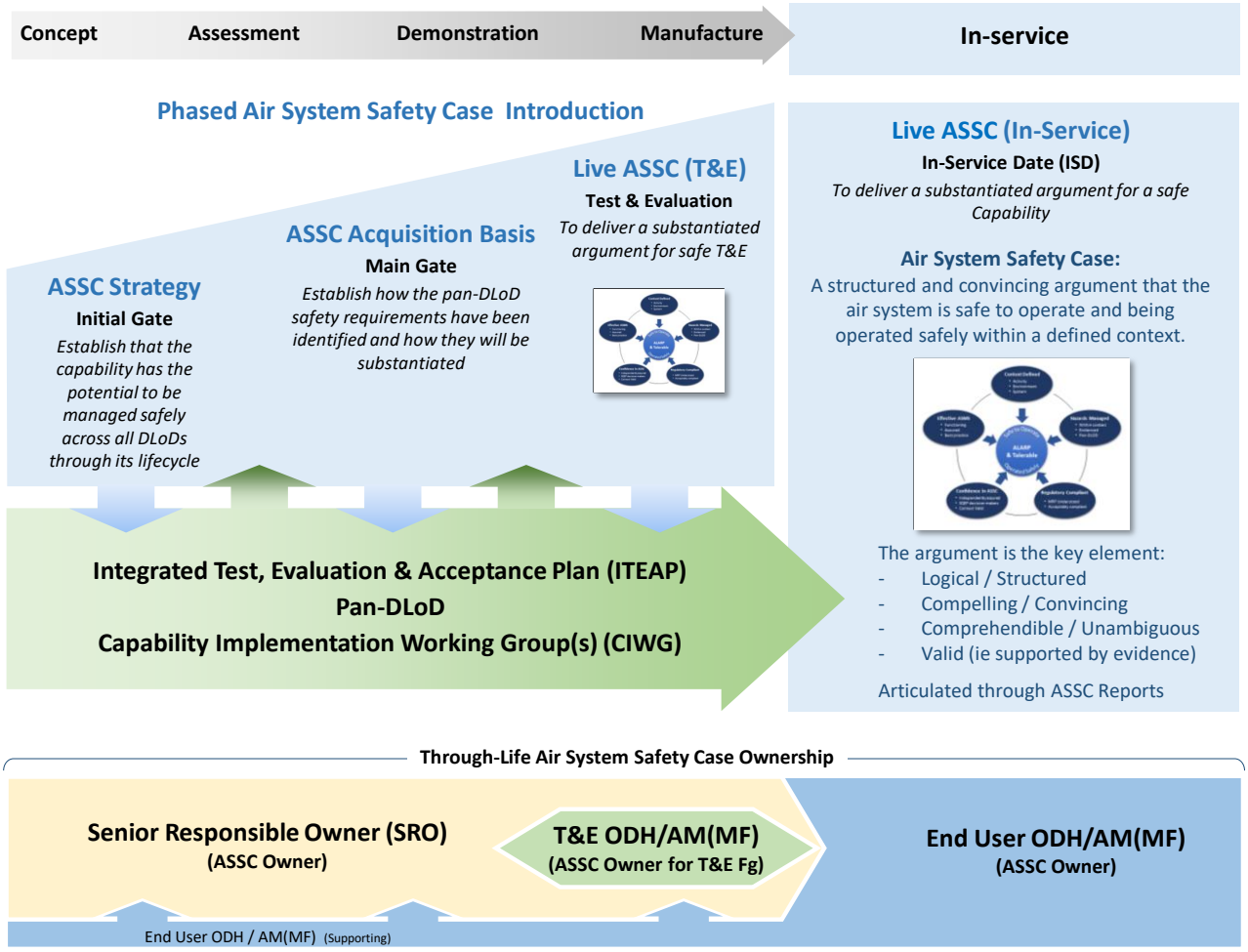
9. **Development of the ASSC**. Initially, the ASSC will be owned and managed by the SRO[34] responsible for the Acquisition of the capability. The associated ASSC Strategy and Acquisition Basis Safety Case Reports[35] need to deliver an overall argument that the ASSC (or its artefacts) are capable of supporting effective future ALARP and Tolerable judgments and demonstrating how it has supported identification and capture of role-related Safety requirements. As such, early and ongoing engagement between the SRO responsible for the Acquisition of the capability and the end user ODH / AM(MF) is essential. The role-related Safety requirements and evidence gaps identified will inform the ITEAP which, through the T&E activity, will gather the evidence required to support the ASSC argument as it matures. Prior to operation of the Air System In-Service, ownership of the ASSC will be transferred to the end-user ODH / AM(MF); at this point the Live ASSC (In-Service) ►is to◄ consist of a structured argument and all the supporting evidence to support the overall Safety claim for the In-Service flying.

10. **T&E Flying**. Where an Air System is undergoing T&E flying as part of initial development or modification, the ODH / AM(MF) responsible for the T&E flying will be required to own and manage a separate Live ASSC (►Development◄) specific to the context of the T&E flying; this Live ASSC (►Development◄) is required to deliver an overall argument that the T&E flying activity is both ALARP and Tolerable. The Live ASSC (►Development◄) will therefore exist in parallel to the Live ASSC (In-Service), with the latter being either owned and developed by the SRO or owned and managed by the end-user ODH / AM(MF). Whilst some elements of the Live ASSC (►Development◄) and the Live ASSC (In-Service) are likely to be common, the context for each will be different and the overall claim is likely to require a different argument strategy. For example, the argument strategy for the Live ASSC (In-Service) might include reliance on a fully-substantiated equipment Safety Assessment and RTS to support world-wide operations in poor weather with the Air System flown by any qualified front line crew, regardless of experience. Conversely, the context for the Live ASSC (►Development◄) is specifically about testing and / or evaluating new capabilities which might not yet have a fully-substantiated equipment Safety Assessment; the argument strategy may therefore focus on the organizational aspects such as the specific competencies of trials personnel, the highly-controlled environment and the specific trials approval / Risk Assessment processes in place. Whilst the context for the Live ASSC (►Development◄) will differ from that of the Live ASSC (In-Service), both in terms of flying to be undertaken and Air System maturity, the T&E organization will need a clear understanding of the end-user's context and approach to the Risk-versus-reward balance in order to conduct role-relatable Safety and fitness-for-purpose assessments. Consequently, the engagement of the end user ODH / AM(MF) remains a requirement, as does the support of the SRO who ultimately remains responsible for developing and delivering the Live ASSC (In-Service) for In-Service flying to the end user.

[34] For civil-initiated procurement of ►Civilian-Owned / Civilian Operated Air Systems◄ which may not have a SRO, the programme manager responsible for planning, governing and overseeing the successful delivery of the programme's output / product will own and manage the ASSC until the Air System is activated on the UK MAR and the ASSC handed over to the AM(MF).

[35] Note: terminology has been chosen to reflect existing regulatory influence, through MACP, in the capability domain, ie: Certification Strategy (at ►OBC◄) and Type Certification Basis (at ►FBC◄).

***Figure 5:*** *Through-Life Applicability and Development of the ASSC.*




11. **In-Service Flying**. As the capability is accepted into service, the responsibility for the ASSC will be handed over to the end user ODH / AM(MF). Thereafter, the ODH / AM(MF) should own and manage the Live ASSC (In-Service) in order to demonstrate through auditable and evidence-based arguments that RtL are reduced to both ALARP and Tolerable. If the Air System is required to undergo future development, the above cycle will repeat for the new capability. The hand-over of the Live ASSC (In-Service) from the SRO to the end-user ODH / AM(MF) must occur in sufficient time for any additional ITEA activity required in support of RtL judgements to be undertaken and demonstrated before Initial Operating Capability (IOC).

12. **Multiple End-Users**. Having a single owner of an ASSC does not limit an Air System *type* to a single ASSC; a single In-Service Air System *type* may be operated by multiple Aircraft Operating Authorities with differing context of use, thus requiring each ODH / AM(MF) operating that type to own and manage a separate ASSC, recognizing that elements of the supporting evidence and / or argumentation may be common to each Live ASSC (In-Service). This principle will also include those circumstances where an In-Service Air System is transferred to a contractor for Maintenance Test Flying (MTF). The end-user ODH / AM(MF) will own and manage the ASSC (In-Service) aligned to the full context of In-Service flying, whereas the AM(MF) for the CFAOS organization conducting the MTF will own and manage a separate Live ASSC for the specific context of the MTF conducted by that organization. Much of the argument and evidence supporting each ASSC will be common; indeed, the ASSC for the MTF activity may rely heavily on the end-user's Live ASSC (In-Service), but with a much narrower context and a focus on the conduct of the MTF activity. Similarly, the end-user's Live ASSC (In-Service) will include claims relating to the Maintenance activity being conducted by the MTF organization. In both cases, a clear articulation of the interface between the organizations, the evidence on which each ASSC is dependent, and a robust line of communication to highlight any weaknesses will be a fundamental part of the argumentation within each ASSC.

**Applicability of the ASSC to UK Military-Registered Air Systems**

13. The requirement to develop and manage an ASSC is subject to the principle that similar aviation activities within the DAE that result in a similar level of Risk or Risk exposure, ought to attract the same level of Regulation, Assurance and scrutiny, regardless of ownership of, or who is operating, the specific Air System. As such, RA 1205 and the guidance within this Manual is applicable to all UK Military-Registered Air Systems, regardless of whether they are owned by the MOD or a civilian organization ►◄. Similarly, whilst the ASSC will be proportional to the context within which the Capability is employed and RtL incurred, the requirement to own and manage an ASSC applies equally to Air Systems operated by a military AOA with a military ADH and to ►the AM(MF) for◄ Air Systems operated by a civilian AOA under CFAOS with an AM(MF).

**The ASSC and Integrated Test and Evaluation**

14. One of the conclusions from Lord Levene's Defence Reform Report was that test and evaluation activity *"should be seen as an integral part of the acquisition process [which] should be undertaken from an early stage, not least because the evidence suggests that this helps to keep costs under control later in the process."* [36] Similarly, previous Niteworks research[37] contended broadly that it is cheaper and more effective to conduct T&E activity earlier, and concluded that more effective and timely ITEA in the Acquisition cycle could accelerate programme development whilst reducing programme Risk. The 2008 MOD T&E Strategy identifies ITEA as *"the MOD solution for ensuring that the supplied solution meets the user's needs"* and articulates that the main purpose of T&E is to provide confidence that:

a. The capability is fit for purpose in the military environment across all DLoD and through life;

b. The capability is safe to use;

c. The MOD has received what it asked for.

15. The Niteworks report[38] also recognized that whilst aspects of capability (and associated ITEA) were out of Air Safety scope (eg lethality of weapons), to a large extent Safety and capability ►will◄ be approached jointly within a notion of 'safely capable'. Without this, any Safety requirements identified and pursued through ITEA may not deliver capability that was safe in the Air Systems' intended role. Thus, the role of ITEA in ASSC development cannot be overstated[38]. Confidence that the ITEA is pan-DLoD and captures all of the stakeholders' requirements, especially those of the end-user ODH / AM(MF), is a key starting-point to ultimate ASSC Assurance. The symbiotic link between the ITEA and the development of the ASSC is depicted at Figure 5. In essence, the ASSC Strategy and Acquisition basis need to progressively develop the structured argument, and feed the supporting evidence requirements into the ITEAP; in turn, the ITEAP needs to generate the evidence required to support the overall Safety argument, including through dedicated T&E activity.

**SPECIFIC INCLUSIONS WITHIN THE ASSC**

16. **Safety-Enhancing Technologies and Techniques**. One of the fundamental aspects for achieving an ALARP argument is the adoption of good practice. The Health and Safety Executive (HSE) defines good practice as the 'measures we would normally expect to see in such circumstances', ie for a similar system and / or activity in a similar context. In line with this principle, the ASSC should explicitly address the inclusion, or justified exclusion, of Safety-enhancing technologies and techniques from across the aviation industry which are applicable to the intended context, with decision(s) captured within the developing ASSC. The consideration of emerging Safety-enhancing technologies and techniques will depend on the anticipated Safety benefit, and the maturity of those technologies and techniques against the programme timeline. Once the Air System is in Service, the periodic review of the Live ASSC (In-Service) will need to confirm that arguments based on the adoption of good practice are still valid, cognisant of any changes in context or adoption of new technologies and techniques across the aviation industry. Examples of Safety-enhancing technologies and techniques include: Collision Warning Systems, Terrain Awareness and Warning Systems, Cockpit Voice / Flight Data Recorders, Windshear Alerting Systems and Flight Data Monitoring programmes.

---

[36] Lord Levene. *"Defence Reform: An independent report into the structure and management of the Ministry of Defence".* June 2011. Part 11: Acquisition, Para 11.5, Page 52.
[37] Niteworks, NW/FS/TE/2169 'Test and Evaluation Project Final Report', June 2010.
[38] Niteworks Report NW/PR/0820/014 MAA Regulatory Research Project Final Report dated 21 October 2016.

17. **High Technical-Merit / Higher-Risk Activities**. As has been articulated previously, the ability to construct an effective ASSC is dependent on the existence and understanding of a clearly defined context; this includes the Air System itself, the capabilities required to be delivered by the system, how they will be achieved, and the operational environment(s) within which the system is to be operated. However, as described in the structured argument example presented at Annex A to Chapter 2, it is likely that certain capabilities or operations will necessitate specific requirements within a number of the DLoDs, and potentially additional or bespoke mitigations to ensure their employment remains both ALARP and Tolerable; indeed, the ODH / AM(MF)s approach to this Risk-versus-reward balance is likely to vary for some activities. This is particularly true for 'high technical-merit or higher-Risk activities' such as NVD operations, air-to-air refuelling, embarked operations, degraded visual environment operations, training for contested airspace operations, the use of equipment and / or procedures cleared under an Operational Emergency Clearance (OEC) and operations with reduced Safety margins[39]. Whilst these activities can be accommodated within a single structured argument for the whole Air System, this approach can distort or overburden the overall strategy, or result in the dilution / obscuration of the specific mitigations required to ensure the safe employment of these niche capabilities[40]; as such, it may be more appropriate to address such activities as a discrete entity or separate module of the ASSC. Whichever approach is adopted, it is essential that the ASSC explicitly addresses all 'high technical-merit or higher-Risk activities' and presents a coherent and convincing Safety argument for the employment of these capabilities, backed up by valid supporting evidence which might be bespoke to these capabilities.

**ASSC ASSURANCE, ENDORSEMENT AND SCRUTINY**

18. **Assurance Framework**. In order to assist the RC, emphasise the centrality of the Safety argument and deliver pan-DLoD balance, an ASSC Assurance framework has been developed and is presented at Annex B to this Chapter. The Assurance framework maps the five facets of the Defence ASSC Model against all four elements of the ASSC function[41] defined in paragraph 6, and has been populated with a series of open questions / challenges which aim to serve two purposes: to form the generation of an explicit Safety argument, and to highlight areas of focus for internal or external review / Audit of the ASSC.

19. **ASSC Endorsement**. There is widespread acknowledgement within industries operating a Safety Case regime that regular review points between the regulator and the operator ensure that Safety considerations influence a system's design without undue regulatory "speedbumps"; moreover, such engagement from the early phases of development engenders a collective understanding of what the regulator deems to be an acceptable basis for operation - in which the operator has a vested interest. This is also true of the relationship between those constructing the Safety Case during the selection and development of the system, and the end-user operator of that system. In line with this guidance, the requirements for ASSC endorsement are detailed in RA 1205.

20. **Independent Assurance**. One of the facets within the Defence ASSC Model is Confidence in the ASSC; this can be achieved by ensuring that the Context is clearly defined in order to define the subsequent Safety argument, that appropriate SQEP are involved in the development of the ASSC and the supporting evidence, and that the ASSC is subject to independent Assurance. Whilst the MAA will be seeking evidence that the ASSC has been subject to independent Assurance as part of the endorsement process detailed at paragraph 19 above, the MAA does not wish to prescribe how this is to be achieved. Those responsible for the development and management of the ASSC are free to determine the most appropriate means of independent Assurance of the ASSC as determined by factors such as the stage of ASSC development and the overall context / complexity of the ASSC; options may include a suitable Independent Safety Advisor, Release To Service Authority, Safety Centre, or the Air Safety Team or Safety Case Manager from another Group or Service, providing that the individual or organization is not unduly influenced by commercial, peer or rank / status pressures.

21. **ASSC Scrutiny**. Recognizing the through-life considerations of a Safety Case to the CADMID cycle of an Air System, alongside the importance of assessing the effectiveness of ASSC development during capability design / selection, the ASSC will be subject to scrutiny as part of a project milestone

[39] For example, tasks utilizing approved Reduced Operating Standard or Military Operating Standard take-off and landing performance.
[40] There is a significant body of evidence, including Service / Board of Inquiry reports, which indicate that this failing is a common theme.
[41] ASSC Strategy, ASSC Acquisition Basis, Live ASSC (►Development◄) and Live ASSC (In-Service).

business case submission. Early engagement between the SRO and the MAA will facilitate issue of the MAA's ASSC scrutiny statement, which will form part of the project's scrutiny report.

►◄

►◄

►◄

# Chapter 4: ANNEX A: ASSC – OPERATING CONTEXT CHECKLIST

The foundation of an ASSC is the ability to make an effective argument which, in turn, is dependent on the existence and understanding of context. This is why context sits in the prime cardinal position of the five facets within the Defence ASSC Model (See Chapter 3, Paragraph 2). The following checklist is provided to assist those responsible for the development of an ASSC to consider those elements that drive Risk; primarily the Air System, the environment and its usage. Considerations of the operating aspects might include:

- ►Crewed / Uncrewed.◄
- Rotary Wing / Fixed Wing / Fast Jet / Multi-Engine.
- Visual Flight Rules / Instrument Flight Rules / Instrument Met Conditions outside of IFR / See and Avoid.
- Automatic Flight Control System and automation philosophy (manual, selected, fully-managed).
- Day / Night / Night Vision / Synthetic / Enhanced Vision.
- Controlled / Uncontrolled airspace.
- Operator - Civil or Military.
- Maintenance - Civil or Military.
- Crewing (single-pilot, multi-crew).
- Environments:
    - Desert, Maritime, Embarked.
    - Snow, Ice, Rain, Dust.
- Military Tasks:
    - Low-level operation.
    - Weapons.
    - Air Combat.
    - Formation / Air to Air Refuelling (AAR).
    - Aerial Delivery / Parachuting.
    - Embarked Operations.
- Other significant operating aspects identified by SMEs.
- Synthetic Training.
- Designed flight envelope.
- Propulsion system.
- Fuel system.
- Area of operation.
- Operating sites.

Intentionally Blank for Print Pagination

# Chapter 4: ANNEX B:
# ASSC - ASSURANCE FRAMEWORK

The five facets of the Defence ASSC Model can be applied against all four elements of the ASSC function: the ASSC Strategy (at ►OBC◄), the ASSC Acquisition Basis (at MG), the Live ASSC (►Development◄) for T&E flying and the Live ASSC (In-Service) once the Air System is delivering the intended service / capability. The ASSC Assurance framework presented below specifically addresses all of the ASSC facets across all ASSC functions, supporting creation of the argument (and ASSC Report) through articulation of the desired state and through explicit ASSC owner / manager response to a series of open questions / challenges. The ASSC framework serves two purposes: areas of focus for internal or external review / Audit of the ASSC, and to assist the generation of an explicit Safety argument. In either case, only one column will apply on any given occasion.

Table B-1: ASSC Framework – General

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Who** | SRO | SRO | T&E ODH / AM(MF) | ODH / AM(MF) |
| **Why** | To establish that capability has the potential to be managed safely across all DLoD through its lifecycle. | To establish how the pan-DLoD Safety requirements have been identified and how they will be substantiated. | To deliver a substantiated argument for safe T&E.<br>To demonstrate that the Air System is safe for the conduct of T&E flying and that the associated RtL is reduced to both ALARP and Tolerable. | To deliver a substantiated argument for a safe capability.<br>To demonstrate that the Air System is safe for the conduct of operations and that the associated RtL is reduced to both ALARP and Tolerable. |
| **Key Outcomes and Outputs** | Safety requirements considered in cooperation with end-user operators / maintainers and captured in a Pan-DLoD URD.<br>Identified Safety requirements not included in the baselined URD are recorded.<br>Produce an ASSC Strategy Report. | Safety requirements considered in cooperation with end-user operators / maintainers and captured in SRD (for Equipment and Logistics DLoD) and in a defined captured mechanism (with identified Delivery Agents) for other DLoD.<br>Safety requirements not represented in this process are recorded.<br>Pan-DLoD ITEAP generated and referenced.<br>Produce an ASSC Acquisition Basis Report. | Development of ASSC by T&E AOA ►ODH / AM(MF)◄, coherent with the ASSC Acquisition Basis and requirements of RA 5880 and RA 2370, including an explicit argument structured around the 5 facets (in accordance with RA 1205 model).<br>Produce a Live ASSC Report. | Handover of ASSC to operating AOA ►ODH / AM(MF)◄ in sufficient time for review and additional ITEA activity prior to ISD.<br>ASSC submission by operating AOA to Independent Assurance.<br>ODH / AM(MF) Live ASSC Report (including Safety Statement) prior to commencement of flying operations and annually thereafter. |
| **MAA ASSC** | MAA review and endorsement of submitted ASSC Strategy Report.<br>Out-note to SRO, stating endorsement and noting any corrective actions. | MAA review and endorsement of submitted ASSC Acquisition Basis Report.<br>Out-note to SRO, stating endorsement and noting any corrective actions. | MAA review and formal acceptance of submitted Live ASSC Report.<br>ODH / AM(MF) gain Assurance, normally provided through organizational approval,), stating acceptance and noting any corrective actions.<br>Air System made active on the UK MAR. | MAA review and formal acceptance of submitted Live ASSC Report.<br>ODH / AM(MF) gain Assurance, normally provided through organizational approval, stating acceptance and noting any corrective actions.<br>Air System made active on the UK MAR. |
| **MAA MAR** | | UK MAR Categorisation and Provisional Allocation of UK MAR Tail Numbers. | Activation on the UK MAR (Development AS). | Re-Categorisation on UK MAR (In-Service). |

Table B-2: ASSC Framework - Context

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Context**<br><br>**Required State** | **Context Defined**<br><br>The intended context of the capability has been captured, covering:<br>• Air System configuration.<br>• Usage.<br>• Environment.<br><br>Context is derived from Concept of Operations and Concept of Employment, and captured in the Baseline URD (Part 1) and the ASSC Strategy.<br><br>Address Technical Merit considerations.<br><br>Explicitly review for inclusion in the ASSC, existing Safety enhancing technologies and techniques from across the aviation industry.<br><br>Context has been endorsed by end-user. | **Context Matured**<br><br>The intended context of the capability has been matured:<br>• Air System configuration.<br>• Usage.<br>• Environment.<br>• Operating Context Checklist at Annex A.<br><br>Context refinement captures Concept of Use.<br><br>Context has been endorsed by the end-user. | **Context Limited**<br><br>The intended context of the capability has been captured within the framework of applicable MRP:<br>• Air System configuration.<br>- (Military Permit to Fly (MPTF) RA 5880)<br>• Usage.<br>- Test Plan RA 2370.<br>• Environment.<br>- Test Plan RA 2370.<br>- CFAOS RA 2501. | **Context Captured and Relevant**<br><br>The in-use context of the capability has been captured within the framework of applicable MRP and reviewed against actual and planned usage:<br>• Air System configuration.<br>- (RTS / MPTF).<br>• Usage.<br>- (Statement of Operating Intent and Usage (SOIU)).<br>• Environment.<br>- (SOIU).<br><br>Explicitly address all higher technical merit and / or higher Risk activities. |
| **Context**<br><br>**ASSC Questions** | How will air vehicle, governance, usage and environment be captured?<br><br>From what documents have they been derived?<br><br>What level of involvement has the end-user had in generating them?<br><br>Describe how the SRD and CSRD will be reviewed to ensure sustained relevance to the operational context. | What documents provide the operational context?<br><br>What level of involvement did the end-user have in creating them?<br><br>When were they generated / last reviewed?<br><br>When was the ASSC Operating Context (MASSC Chapter 4 Annex A) addressed and by whom? | Describe how test activity captures the Air System role in context.<br><br>Describe how Assurance can be gained that supplier-provided data / assessment has been obtained in role context. | When was the last review of Concept of Use and SOIU?<br><br>Does current or planned usage of the Air System deviate from intended usage?<br><br>Where is any excursion, and associated authority, captured (eg OEC)?<br><br>Is the excursion limited or enduring?<br><br>Demonstrate how the excursion will be resolved. |

Table B-3: ASSC Framework – Hazards Managed

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Hazards Managed**<br><br>**Required State** | **Hazard ID and Analysis**<br>The pan-DLoD Hazards of the context have been identified and analyzed in relation to the context through mechanisms including:<br>• Those captured at RA 1210.<br>• Functional Hazard Analysis.<br>• Analysis of previous Accidents / Incidents / in legacy systems.<br>• Analysis of the Defence Lessons Identified database.<br>• Reference to a comparator Air System.<br>• Process and associated SQEP for Hazard ID and analysis is defined.<br>Linkage between Hazard ID and analysis, and development of Safety requirements for integration into the URD, can be demonstrated. | **Hazard Analysis and Mitigation**<br>Mitigations to identified Hazards are represented in Safety requirements and development into SRD (or pan-DLoD equivalent).<br>Impact of Safety requirements development (including refinement and prioritisation within, or exclusion from, URD / SRD / CSRD / Customer-Supplier Agreements) on identified mitigations is captured; ie additional Training Needs Analysis, demonstration through a mature ITEAP (and associated acceptance strategy), supported by an established ITEA WG, that T&E evidence relating to capability effectiveness vs Safety requirements (in role) will be recorded and reviewed during the acceptance process, including the conditions and mechanisms for end-user ODH / AM(MF) consultation where there is an impact to Hazard mitigation. | **Risk Assessment of Aircraft operation and trials activity**<br>• Risk Management conducted (in accordance with RA 1210).<br>• Trials Risk Assessment conducted (in accordance with RA 2370). | **Hazards (in context) are managed**<br>The Unified Risk Register is effectively and demonstrably based on single Risks identified within individual DLoD domains (for example, derived from MACP for the Equipment-DLoD or the Residual Training (Trg) Gap Statement for the Trg-DLoD), assessed and mitigated in context to both ALARP and Tolerable.<br>All Risk mitigations are evidenced with identified owners pan-DLoD.<br>The Air System has undergone role relatable T&E to expose potential hazards in a representative environment, with outcomes transferred to the end-user ODH / AM(MF) Risk Management process. |
| **Hazards Managed**<br><br>**ASSC Questions** | When will pan-DLoD Hazard identification and analysis be conducted?<br>Demonstrate that all ITEA stakeholders have been identified and included in the pan-DLoD Hazard identification.<br>Demonstrate that Hazards / single Risks associated with individual DLoD have been integrated into a single role-related Hazard log.<br>How will Hazard analysis inform identification of Safety requirements?<br>How will Safety requirements be integrated into the URD and wider ITEAP? | How was pan-DLoD Hazard identification and analysis conducted?<br>How was the ASSC Operating Context referenced?<br>Describe the involvement of ITEA stakeholders.<br>Provide an overview of the Hazard controls assessed as likely to be weak in effectiveness (from analysis or learning from experience), together with an assessment of criticality, and explain how this has informed the identification of Safety requirements.<br>Identify any Safety requirements that have been subject to reduced priority or exclusion from URD / SRD – what is the end-user ODH / AM(MF) view?<br>What are the contracting and / or governance mechanisms, and who are the delivery agents for Safety-related User Requirement (UR), out with the Equipment and Logistics DLoDs? | Identify the process used to conduct pan-DLoD Hazard analysis and mitigation for T&E flying activity.<br>Identify any Hazards and associated controls common to multiple T&E flying events – where any controls are assessed to be weak, justify how they can be borne within an ALARP and Tolerable judgment.<br>On transfer of Air System between organizations, identify the arrangements for transfer of operating risks (out with any subsequent T&E flying activity) previously identified and managed by the ODH / AM(MF).<br>Access to evidence generated by the SRO. | What is the impact to Hazard management of any excursion between documented context and actual / planned usage?<br>Provide an overview of Risk controls assessed to be weak, together with an assessment of criticality, and justify why they can be borne within a both ALARP and Tolerable judgment.<br>What owners have been assigned to these controls and how will they be held to account?<br>To what extent has Safety reporting endorsed or challenged assessed effectiveness?<br>How are the hazards and Live ASSC evidence checked and verified for continued applicability? |

Table B-4: ASSC Framework – Regulatory Compliance

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Regulatory Compliance**<br><br>**Required State** | SRO can demonstrate MRP compliance within own organization.<br><br>SRO can demonstrate how compliance of emerging capability will be managed and demonstrated.<br><br>• Processes.<br>• SQEP.<br>• Compliance Monitoring. | SRO can demonstrate continued compliance of own organization.<br><br>SRO can demonstrate how any non-compliance (vs MRP) with emerging capability has been addressed (including impact to Hazard management), providing evidence of any required AAMC, Waivers or Exemptions (AWE) in the Safety Case Report prior to MG.<br><br>SRO can demonstrate how any nonconformity (vs end-user AOA Orders / Operating Manual) has been addressed. | AOA approved. ►ADH / AM(MF)◄ endorsed for T&E:<br><br>• CFAOS<br>• ADH<br><br>Type Airworthiness<br><br>• Design Approved Organization Scheme.<br>• Type Airworthiness Authority.<br>• MPTF.<br><br>Continuing Airworthiness<br><br>• Continuing Airworthiness Management Organization.<br>• Maintenance Approved Organization Scheme / Mil 145. | ODH / AM(MF) demonstrates compliance (vs MRP), providing evidence of any AWE (and accounting for any impact to Hazard management) in the Safety Case Report.<br><br>ODH / AM(MF) demonstrates conformity (vs orders / Operating Manual), providing evidence of any AWE (and accounting for any impact to Hazard management) in the Safety Case Report. |
| **Regulatory Compliance**<br><br>**ASSC Questions** | Demonstrate compliance within the SRO organization.<br><br>How will prospective regulatory compliance for the future Air System be assessed pan-DLoD?<br><br>• How will AAMC be developed?<br>• What is the mechanism to seek end-user ODH / AM(MF) input to / assessment of the AAMC?<br>• What is the mechanism to seek AAMC approval?<br><br>How will prospective non-conformance with end-user ODH / AM(MF) orders / Ops Manuals be assessed?<br><br>• How will the end-user ODH / AM(MF) be involved in securing dispensation / mitigation for the explicit ASSC argument? | Is the Air System from the preferred supplier non-compliant with MRP?<br><br>• Will the supplier subsequently deliver compliance under contract within Demonstration and Manufacture stages?<br><br>• If not, what are the approved AAMC from the MAA?<br><br>Is the Air System from the preferred supplier non-compliant with end-user ODH / AM(MF) orders / Ops Manual?<br><br>• Will the supplier subsequently deliver compliance under contract within Demonstration and Manufacture stages?<br><br>• If not, what is the end-user ODH / AM(MF) view regarding the impact of any associated Waivers / Exemptions on the Safety argument supporting future ALARP and Tolerable judgements? | Describe any current or planned noncompliance (vs MRP) or non-conformance (vs ODH / AM(MF) orders / Ops Manuals.<br><br>• Outline AWE arrangements.<br><br>• What owners have been assigned to pursue resolution?<br><br>• Describe when and how non-compliance or non-conformance has been assessed for impact to Hazard management. | Describe any current or planned non-compliance (vs MRP) or non-conformance (vs ODH / AM(MF) orders / Ops Manuals.<br><br>• Outline AWE arrangements.<br><br>• What owners have been assigned to pursue resolution?<br><br>• Describe when and how non-compliance or non-conformance has been assessed for impact to Hazard management. |

Table B-5: ASSC Framework - Confidence

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Confidence**<br><br>**Required State** | All ITEA stakeholders have been identified and engaged in context capture and Hazard analysis:<br>• Operator.<br>• Type Airworthiness.<br>• Continuing Airworthiness.<br>• Other DLoDs.<br>• Capability Management (Requirements Managers).<br>• Acquisition Management.<br>• Regulators.<br>• Independent T&E.<br>• Role T&E.<br>• Science and Technology Community, eg Defence Science and Technology Laboratory (DSTL).<br>• DE&S (Operating Centre Directors & SME staff).<br>• End-User Safety Staff.<br><br>Weaknesses in other ASSC facets are accounted for.<br><br>Independent Assurance should be obtained. | Provenance, history and current status of pan-DLoD Safety requirements, including SQEP credentials of personnel providing ITEA support, can be accounted for.<br><br>Pan-DLoD ITEA delivery mechanism is in place, which includes:<br>• Independent Test of qualitative elements eg handling qualities, human machine interface (HMI) / workload and systems functionality / performance.<br>• Independent Evaluation of quantitative elements, eg Aircraft performance.<br><br>Weaknesses in other ASSC facets are accounted for.<br><br>Issues identified by the MAA with regard to ASSC Strategy have been addressed.<br><br>Independent Assurance should be obtained. | Independent and Operational Assessors input to design and sub-system ground testing.<br><br>Independent and Operational Assessors included within Test Plan.<br><br>Independent Assurance should be obtained. | Independent Assurance of ASSC:<br><br>Independent Test reports<br>• Independent Evaluation Reports.<br>• Role T&E Reports.<br>• Independent Safety Assessment Reports.<br><br>Issues identified by the MAA with regard to (SRO) ASSC Strategy and Acquisition Basis have been addressed.<br><br>Issues identified by previous Independent Assurance have been addressed. |
| **Confidence**<br><br>**ASSC Questions** | What are the principal areas of concern within the other (four) facets of the ASSC, and how is this likely to impact the ability of the SRO to develop an ASSC?<br><br>Acquisition Basis that can effectively influence design / selection? | What are the principal areas of concern from the other (four) facets? Describe any associated impact to the provenance of identified Safety requirements?<br><br>What was the MAA response to the ASSC Assessment Strategy and how have any issues been addressed?<br><br>Is there sufficient evidence across the other (four) facets of the ASSC to meet evaluation and acceptance criteria?<br><br>Describe how qualitative tests (eg HMI / Workload, Handling Qualities, System Functionality) being conducted independently of the supplier.<br><br>Describe how independent evaluation of supplier data will be conducted. | What are the principal areas of concern arising from the other (four) facets of the ASSC and how can they be borne within a both ALARP and Tolerable judgment?<br><br>How have any issues highlighted by the MAA for ASSC Strategy and / or Acquisition basis, relevant to the conduct of T&E flying, been addressed? | What are the principal areas of concern arising from the other (four) facets of the ASSC and how can they be borne within a both ALARP and Tolerable judgment?<br><br>What was the last response from independent Assurance of the Live ASSC, and how has it been addressed?<br><br>Where evidence is required in support of Operational T&E conducted by the FLC:<br>• To what extent is it provided by SQEP personnel / agencies?<br>• To what extent is it independent?<br>• To what extent is it evaluated and integrated into the ADS / RTS by SQEP personnel / agencies? |

Table B-6: ASSC Framework – Effective ASMS

| ASSC Facets | ASSC Strategy (►OBC◄) | ASSC Acquisition Basis (►FBC◄) | Live ASSC (►Development◄) | Live ASSC (In-Service) |
|---|---|---|---|---|
| **Effective ASMS**<br><br>**Required State** | SRO ASMS in accordance with RA 1200.<br><br>Issues identified in internal / external ASMS Review addressed. | SRO ASMS in accordance with RA 1200. | ASMS in accordance with RA 1200<br><br>Issues identified in internal / external ASMS Review addressed. | AOA ASMS in accordance with RA 1200<br><br>Issues identified in internal / external ASMS Review addressed. |
| **Effective ASMS**<br><br>**ASSC Questions** | When was the last 1st / 2nd / 3rd party ASMS review?<br><br>What were any weaknesses identified?<br><br>What is the status of the recovery plan for these areas? | When was the last 1st / 2nd / 3rd party ASMS review?<br><br>What were any weaknesses identified?<br><br>What is the status of the recovery plan for these areas? | When was the last 1st / 2nd / 3rd party ASMS review?<br><br>What were any weaknesses identified?<br><br>What is the status of the recovery plan for these areas? | When was the last 1st / 2nd / 3rd party ASMS review?<br><br>What were any weaknesses identified?<br><br>What is the status of the recovery plan for these areas? |

# Chapter 5: COMMON PITFALLS OF SAFETY CASES

## ACADEMIC CROSS-REFERENCES

1. This chapter has been written with reference to the following academic papers; those responsible for the development and maintenance of an ASSC may wish to refer to these documents for further guidance:

   a. Charles Haddon-Cave QC. *"The Nimrod Review – An independent review into the broader causes surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006."* The London Stationary Office, 28 October 2009.

   b. MOD. *"An Introduction to System Safety Management in the MOD – Part 2, System Safety in MOD Acquisition."* Issue 4, 2018. (Note: this is widely referred to as *"The White Book"*).

   c. ►Dr◄ Tim Kelly. "*Are Safety Cases Working?"* Safety Critical Systems Club Newsletter, Volume 17, No 2, January 2008, pages 31-33[42].

   d. Office for Nuclear Regulation. "The Purpose, Scope and Content of Safety Cases." Revision 4, July 2016.

## INTRODUCTION

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

   a. They contain assertions rather than reasoned argument.

   b. There are unjustified and implicit assumptions.

   c. Some major Hazards have not been identified and are therefore never studied.

   d. There is a poor treatment of data with uncertain pedigree, and the effect this uncertainty has on subsequent assessments.

   e. They don't deal well with Human Factors.

   f. They don't deal well with software.

   g. There is inadequate involvement of senior management.

   h. Ownership of the Safety Case is not always clear.

3. The MOD White Book[11] argues that Safety Cases can be considered the tangible products of an effective Safety Management System, and that the intangible product is a safer system. However, having a Safety Case does not in itself reduce Risk: it is only when the findings are acted upon and the outputs implemented that Safety will improve and people will be safer[43].

4. A key aspect of the Safety Case is that it ►will◄ highlight the major Hazards and concentrate on these: often Safety Cases can be swamped by a mass of detail on all the Hazards from the trivial to the most significant[43].

5. In the Nimrod Review, Haddon-Cave expressed ►the◄ view that the Safety Case regime had lost its way and had led to a culture of 'paper Safety' at the expense of real Safety; indeed, Safety Cases had become positively dangerous and lulled people into a sense of false security. They were generally big, fat, glossy, consultant-produced documents which said the kit was "safe" when manifestly it was not.

6. There are many open-source guides on the purpose, scope and content of a Safety Case, available from bodies such as the HSE, York University and the Office for Nuclear Regulation. Most of these guides reference the Nimrod Review, specifically Chapters 9-11 and 22 which detail the specific issues with the Nimrod Safety Case itself, and the more generic pitfalls and shortcomings associated

[42] Available at: https://www-users.cs.york.ac.uk/~tpk/2008scscarticlekelly.pdf.
[43] MOD. An Introduction to System Safety Management in the MOD - Part 2, System Safety in MOD Acquisition.

with Safety Cases. The remainder of this chapter is therefore designed to provide the reader with a synopsis of both aspects.

**AN EXAMPLE – THE NIMROD SAFETY CASE IN 2006**

7. The loss of Nimrod MR2 XV230 on 2 September 2006 resulted in the biggest single loss of life of British service personnel in one incident since the Falklands War. However, perhaps the most damning aspect associated with the loss of XV230 was that, unlike previous Nimrod accidents[44], it is 'at least as likely as not' that nothing actually failed from a technical perspective to cause the catastrophic mid-air fire that resulted in the loss of the Aircraft and the death of all 14 service personnel on board. This statement is supported by the Nimrod Review which concluded that the ignition source was the cross-feed hot air duct in the starboard No.7 Tank Dry Bay (which was operating as designed) and the most likely source of fuel was an overflow through the No.1 Tank blow off valve[45] located forward of the Dry Bay (which also operated as designed). Ultimately, the Aircraft was flying in the as designed-condition, had been maintained correctly, was operated correctly throughout the flight including emergency handling and yet, despite no technical failure, the Aircraft was lost.

8. The requirement for a Safety Case to identify, assess, and mitigate potentially catastrophic Hazards before they could cause an Accident was mandated for military Aircraft[46] and other military platforms by regulations introduced in September 2002. The Nimrod Safety Case was completed by 2005, and therefore represented the best opportunity to capture the serious design flaws in the Nimrod which had lain dormant for years. Unfortunately, as Haddon-Cave concluded: *'the Nimrod Safety case was a lamentable job from start to finish. It was riddled with errors. It missed the key dangers. Its production is a story of incompetence, complacency, and cynicism. The best opportunity to prevent the accident to XV230 was, tragically, lost.'* Moreover, not only did the Safety Case fail to identify the specific Hazards associated with the design flaws which ultimately materialised to cause the Accident, but it positively stated that either the Hazards were eliminated, or it presented mitigations which did not exist. The heart of the problem was that the Safety Case was fatally undermined by an assumption by all the organizations involved that the Nimrod was 'safe anyway', because the Nimrod fleet had successfully flown for 30 years, and they were merely documenting something which they already knew. The Safety Case became essentially a paperwork and 'tick-box' exercise. Specific failings included:

a. **The Safety Case did not reflect the as-designed or as-built standard of the Aircraft**. The Safety Case incorrectly stated that the Hazard associated with a fire in the affected zone was mitigated by the presence of a fire detection and suppression system; neither actually existed within this zone. Having failed to correctly identify and assess the fire Risk in the affected zone (discussed at sub-para e below), this false claim of a potentially-compelling recovery barrier could also discourage any further critical intellectual rigour about the fire Hazard.

b. **The Safety Case did not reflect how the Aircraft was actually being operated**. The Safety Case incorrectly stated that the cross-feed duct (a hot-air gas pipe which was the ignition source of the fire) was only in use during engine start; in fact, this duct was routinely in use throughout flight in order to supply a supplementary air conditioning system. This is symptomatic of a Safety Case which was constructed without operator input, otherwise this error would have been identified.

c. **The Safety Case did not reflect the current condition of the Aircraft**. The Safety Case stated that the bleed ducting (including the cross-feed duct) was insulated and that therefore surface temperatures will be below the bleed air temperatures, thus implying that the insulation would mitigate the bleed ducting as a source of ignition. However, the Safety Case failed to note that: (a) there were gaps in the insulation; (b) some parts of the bleed ducting had no insulation;

[44] For example, XV256 was lost following multiple bird-strikes resulting in multiple engine failures; XW666 was deliberately ditched following electrical and mechanical failures resulting in a punctured fuel tank and subsequent fire which could not be suppressed; XV239 was stalled with insufficient height to recover due to Human Factors. Nimrod Review Page 21.

[45] The BOI (Board of Inquiry) assigned equal probability to the source of fuel being overflow from the blow off valve during air-to-air refuelling or a leak from a fuel coupling (which would constitute a technical 'failure'). Following further evidence, Haddon Cave concluded that the most likely source of fuel was overflow during AAR. Nimrod Review Page 9.

[46] Now referred to as military Air Systems.

and (c) the insulation was in poor condition in some areas. The Safety Case did not reflect the as-designed or as-built standard of the Aircraft, nor did it reflect the current condition of the Aircraft.

d. **Lack of maintainer input to the Safety Case and failure of the ASMS**. Haddon Cave concluded that a leak from a fuel coupling was the second most likely source of the fuel in the accident scenario. The Safety Case stated that *'from in-service data the potential for fuel pipe leakage is given as improbable'* – specifically the likelihood of a leak from a fuel coupling was once in a million flying hours. Experience and In-Service data showed this assessment to be to be far too optimistic[47]. This indicates a failure to include input from actual maintainers in the construction of the Safety Case, and a failure of the ASMS supporting the Safety Case.

e. **Lack of rigour during Hazard identification and failure of the ASMS**. The Safety Case failed to identify the zonal Risk presented by the location and proximity of the fuel blow-off value immediately forward of the affected zone (such that any fuel expelled from the blow-off valve could track back along the fuselage into the No 7 Dry Bay). This was not just a theoretical possibility; previous In-Service experience had identified that fuel could be expelled from this blow-off valve during air-to-air refuelling, and that fuel tracking back along the outside of the fuselage would re-enter the fuselage through joints / seals further aft. This indicates a general lack of rigour associated with Hazard identification, a lack of critical review of In-Service occurrence data, and a failure of the ASMS.

f. **Failure of independent scrutiny and Assurance of the Safety Case**. The issues identified above are symptomatic of a generally poor standard of accuracy and analysis throughout the Safety Case. Moreover, the baseline Safety Case reports produced by the contractor left over 30% of the hazards 'unclassified' and 40% of the Hazards remained open. In addition to the failures in the generation of the Safety Case highlighted above, there was a failure in the independent scrutiny and Assurance of the Safety Case, which undermined any confidence in the Safety Case.

Ultimately, the Nimrod Safety Case had not reduced the Risks to the Nimrod fleet to ALARP, and the best opportunity to identify the fatal Risk was lost.

**GENERIC SHORTCOMINGS OF SAFETY CASES**

9. The more generic types of shortcomings and traps with Safety Cases identified in the Nimrod Review are reproduced below. This encompasses work by Dr Tim Kelly of the University of York and endorsed by Charles Haddon-Cave in his report.

10. Charles Haddon-Cave identified the following shortcomings common to Safety Cases[48]:

a. **Bureaucratic length**. Safety Cases and Reports are too long, bureaucratic, repetitive and comprise impenetrable detail and documentation. This is often for 'invoice justification' and to give Safety Case Reports a 'thud factor'.

b. **Obscure language**. Safety Case language is obscure, inaccessible and difficult to understand.

c. **Wood-for-the-trees**. Safety Cases do not see the wood for the trees, giving equal attention and treatment to minor irrelevant Hazards as to major catastrophic Hazards, and failing to highlight, and concentrate on the principal Hazards.

d. **Archaeology**. Safety Cases for 'legacy' platform often comprise no more than elaborate archaeological exercises of design and compliance documentation from decades' past.

e. **Routine outsourcing**. Safety Cases are routinely outsourced by Delivery Teams (DT)[49] to outside consultants who have little practical knowledge of operating or maintaining the platform, who may never even have visited or examined the platform type in question, and who churn out voluminous quantities of Safety Case paperwork (`bumpf' and outsized Goal Structured Notation

[47] The Nimrod Review states that there were 30 fuel leaks from couplings per year in 1988, and by 2006 'a leak per fortnight' for operational Aircraft (p152).
[48] The Nimrod Review, Chapter 22, Paragraph 22.7, Page 534.
[49] ►Charles Haddon-Cave QC◄ referred to Integrated Project Teams as they were then called; these are now termed Delivery Teams.

charts) in back offices for which Integrated Project Teams (IPTs)[49] are charged large sums of money.

f. **Lack of vital operator input**. Safety Cases lack any, or any sufficient, input from operators and maintainers who have the most knowledge and experience about the platform. '...any review of the Nimrod Safety Case *"must involve appropriate air and ground crews in order to ensure that current practices are fully understood; those personnel, after all, both know most about how our aircraft are operated and flown, and also have the greatest personal interest in having levels of safety with which all involved are comfortable."*[50] Operators at RAF Kinloss were not even aware of the existence of the original Nimrod Safety Case.

g. **Disproportionate**. Safety Cases are drawn up at a cost which is simply-out of proportion to the issues, Risks or modifications with which they are dealing.

h. **Ignoring age issues**. Safety Cases for 'legacy' Aircraft are drawn up on an 'as designed' basis, ignoring the real Safety, deterioration, Maintenance and other issues inherent in their age.

i. **Compliance only**. Safety Cases are drawn up for compliance reasons only, and tend to follow the same, repetitive, mechanical format which amounts to no more than a secretarial exercise (and, in some cases, have actually been prepared by secretaries in outside consultant firms). Such Safety Cases tend also to give the answer which the customer or designer wants, ie that the platform is safe.

j. **Audits**. Safety Case Audits tend to look at the process rather than the substance of Safety Cases[51].

k. **Self-fulfilling prophesies**. Safety Cases argue that a platform is 'safe' rather than examining why Hazards might render a platform unsafe, and tend to be no more than self-fulfilling prophesies.

l. **Not living documents**. Safety Cases languish on shelves once drawn up and are in no real sense 'living' documents or a tool for keeping abreast of Hazards. This is particularly true of Safety Cases that are stored in places or databases which are not readily accessible to those on Front Line who might usefully benefit from access to them. As an example, the Nimrod Safety Case was only fully accessible from one computer terminal at BAE Systems at Chadderton.

**SAFETY CASE 'TRAPS' – ARE SAFETY CASES WORKING?** [52]

11. Charles Haddon-Cave commented that the above criticisms are not new, nor confined to Safety Cases for military platforms. He also highlighted an article entitled *'Are Safety Cases Working?'* by Dr Tim Kelly of the University of York which highlights seven examples or 'traps' to avoid. Charles Haddon-Cave suggested that the article should be compulsory reading for many of the current purveyors of Safety Cases; as such, each of the highlighted 'traps' are précised in the following paragraphs:

a. **The 'Apologetic Safety Case'**. Safety Cases have little hope of adding value if they are impotent in their influence on the design and operation of the system in question; Safety Cases shouldn't be produced after the design has been finalized, but sometimes they are! The production of a thorough and rigorous Safety Case once the design has been finalised has the potential to reveal uncomfortable truths about the Safety and / or certifiability of the system, forcing a choice between: often economically and politically unacceptable re-design; operational limitations which constrain employment of the capability; or adopt the 'apologetic Safety Case' constructed to pick up the tatters of the evidence available and stitch them together to make the best possible job of the Safety argument: "X doesn't quite work as intended, but it's OK because..." A Safety Case must be given the opportunity to work if it is going to deliver the Safety benefits; development of the Safety Case should be started at the earliest possible opportunity,

[50] BOI Report, Part 5, Commander-in-Chief Air Command's Comments dated 2 November 2007.

[51] Charles Haddon-Cave ►QC◄ referred to Lord Cullen when quoting the evidence of a number of witnesses, including Major Holden, Transport Safety Consultant, formerly Inspector of Railways, who drew attention to weakness in auditing: *"My concern has been that there has been a lack of penetration in the audits, which have tended to chase paper trails rather than check that what should be going on on the ground is, in fact, going on. This lack of penetration may, in part, be due to the lack of skill of the auditors but it may also lie in the belief that all that is required is a pure compliance audit of the accepted safety case. The vital question as to whether or not the safety case itself is adequate and appropriate to the circumstances is seldom asked".*

[52] Tim Kelly. "Are Safety Cases Working?" Safety Critical Systems Club Newsletter, Volume 17, No 2, January 2008, pages 31-33.

incorporating design detail and associated Safety evidence as soon as it becomes available. Not only will this then help to identify what remaining Safety evidence needs to be gathered through development to support the final Safety argument, but when it becomes obvious that there will be difficulty in making the case for acceptable Safety, there is still the option to feed this back into the design process as a driver for change.

b. **The Document-Centric View**. Perhaps the biggest 'trap' in Safety Case development is that Safety Cases are often thought of as documents, such that the underlying aim of the Safety Case is to produce a document. Indeed, early advice within MOD JSP 430 stated that 'a Safety Case is a comprehensive and structured set of documentation…'. More correctly, this ►ought to◄ have read 'a Safety Case is commonly *presented using*, and *communicated through*, a structured set of Safety documentation'. This distinction is important. Those responsible for managing Safety and RtL should not be reassured by paper, word-processor files, spread-sheets or HTML documents, but instead by a structured, compelling argument with relevant and comprehensive supporting evidence. Safety Case Reports can exist even if there is no Safety Case, and vice-versa. Unless a requirement to produce a Safety Case Report is utilized as an opportunity to apply intellectual rigour and 'dig' deep' to gain (and then present) a true understanding of what makes the system safe (or unsafe), there is a danger that lots of money / effort will be spent producing a document that will quite possibly have no beneficial impact on achieved Safety.

c. **The Approximation to the Truth**. It is all-too-easy to present a Safety Case which appears to be coherent and compelling by ignoring some of the rough edges that exist in reality, particularly when utilizing a graphical notation such as Goal Structured Notation or Claims-Argument-Evidence. For example, it is easy to present a claim within the GSN diagram that states that 'all identified Hazards have been acceptably mitigated' and then point the reader to the Hazard Log as the source of the supporting evidence for this claim when, *in reality*, the argument isn't so straightforward. Not only are such approximations to the truth misleading and serve to undermine the value of producing a Safety Case Report, but they can dissuade further objective intellectual rigour being applied to management of the Hazards.

d. **Prescriptive Safety Cases**. The phrase 'prescriptive Safety Cases' may sound like a contradiction in terms; however, it is possible to fall into the trap of making Safety Cases *routine* or *run-of-the-mill*. First, it is easy to become obsessed with compliance to accepted structures and build arguments through a clause-by-clause analysis of a Safety standard, thus losing sight of the primary objective of creating a convincing Safety argument for the system being considered. Second, the Safety Case can become a parade of detail that may seem superficially compelling but, again, fails to establish a coherent Safety argument. Finally, Safety Cases can become routine through re-use and over-familiarity; organizations should be concerned when every Safety Case from a particular domain starts to look the same as this may be indicative of a lack of objectivity or intellectual rigour. Instead, the reviewer needs to be asking if the Safety Case is really revealing the arguments that need to be made, or are the issues being shoe-horned into the framework of a previously accepted structure? As with Risk Assessments, it is easy to constrain thinking to that which is already captured and presented, rather than considering the issues which have not yet been identified.

e. **Safety Case Shelf-Ware**. Safety Cases serve little purpose if, after their initial development and acceptance, they are consigned to a shelf, never again to be touched. The development of a robust Safety Case involves substantial intellectual effort and contains detailed information concerning the safe employment, maintenance and behaviour of the system in operation. Indeed, just as the Safety Case must represent the as-designed, as-maintained and as-operated condition of the system, the accepted Safety Case is only valid if the system is employed in accordance with the procedures and mitigations captured within it. The Safety Case is worthless if it is so inaccessible or unapproachable that it is never again referred to.

f. **Imbalance of skills**. The successful implementation of a Safety Case regime requires at least two specific skill-sets. First, those developing the Safety Case must have the skills to assemble and articulate the Safety Case; second, those required to assure / Audit the Safety Case (often the regulator) must have the skills to review and critique the Safety Case. Whilst the

former is widely recognized, the latter is often overlooked and the Safety Case approach cannot work effectively if there is an imbalance between these skill-sets. Whilst it is wrong to think of the regulators as opponents, the health of a Safety Case regime lies in the existence of someone to objectively and intellectually challenge the claims and assumptions of the Safety Case; a strong case will stand up to such a challenge, whereas a weak case will be uncovered, and changes prompted.

g. **The illusion of pictures**. Graphical tools such as GSN and Claims-Argument-Evidence can be very helpful in the development and presentation of the Safety argument that should form the core of any Safety Case. However, there is a significant risk associated with the use of such notations – people are easily 'dazzled' by complex, coloured, hyper-linked graphic illustrations which gives both the developers and viewers a warm sense of overconfidence. The quality of an argument cannot be judged by a word count or the number of colours used - the modern-day analogue of 'arguing by weight of paper'. Those responsible for the development of the Safety Case must ensure that when graphical notations or support tools are utilized, they are employed as an aid to structured thinking and do not become the end in themselves. Equally, both developers and reviewers must ensure that they remain fully engaged in assessing the adequacy of the reasoning presented, and not be distracted by the method of presentation.

12. In summarising his article, Kelly uses the examples above to highlight that it is possible to lose sight of the principles that are key to gaining value from Safety Case development:

a. Safety Case development ►is to◄ be initiated early enough in the lifecycle such that there is an opportunity to influence the evolving design.

b. Safety Cases ►are to◄ be developed in such a way as to encourage their use and Maintenance in system operation, ie once introduced into service.

c. The skills must exist to enable stakeholders to properly scrutinise and critique Safety Cases.

d. Safety Cases must engage in accurate and in-depth analysis of the specifics of the system in question.

e. The Safety Case *message* is more important than the *medium*.

13. Finally, Kelly argues that for industries that have been utilizing Safety Cases for some time, they should no longer be satisfied simply because Safety Case regimes are in place and because Safety Cases are being produced and accepted; they ►are to◄ be continuously and diligently examining whether the Safety Cases being produced are adding value to the Safety processes. They ►will◄ be, but only if traps such as those articulated above are avoided.