Guidance on the Conduct of Aircraft Zonal Hazard Analysis (ZHA)

J P Jones & M Wilson

Issue 2

28 September 2016

DISTRIBUTION

Task Sponsor

Dr Steve Reed, Dstl.

Mandy Cox, MAA Structures4-Gen

SAAG and AAPWG Members

See SAAG and AAPWG.

EXECUTIVE SUMMARY

A zonal hazard is a form of common cause failure (CCF) that can be described as an unsafe interaction between one system and another arising as a consequence of their relative spatial separation. Under Regulatory Article (RA) 1210 Duty Holders (DH) are required to identify and assess the risk to life on platforms they are responsible for and demonstrate that these risks are Tolerable and ALARP. For zonal hazards, demonstrating this has proved difficult because many aircraft entered service before zonal hazard analysis (ZHA) became an established technique or earlier analyses conducted may have been invalidated due to modification or other changes of use.

To address this requirement, DH therefore need to develop a strategy to assess the risk posed by zonal hazards for the platforms they are responsible for. However, in practice the derivation of an appropriate strategy is influenced by life-cycle position, the availability of design information and the degree of change the aircraft type has been subject to.

For example, newer aircraft commonly have undergone a zonal safety analysis in accordance with the practice defined in Aerospace Recommended Practice (ARP) 4761. However, compliance with this standard on its own may not provide sufficient evidence to satisfy the requirements of RA1210, as this does not produce fully articulated zonal risks without further activity. Whereas if an aircraft has been subject to a change of use (e.g. modification) or has been in-service for some time, then it is likely that a whole aircraft ZHA will need to be conducted to provide the necessary evidence to show that the risk from zonal hazards is acceptable.

Experience suggests that a whole aircraft ZHA is best completed in a number of phases: a Preparation Phase that focuses on ensuring that subsequent hazard identification and analysis is conducted effectively; a Hazard Identification Phase that should be conducted systematically to identify credible zonal hazards; and, a Hazard Risk Assessment Phase that involves the determination of a representative probability for the accident sequence associated with each zonal hazard, determination of accident severity and subsequent assessment of risk. To ensure that the risk assessment is as accurate as possible it is important that the probability values used are also as representative as possible. To achieve this it is recommended that many information sources (e.g. in-service maintenance data, condition survey results, anecdotal information etc.) are utilised and qualitatively adjusted to produce a representative accident sequence.

Once completed, a full ZHA should give sufficient evidence to satisfy the requirements of RA1210 and therefore enable an improved understanding of the aircraft aggregate risk. The ZHA can bring other benefits in that it can improve current airworthiness standards by identifying husbandry and condition issues; help develop a more effective maintenance policy; provide evidence to support future airworthiness decisions, such as a Life Extension Programme; and, inform the focus of an ageing aircraft audit.

AUTHORSHIP

Authors:

Mr Mark Wilson

Mr Jeff Jones

Release Authority:

Mr M G Tier – Head of Engineering.

K E Wiliiams – Ageing Aircraft Project Manager, QinetiQ Air Division.

QinetiQ Ltd, MOD Boscombe Down, Salisbury, Wiltshire, SP4 0JF.

This document was prepared by QinetiQ, under the terms of DEFCON705 as agreed in contract FATS 2 LTPA DSTLX-1000046757 with Defence Science and Technology Laboratories.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AAA	Ageing Aircraft Audit
AD	Accidental Damage
AIT	Auto Ignition Temperature
AoR	Area of Responsibility
AAPWG	Ageing Aircraft Programmes Working Group
AASysA	Ageing Aircraft Systems Audit
ADS	Aircraft Document Set
ALARP	As Low As is Reasonably Practicable
AMM	Aircraft Maintenance Manual
ARP	Aerospace Recommended Practice
ASIMS	Air Safety Information Management System
CAMO	Continuing Airworthiness Management Organisation
CS	Condition Survey
DE&S	Defence Equipment and Support
DO	Design Organisation
Dstl	Defence, science and technology laboratories
DH	Duty Holder
ED	Environmental Damage
EWIS	Electrical Wiring Interconnect System
FMECA	Failure Modes Effects and Criticality Analysis
FOD	Foreign Object Damage
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HAZOPS	Hazard and Operability Study
ID	Identification
JSP	Joint Service Publication
JNCO	Junior Non-Commissioned Officers
LEP	Life Extension Programme
LRU	Line Replaceable Unit

MAA	Military Aviation Authority
Mk	Mark
MMS	Master Maintenance Schedule
MOD	Ministry of Defence
MRP	MAA Regulatory Publication
OSD	Out of Service Date
PR	Particular Risk
PT	Project Team
RA	Regulatory Article
RCM	Reliability Centred Maintenance
RAF	Royal Air Force
SAAG	Systems Airworthiness Advisory Group
SAE	Society of Automotive Engineers
SC	Safety Case
SCR	Safety Case Report
SI(T)	Special Instructions (Technical)
SIM	Systems Integrity Management
SM	Service Modification
SME	Subject Matter Expert
SMP	Safety Management Plan
SNCO	Senior Non-Commissioned Officers
SQEP	Suitably Qualified & Experienced Personnel
S&EP	Safety and Environmental Protection
STANEVAL	Standards and Evaluation
SWIFT	Structured What-If Technique
SysI	Systems Integrity
TAA	Type Airworthiness Authorities
ZHA	Zonal Hazard Analysis
ZSA	Zonal Safety Analysis

1 INTRODUCTION

1.1 BACKGROUND

In the development of an aircraft, the design organisation (DO) seeks to remove, as far as possible, any hazards present on their design. For those hazards that remain, within the UK military aviation domain, Duty Holders (DH) have an on-going requirement to identify and assess the risk to life (RtL) on the systems within their area of responsibility (AoR). With respect to the risk posed by zonal hazards this has proved difficult because:

- Many aircraft entered service before Zonal Hazard Analysis (ZHA) became an established hazard identification and analysis technique and the extent to which zonal hazards were considered on these types is not known;
- Changes to aircraft configuration may have invalidated earlier zonal analyses conducted.

In practice, the responsibility for the identification and assessment of equipment risks and therefore zonal hazards is delegated to the Type Airworthiness Authority (TAA) situated within a Project Team (PT). Consequently, the TAA may have insufficient evidence to argue that the risk from zonal hazards on the systems they are responsible for is acceptable. The TAA may therefore a need to conduct their own zonal hazard identification and analysis to gather sufficient evidence to produce a credible zonal safety argument that addresses current UK military aviation regulatory requirements.

However, a TAA–and other organisations have little recognised guidance to assist them in determining how the risk from zonal hazards should be addressed. Whilst there is existing civil aviation guidance in Aerospace Recommended Practice (ARP) 4761 [1] for undertaking Zonal Safety Analysis (ZSA), this is designed mainly to support the certification of new aircraft and, for reasons to be discussed later, is, arguably, less appropriate for use on legacy/in-service aircraft.

Recognising QinetiQ's experience of conducting ZHA, the Dstl tasked QinetiQ [2], through the Ageing Aircraft Programmes Working Group (AAPWG), to produce a paper that captured a process for undertaking a whole aircraft ZHA of a legacy aircraft. This paper was delivered in April 2012 and covered ZHA preparation, zonal hazard identification, reporting and some of the lessons learned from the many ZHA that QinetiQ had conducted.

Post Issue 1 of the AAPWG ZHA Paper, QinetiQ was tasked to update the Paper to broaden the scope of issues. Issue 2 therefore includes additional guidance on:

- The selection of an appropriate zonal hazard strategy for a given platform type;
- The assessment of zonal hazard probability and the management of hazards;
- Experiences and examples from more recent ZHA projects;
- Addressing issues with respect to ZHA identified in the Nimrod Review;

- How the results of a ZHA may be exploited.

Issue 2 also incorporates AAPWG stakeholder comments and certain recommendations from Issue 1 of the Paper and reflects the latest publication state of MRP and Defence Standards.

1.2 PURPOSE OF THIS PAPER

This updated Paper seeks to satisfy two goals. It seeks to inform:

- The development of MOD policy with respect to how the risk posed by zonal hazards to the safe operation of UK military aircraft should be addressed;

- DH and TAA safety staff associated with in-service aircraft how they may address the risk posed by zonal hazards.

Whilst this Paper is predominately focused on in-service UK military aircraft, it is also applicable to remotely piloted air systems and new aircraft being brought into service.

1.3 ZONAL HAZARD DESCRIPTION & DEFINITION

Before the requirement to address zonal hazards is considered, it is first appropriate to define what is meant by a zonal hazard and identify some of its attributes.

A zonal hazard is a type of Common Cause Failure (CCF) [3]. CCF arise due to a lack of independence between given components. In the case of a zonal hazard, an unsafe situation is created when one component in a system interacts with another component as a consequence of their mutual physical disposition. Consequently, the term *zonal hazard* and *zonal hazard cause* are defined as:

- **Zonal hazard –** An unsafe interaction between one system and another system or structure within a defined zone arising as a consequence of their relative spatial separation;

- **Zonal hazard cause –** A necessary initiating event or property within a component or system that must occur for the zonal hazard to exist.

A zonal hazard may have a single or multiple causes. These causes may arise as a consequence of a component or system fault (e.g. a leak from a union), due to a property of a component or system (e.g. the operating temperature a component reaches) or human factors issues. Zonal hazards may also not be constrained to a single zone. They also can include instances where a zonal hazard cause originates in one zone but the hazardous effect is manifested in another zone. Such a hazard is described as a *cross zonal hazard* and is defined as:

- **Cross zonal hazard –** A hazard in which a hazard cause initiates in one zone but the hazardous interaction with a different system or structure occurs in another zone.

Consequently, ZHA is described appropriately in the UK MOD Acquisition System Guidance (ASG) [4] as**:** 'An analysis of the physical disposition of the system and its components in its installed or operating domain**.'** Examples of the different types of issue that can create a zonal hazard cause can be seen in Appendix A,

1.4 REQUIREMENT TO CONDUCT ZHA

BASIC REQUIREMENT

The fundamental justification for conducting a ZHA on a given platform is that it will provide the DH, as the risk owner, with a more comprehensive understanding of the individual zonal and cross-zonal hazards present on the platform and the resultant single risks. Once these hazards and single risks have been identified they can be used to derive a better understanding of the aggregate risk arising from platform operation.

This is particularly relevant as the majority of system safety analysis techniques utilised in the air domain are based on functional models of systems (e.g. failure modes and effects analysis (FMEA) and fault tree analysis (FTA)) and the results derived from these models are used routinely to underpin quantitative safety claims. These models frequently assume that the systems being modelled are functionally independent i.e. they are free from influence of CCF. If these models are not adapted to include the influence of CCF, including zonal hazards, then the subsequent quantitative calculations of risk may be underestimated and the associated safety claims flawed.

To reduce the possibility that hazards are missed a diverse range of hazard identification and analysis techniques should be employed by a risk owner on the platform or system they are responsible for (an approach advocated in RA 1210 [5] and DEF STAN 00-56 [6]). As ZHA is used to examine hazards and safety concerns which result from where a component is located, it complements many of the safety analysis approaches which examine only functions of systems. Common with any single hazard identification and analysis technique, the application of ZHA alone will not ensure that all credible risks to a platform or systems safety are identified.

UK MILITARY REGULATORY REQUIREMENT

Currently, there is no direct requirement in UK MOD Military Regulatory Publications (MRP) that compels a DH to conduct ZHA. There are several indirect references to ZHA in the MRP, DEF-STAN 00-56, DEF STAN 00-970 [7] and the ASG [4] but these identify largely that ZHA is one of several hazard identification and analysis techniques that can be used in the process of hazard identification and management; or they identify how ZHA can support other airworthiness objectives (these latter issues are discussed further in Section 4).

However, RA 1210 requires DH to identify the RtL present on the platforms within their AoR and to ensure that these RtL are at least Tolerable and As Low As Reasonably Practicable (ALARP). It further identifies that hazard analysis conducted should cover zonal issues. As zonal hazards are a recognised class of hazards it is reasonable to conclude that to comply with the intent of

RA 1210, a TAA must, on behalf of the DH, have in place a satisfactory argument, with appropriate supporting evidence, to show that the risk from zonal hazards are at least Tolerable and ALARP for each platform in their AoR.

Using the definition of an Air System Safety Case (SC) in RA 1205 [8], it follows also that this zonal safety argument and evidence should be captured within the respective platform's SC. Moreover, RA 1205 further identifies that a platform's SC should be revised if necessary to ensure its continuing relevance and its fitness for purpose. Thus, if any of the context or assumptions underpinning existing evidence used to address the risk posed by zonal hazards changes, then to maintain a satisfactory zonal safety argument either the zonal safety evidence (i.e. the ZHA) must be updated or a new, potentially more restrictive, safety argument must be created.

Consequently, although there is no direct requirement to a conduct ZHA on a given platform, it is difficult to see how a TAA can provide a platform DH with sufficient evidence to meet the requirements of RA 1210 and 1205 without having a strategy in place to address the risks from zonal hazards. This strategy should have the Goal of providing the DH with sufficient and appropriate evidence to enable an argument that risks from zonal hazards on the platforms within their AoR are Tolerable and ALARP throughout the platform life-cycle.

1.5 BENEFITS OF CONDUCTING A ZHA

In addition to satisfying the indirect regulatory argument described above and gaining a more complete understanding of the risk present on a platform, a TAA can gain other benefits from the conduct of an independent and systematic ZHA. Through the ALARP evaluation process, it can help sustain airworthiness through:

- The initiation of design changes.
- The issue of SI(T), pending more permanent actions being taken.
- The amendment of maintenance policy. This includes informing the development of the platform Reliability Centred Maintenance (RCM) based maintenance schedule.

It can also bring the further benefits that it can:

- Provide a basis for reviewing a platform hazard log to ensure its completeness.
- Inform other sustainment activities, such as the scope of an Ageing Aircraft Audit.
- Help validate the existing aircraft document set (ADS).

These issues are considered in greater depth in Section 4 of this Paper.

1.6 RELATED TERMS AND ACTIVITY

Within the MOD aviation domain there are terms in use similar to those used in ZHA and activities that are, in part, similar to those conducted as part of a ZHA. Therefore, the differences in these terms and their relevance to the identification and risk assessment of zonal hazards is considered before further consideration of ZHA is carried out.

The MOD's approach to developing scheduled maintenance tasks using RCM logic is defined in DEF STAN 00-45 [9]. This introduces the 'Zonal and External Surface Area' inspections, commonly referred to as a 'zonal survey.' These are a form of general visual inspection designed to detect damage, deterioration and discrepancies and assess the general condition of a given zone. A similar physical inspection is also carried out as part of a condition survey (CS), mandated as part of an Ageing Aircraft Audit (AAA) [10]. As with a zonal survey, a condition survey predominately identifies individual accidental and environmental damage and degradation effects.

The focus of a zonal survey and CS is therefore the identification of single issues, predominately on a single system, that requires corrective action in order to restore the design integrity of the aircraft. These issues may be therefore considered as a zonal hazard cause or contribute to the development of an accident sequence. Whilst an appropriately trained practitioner may recognise that certain identified issues may compromise the independence of other systems, these surveys do not result directly in the production of articulated zonal hazards that can be risk assessed.

1.7 SOURCES UTILISED

This Paper has been informed by QinetiQ's experience of undertaking ZHA on a variety of MOD aircraft types, at different points in their life-cycle, and a tailored literature review of existing MOD regulatory policy and other safety material in the public domain. The specific ZHA conducted by QinetiQ include:

- Gazelle Mk1;
- Puma Mk1;
- Puma Mk2;
- Sea King (Mks 3 / 3A / 4 / 5 / 7);
- Harrier GR Mk9 / T12;
- Tornado GR Mk4/4A;
- Tucano T Mk1;
- BAe125 CC Mk3;
- BAe146 CC Mk2;
- VC10;
- Sentinel R Mk1;
- Defender T Mk 2 & Mk 3;
- Islander T Mk 1 & Mk 2B.

2 DEVELOPMENT OF A ZHA STRATEGY

2.1 OVERVIEW

As discussed in Section 1.4, the TAA of all aircraft types in the UK military air domain have a common Goal with respect to addressing the risk from zonal hazards; however, the appropriate strategy to achieve this Goal will be different for each aircraft type. Therefore, to assist TAA in formulating an appropriate zonal hazard strategy for their aircraft types, a number of typical scenarios found in the UK military aviation domain have been created and a possible top level zonal hazard strategy has been created for each of these. As the determination of a suitable approach is dependent on a number of factors, each of these factors is examined in turn before individual strategies are developed.

2.2 TYPICAL LIFE CYCLE POINT ZONAL HAZARD SCENARIOS

In the UK military air domain, arguably, the majority of aircraft types can be approximated to one of the following four scenarios:

SCENARIO 1 – NEW AIRCRAFT

This aircraft has yet to achieve Release to Service (RTS) or has been in-service for a few years. It has undergone a Zonal Safety Analysis (ZSA), completed by the DO iaw ARP 4761 [1]. The hazard analyses conducted are based on theoretical assumptions or limited in-service experience. Any preliminary hazards identified by the DO that have not been adequately addressed should have been captured within the platform's hazard log and subject to TAA review.

SCENARIO 2 – AIRCRAFT AT MIDLIFE POINT

This aircraft type has achieved RTS and Full Operating Capability and has been in-service for many years and is approaching its first AAA, as required in RA 5723 [10]. This aircraft has had a ZSA conducted at the entry into service point that is cited as evidence in the Safety Case, and it has undergone some modification. The existing hazard log is reasonably mature and utilises in-service probability data.

SCENARIO 3 – MATURE AIRCRAFT

This aircraft will have been in-service for a considerable time and is past the point at which an AAA must be conducted. This aircraft may have been developed under a different regulatory regime to that currently in place, e.g. British Civil Airworthiness Requirement, and the original design evidence is now difficult to secure. This aircraft has had numerous modifications embodied and its hazard log is mature and utilises in-service probability data.

SCENARIO 4 – MAJOR MODIFICATION OR UPGRADE

This aircraft has been in-service for some time but is undergoing a significant modification programme that updates several systems that are positioned across multiple zones. This upgrade includes replacement of multiple components.

2.3 FACTORS AFFECTING SELECTION OF ZONAL HAZARD STRATEGY

PRESENCE OF EXISTING ZSA

Safety Cases for aircraft that have been accepted into the MOD inventory over the last decade or so (in some cases longer) frequently have cited ZSA as evidence that the risk from zonal hazards is acceptable. These ZSA have usually been completed using the approach defined in ARP 4761 [1]; this involves defining a set of questions in a checklist that is used subsequently by the assessor during a survey of each zone. ARP 4761 provides civil aircraft certification guidance for undertaking a ZSA during the development phase of a new aircraft or a major modification to a legacy aircraft and is referenced in RA1210 [5] as a recognised form of hazard identification technique.

ARP 4761 states that a 'ZSA should be performed on each zone of the aircraft.' The objective of the analysis is to ensure that the equipment installation meets the safety requirements with respect to:

a. Basic Installation. The installation should be checked against the appropriate design and installation requirements;

b. Interference Between Systems. The effects of failures of equipment (or components) should be considered with respect to their impact on other systems and structure falling within their physical sphere of influence;

c. Maintenance Errors. Consideration to installation maintenance errors and their effects on systems or aircraft e.g. the effects of poor maintenance practices.

The results of a ZSA are usually a completed checklist that affirms whether the defined requirements have been met or if the assessor believes there is an issue with respect to interference between different systems or another safety issue. Each checklist item in the ZSA considers a single individual safety issue and, in some instances, these can be equated to a zonal hazard cause. In others, where a potential interference between two or more systems is identified this can be equated to a zonal hazard. However, the Authors' experience of reviewing ZSA or attempting to use them as appropriate evidence to support a safety argument with respect to zonal hazards has highlighted a number of issues.

The effectiveness of a typical ZSA process is dependent on the scope of the questions detailed in the checklist. The use of a checklist helps ensure that good practice and practical experience

is captured and specifically addressed in an assessment; however, if a relevant safety issue is not detailed within the checklist, then there is a chance that this issue may be overlooked.

It has been noted also in the observed ZSA that, almost invariably, where compliance with a required standard or other criteria has been achieved no further safety consideration has been recommended in the ZSA. TAA personnel appear to have routinely interpreted this as meaning that the particular issue being considered cannot therefore contribute to an accident sequence and, consequently, that no further action is required. This deduction can be misplaced as compliance with standard or other criteria does not mean that the conditions for a hazard to exist cannot arise.

Furthermore, the majority of ZSA reviewed by the Authors have all been carried out by the DO or manufacturer. In these cases very few checklist non-compliances were identified and relatively few examples of potential interference between systems were recorded. Whilst it is recognised that a DO led ZSA may be informed by component qualification data or testing information that may allow some potential interactions to be discounted, the general low numbers of system interference interactions implies that according to the ZSA there are few credible zonal hazards on the examined platforms. This trend could reflect that the DO have made optimistic assumptions about how a given system will behave in-service, that an issue identified has been addressed by design action, or, that the hazard identification activity has not been comprehensive.

For example, if we consider the separation between two hydraulic pipes in a zone. To address the concern that these pipes might lose their integrity and leak fluid into the zone, a ZSA may include a checklist requirement for an assessor to confirm that the mutual separation of fluid bearing pipes in the zone is compliant with the requirements of DEF STAN 00-970 [7]. If the ZSA inspection confirms this, it is common to see no further action taken with respect to this issue. However, over time, experience tells us that this separation may close due to accidental damage, environmental degradation or maintenance error. This may result in the pipes chafing, causing a loss of pipe integrity and the introduction of accelerant into the zone - creating a zonal hazard cause. Here if the checklist criteria has not been defined to address appropriately in-service degradation, the reliance of both the organisation that set the checklist criteria on compliance with a standard to mitigate a particular safety concern and the absence of a realistic consideration of in-service conditions could result in a credible zonal hazard cause being missed, its contribution to other accident sequences not determined and the associated risk unassessed.

Therefore, a ZSA can provide evidence to underpin a safety argument based on demonstrating compliance with the related ZSA checklist. A ZSA, on its own, does not provide a comprehensive list of zonal hazards or an assessment of the risk posed by those hazards and its quality is related to the scope and the relevance of the issues covered in the analysis. It can therefore only provide part of the necessary evidence to satisfy a goal that the risk from zonal hazards can be shown to be Tolerable and ALARP on the platform being assessed.

In the MAA Systems Integrity (SysI) Handbook [12] it is recognised that a change of aircraft usage may threaten an aircraft's SysI. This suggests that a change of aircraft usage may introduce: failure modes that were not originally identified by the DO; changes to the operating properties of existing components; or, affect the frequency at which some known failure modes occur. Moreover, the cumulative effect of apparent relatively minor changes may have a tangible effect on the SysI of a platform. A change in aircraft usage may therefore introduce new zonal hazard causes or change the probability at which certain existing zonal hazard causes are initiated.

A change of usage is considered to have occurred when the aircraft is subject to:

- Modification – this includes where new components are introduced or where the fit or function of existing components is changed;
- Change of sortie profiles or a significant update of the Statement of Operating Intent and Usage;
- Operation in differing environments;
- Increasing loads;
- Changes to maintenance policy.

If an aircraft has been subject to any of the above changes, then elements of any existing ZSA may no longer be valid. In such circumstances it would then be hard to justify a claim that the existing analysis of zonal hazards continues to provide sufficient evidence to satisfy the TAA Goal with respect to zonal hazards.

In some cases individual modification programmes may have been subject to specific, targeted zonal assessment (i.e. either a ZSA or ZHA) to assess their impact on platform. If done effectively, these assessments can provide sufficient additional evidence to support the required safety goal. However, many of the targeted zonal assessments seen by the Authors did not assess whether the embodiment of the modification could interfere with components and systems beyond the immediate zonal boundaries, i.e. address whether new cross-zonal hazards have been created. This reflects possibly the lack of guidance within ARP4761 [1] on the need to address cross-zonal hazards.

Therefore, where an aircraft type has been subject to a change of use, TAA need to ensure that a full assessment of the change in risk from zonal hazards is carried out and that it considers all the implications of the change, including cross zonal effects.

On some platforms, the original design evidence produced as part of the certification of the platform can be difficult to obtain from the DO. This information will contain the assumptions, rationale and test evidence that has shaped the identification of hazards and design responses before the platform in question was introduced into service.

When TAA personnel are assessing or reassessing potential component to component interactions, perhaps as a consequence of an identified change of use, the ability to establish whether the interaction is hazardous is hindered by the absence of this original design information. For example, access to component certification evidence will help establish what component failure modes are credible and therefore what potential type of system to system interactions are possible.

The absence of DO evidence or a lack of understanding of the assumptions underpinning the evidence may provide justification for conducting further analysis or reassessing earlier hazard analyses conducted. For example, if it cannot be shown that particular system to system interaction has been addressed and the aircraft has undergone a change of use, then this may raise a requirement for an in-service assessment of that hazard.

In this case the availability of design evidence will help determine the scope of what hazard analysis a TAA needs to conduct in order to ensure that the understanding of the risk arising from platform operation is kept current and the requirements of RA1210 [5] and RA 1205 [8] are met.

2.4 POTENTIAL STRATEGIES TO ADDRESS ZONAL HAZARD RISK

ZHA SCOPE

SCENARIO 1 - ZONAL HAZARD STRATEGY FOR A NEW AIRCRAFT

If a TAA has the responsibility for addressing the risk posed by zonal hazards on a new aircraft, they are likely to have as evidence a ZSA completed by the DO as part of the certification process. Almost invariably this ZSA will have been completed iaw the approach defined in ARP 4761 [1]. However, given the limitations of a whole aircraft ZSA identified earlier, a TAA zonal safety argument underpinned only by this ZSA would not give the TAA sufficient evidence to argue that the risks posed by zonal hazards are Tolerable and ALARP. To address these gaps and to be able to create a credible zonal safety argument, a TAA should therefore as a minimum undertake the following additional activity:

- The identified residual safety issues in the ZSA should be formed into articulated zonal hazards, captured in the platform hazard log and an assessment of the risk posed by the associated accident sequence determined;
- A sample of zones should be subject to an independent hazard identification and analysis exercise. This is to provide assurance that the ZSA is comprehensive (i.e. it has identified all

credible zonal hazards and has considered all potential failure modes that are likely to apply to an in-service aircraft). This can be carried out by personnel from the TAA or an independent organisation.

If the evaluation of the ZSA identifies that some credible zonal hazards have not been identified then confidence in the ZSA and its suitability as evidence to support an argument that the risk posed by zonal hazards are tolerable and ALARP will be undermined. In these circumstances the absence of comprehensive evidence can be addressed by undertaking a new, whole aircraft ZHA. Other approaches to bridging the gap in evidence, such as conducting a 'desk-top' assessment, may appear as a possible alternative option to this; however, the difficulty in gathering sufficient information sources to do this and integrating the different assumptions used in the various sources of information together will quickly erode any perceived advantages in this approach. Whilst the need to undertake a ZHA may be unwelcome, it will ensure the zonal hazard evidence available reflects the current configuration of the platform; the analysis conducted uses the latest sources of information to determine accident probability rates; and, that the identified hazards can be readily integrated into the platform hazard log.

SCENARIO 2 - ZONAL HAZARD STRATEGY FOR A MID-LIFE AIRCRAFT

If a TAA has the responsibility for constructing a credible zonal safety argument for an aircraft that has been in service for some years and that has already had a satisfactory ZSA, then a reasonable argument that will meet the needs of RA1210 [5] and RA 1205 [8] can be produced by adopting a 'differences' strategy. As the aircraft may have been subject to a change of usage and experienced effects of ageing and poor maintenance practice, the strategy should focus on identifying the zonal safety impact of these changes. The evidence gained from this activity combined with the original ZSA can support an effective, updated safety argument. To implement this approach the TAA could therefore:

- Determine the scope of the changes to the aircraft and its operation since the original ZSA was completed and review the assumptions used in the original hazard analysis;

- If changes or inappropriate assumptions are identified or new issues have been identified in any updated ZSA produced, then these should be assessed to see if any new zonal hazards, including cross-zonal hazards, have been created, or, if the probability of the accident sequences associated with the existing zonal hazards remains appropriate;

- Conduct a check that the in-service Hazard Log has incorporated correctly the extant zonal hazards and has been updated to include any new zonal hazards identified or necessary changes to existing hazards have been made.

This approach is predicated on the assumption that the original ZSA was comprehensive and had accurately captured the in-service zonal hazards present on the platform, and that these hazards were effectively captured in an in-service hazard log. If these conditions cannot be met, then it is necessary to broaden the scope of the activity undertaken to positively re-establish what in-service zonal hazards exist. In these circumstances, the most effective way to provide

credible evidence that zonal hazards have been systematically identified is to conduct a new, dedicated ZHA.

SCENARIO 3 - ZONAL HAZARD STRATEGY FOR A MATURE AIRCRAFT

If a TAA has to create a cogent zonal safety argument for a mature aircraft, then it is likely the following constraints will exist:

- Original design evidence from the DO demonstrating effectively that the risk from zonal hazards had been considered and shown to be acceptable, may not be present;
- The evidence to show that modifications embodied over the life of the aircraft, other changes of use, recently identified potential hazard causes have been systematically assessed for their hazardous effect may be inconsistent or absent;
- The effects of ageing on the platform have not been taken into account during any extant zonal assessments; this may affect the probability at which failures may occur or unforeseen modes of failure.

In this case, there is unlikely to be sufficient appropriate and trustworthy evidence to generate a coherent and satisfactory safety argument with respect to zonal hazards. To produce a compelling safety argument, experience has shown that it is likely to be more cost effective to conduct a new, whole aircraft ZHA. Such a step will involve a fresh physical survey of the platform, ensuring that the analysis conducted reflects the current 'as-operated' and 'as maintained' platform and that the platform Hazard Log is populated with representative zonal hazards and causes.

SCENARIO 4 - ZONAL HAZARD STRATEGY FOR A PLATFORM MAJOR MODIFICATION OR UPGRADE

In this situation, the challenges faced in producing and sustaining a valid zonal safety argument are similar to those described in Scenario 2 and consequently, the necessary actions are the same as those described in Scenario 2. The difference is that in a defined modification or upgrade programme the scope of the configuration and functional changes made to the aircraft is known. Therefore, the bounds of the subsequent activity to determine if new zonal hazards have been created or existing ones require amendment can more easily be estimated.

Dependent on the scale and nature of the modification or upgrade programme different issues may arise that will affect what the results of the applied ZHA will be. For example, a modification or upgrade programme may reduce the level of zonal risk present. The programme may reduce the number of components in a given zone or introduce a component that has greater reliability or fewer hazardous properties.

3 WHOLE AIRCRAFT ZHA PROCESS

3.1 OVERVIEW

A process has been developed for undertaking a ZHA of a legacy aircraft. The ZHA Process was developed following a review of a wide range of legislation, regulatory and guidance material and has evolved from the practical experience gained from undertaking ZHAs on multiple aircraft types. Whilst this process was designed to tackle the challenges posted by a mature, in-service aircraft, it can be tailored to fit any of the scenarios discussed within Section 2. *Figure 1* provides an overview of the developed legacy aircraft ZHA Process.

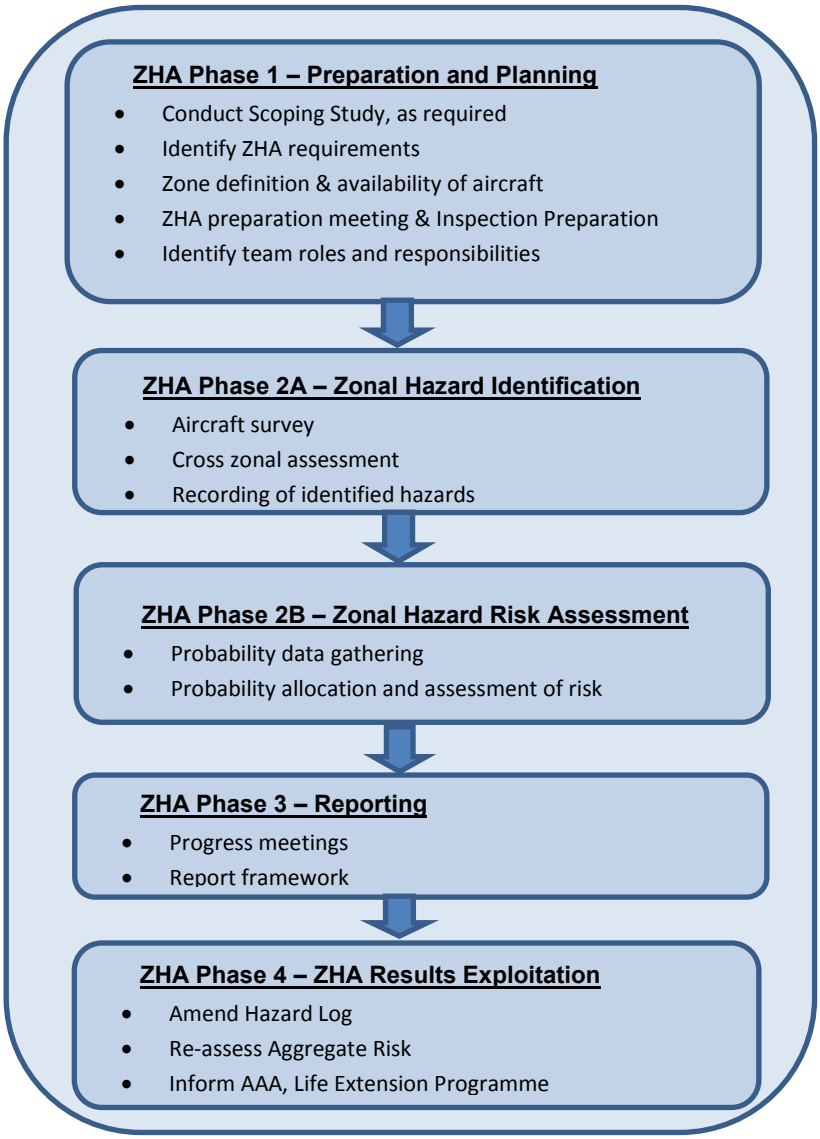


Figure 1 – ZHA Process Overview

3.2 PHASE 1: ZHA PREPARATION

The necessary preparation activity required to conduct a successful ZHA is detailed in this Section. This is split into two parts, the Initial Preparation, that aims to define the task and its boundaries, and, the Inspection Preparation, that focuses on ensuring that the hazard identification activity can be conducted efficiently.

The TAA, usually positioned in the platform PT, may however elect to conduct a ZHA Scoping Study ahead of the main ZHA. This will enable the TAA to de-risk the task by ensuring that: the ZHA will satisfy the regulatory demands placed on them; they have sufficient resources to conduct the ZHA; and, that all necessary support can be put in place ahead of the planned ZHA start date.

The conduct of a Scoping Study will draw upon the experience of the ZHA Provider to identify:

- The technical scope of the ZHA;
- The ZHA Stakeholders and their roles and responsibilities;
- The ZHA dependencies, including access to IT systems and documentation;
- A draft Project and Resource Plan.

INITIAL PREPARATION ACTIVITY

REQUIREMENT DEFINITION AND SCOPE

The first part of the Preparation that needs to be completed is the ZHA Requirements Definition. This seeks to define the boundaries of the ZHA that needs to be completed in order to satisfy the Goal that all credible zonal hazards have been identified for the subject aircraft type. This activity should be informed by lessons learned from any previous ZHA type activities performed on the aircraft, from ZHA conducted on other aircraft types and take into account any other contextual factors that might influence the ability of the ZHA Team to achieve the desired Goal.

The challenge organisations face is that, if the scope of the ZHA is made too narrow, then the resultant analysis may be insufficient to sustain credibly the desired zonal safety goal. Whereas if the scope of the analysis attempted is too broad, then disproportionate resources will be required to complete the ZHA. In particular, sustaining a claim that all zonal hazards have been identified is difficult because:

- It can be difficult to identify all the hazard causes that can originate from a given system or component. At any stage in a platform life-cycle, it is doubtful that all potential ‘erroneous’ and ‘spurious’ functional behaviours of a given component are known. Therefore it cannot be confidently claimed that all potential interactions between adjacent systems have been identified and assessed;

- Determining all the functional consequences of a zonal interaction between two systems can consume disproportionate resources. For example, where a system impinges on a large wiring loom, in a mature aircraft where accurate wiring diagrams are rare, identifying the function of every wire in the loom and therefore all the potential platform level effects of the interaction could take a large number of working hours.

Judgements as to what an acceptable ZHA scope should be in order to comply with the requirements of RA1210 [5] can therefore be difficult to make. However, the Health and Safety Executive acknowledge in their guidance [13] for determining whether ALARP has been achieved recognise that absolute safety cannot be guaranteed and, accordingly, that it is not reasonable for a TAA to expend disproportionate resources on achieving marginal safety benefit. TAA have to therefore make a trade-off between ensuring that the ZHA is as comprehensive as possible, providing the best possible evidence to satisfy the desired ZHA Goal, and the level of resources committed to the task.

For an in-service aircraft, determining what failure modes can be reasonably analysed depends on the complexity of the system being considered and the availability of technical information. Experience suggests it is difficult to define and analyse the consequences of erroneous and spurious component behaviour. For some components e.g. a fuel control valve, it may be possible to predict failure modes and therefore assess their zonal impact, whereas predicting failure modes of a set of integrated modular avionics components is not likely to be feasible.

In the case of Particular Risks (PR), such as an engine disc burst or wheel rim release, these are described in ARP4761 [1] as 'those events or influences which are outside the system(s) and item(s) concerned, but which may violate failure independence claims.' This definition is similar to that as a zonal hazard used in this Paper and, arguably, they could fall within the scope of a ZHA. However, an analysis of a PR requires specific, often complex skills and DO often have to meet specific regulatory requirements with respect to these risks. Therefore, as these risks require separate analysis, they are usually considered to be out of scope of a ZHA.

Consideration of whether the ZHA should be limited to the assessment of unmitigated zonal hazards or whether a full risk assessment process should be conducted is also needed. If the ZHA is to include the identification and consideration of available mitigation in the assessment of zonal risk, then the ZHA Team will need to be aware of this so that timely action can be taken to identify all credible mitigations and controls before the hazard analysis commences.

Determining the scope of the ZHA should also consider whether role equipment is to be considered within the boundaries of the ZHA. Moreover, if the aircraft type contains more than one aircraft mark (Mk) it should be determined whether all Mks are to be examined. This decision may be affected by the Out-of-Service Date (OSD) for the aircraft type, as if one Mk is due to be retired soon inclusion of that Mk may not be justifiable on cost grounds or it may be appropriate to only target high risk areas on that particular aircraft Mk.

Whatever choices are made with respect to what types of failure or property are considered to be within the scope of a ZHA, whether the analysis will include role equipment or if all Mks of a

particular aircraft are to be covered, it is important that all decisions are clearly stated and captured as assumptions in order to provide sufficient context to judge whether the ZHA results are capable of supporting the desired safety goal.

ON-AIRCRAFT INSPECTION FACILITY

The location and suitability of facilities to support ZHA inspections should also be considered as part of the Preparation, particularly where inspections may need to be performed on aircraft in a variety of locations. Facilities that have suitable heating and lighting will need to be provided for the full duration of inspections. For example, a maintenance hangar is likely to be a more appropriate facility for ZHA inspections than a Hardened Aircraft Shelter.

AIRCRAFT ZONE DEFINITION

The ZHA Team should also confirm the zonal scheme that is to be used in the forthcoming ZHA. MOD aircraft are normally divided into logical working areas, or zones, which are used for reference during maintenance. The zones are defined in the Aircraft Document Set (ADS); normally within the platform Topic 1 Aircraft Maintenance Manual (AMM) or the platform Topic 5A1 Master Maintenance Schedule (MMS). This zonal scheme should be used as far as possible in the ZHA as it will be familiar to most users of the ZHA and be consistent with other zonal base activity carried out on the aircraft (e.g. the RCM process).

If the ZHA is being conducted on an aircraft early in its life-cycle or before a zonal scheme has been derived then during the Preparation Phase the ZHA Team may have to derive a zonal breakdown scheme for use in the ZHA inspections. It may also be appropriate to group several zones together, for example if there is no physical barrier between the existing zone boundaries, as this will make the ZHA task more manageable.

SELECTION OF AIRCRAFT FOR INSPECTION

The ZHA Team must engage with the Task Sponsor to identify and select sufficient aircraft for hazard identification activity to ensure that the results of the ZHA can be considered to be representative of the whole aircraft fleet. As there may be different Mks and variants within an aircraft fleet, positioned at different locations, the selection of aircraft for inspection requires careful consideration during the preparation and planning phase.

To ensure that the aircraft selected for inspection are as representative as possible, the chosen aircraft should have been maintained in accordance with the type maintenance policy, and have all fleet special instruction (technical) (SI(T)) and service modifications (SM) embodied. Where there are different Mks within a fleet, all variants should be inspected to ensure that all zonal hazards are captured. There may also be configuration or modification differences within a single aircraft Mk. In these cases, one Mk should be treated as the baseline for a comprehensive inspection and a differences inspection carried out on the other variants or differences.

If the scope of the ZHA includes role equipment, the ZHA Team should ensure that this equipment is fitted to the examined aircraft. It may be possible to utilise assets such as

instructional training aids used in a ground training role, as these are often stripped and configured to allow students to gain a thorough understanding of the design and their use can minimise the impact the ZHA might otherwise have on operational assets. However, use of these alternate assets alone is not sufficient to conduct a credible ZHA and reference must always be made to a fleet representative aircraft in the hazard identification activity.

IDENTIFICATION OF SQEP TEAM MEMBERS AND ZHA TEAM STRUCTURE

The ZHA delivery organisation must also identify suitably qualified and experienced personnel (SQEP), as required by RA1002 [14] to conduct the ZHA and organise a ZHA team structure capable of effectively delivering the ZHA. Experience has shown that as the identification and analysis of zonal hazards requires a certain amount of engineering judgement, the ZHA should be carried out by experienced system safety engineers who possess a variety of aircraft and system safety skills.

The ZHA sponsor should also arrange for the ZHA Team to be supported by the aircraft design and maintenance organisations on an arising basis so that specific platform design characteristics, such as component operating parameters, can be identified. To ensure current aircraft type knowledge is included within the Haz ID phase, the ZHA Team should also engage with personnel who operate and maintain the aircraft. The ZHA Team may also need support from an aircrew representative to provide input on the criticality of hazardous system interactions.

Prior to starting the ZHA inspections, all team members should be briefed on the roles and responsibilities they will hold. Where possible, the same team members should be used throughout the hazard identification and analysis activity so that the factors affecting identified hazards are not lost during the analysis. Suggested project roles and responsibilities for a whole aircraft ZHA are defined in Appendix B and a possible ZHA team structure is shown in *Figure 2* below. It should be noted that an individual may fulfil more than one role at any one time.

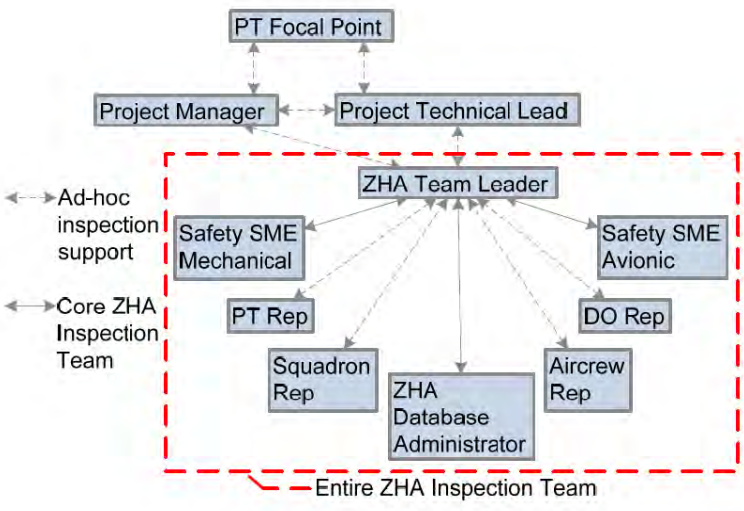


Figure 2: A Typical ZHA Team Role Composition.

Day to day Zonal access planning needs to be undertaken to ensure that aircraft allocated for the ZHA inspections are available for sufficient time to enable all stages of the ZHA inspection to be successfully completed and the overall duration of the Haz ID Phase can be estimated.

The size of a zone and complexity of systems within a zone are key factors that affect the length of time required to inspect a zone. Experience has shown that the time taken to complete an inspection of a zone can range from 0.5 hours for a very simple zone to 8 hours for a high complexity zone. Below are details of the typical types of zone complexities encountered on ZHA tasks completed to date and the estimated time taken to inspect each type of zone:

- **Very Low Complexity Zone:** A typical very low complexity zone is shown in *Figure 3*. These are zones that do not contain system components, and mainly consist of structural components. However, the zone should still be inspected. The anticipated time to complete an inspection of such a zone is 0.5 hours.

Figure3: Example of a Very Low Complexity Zone

- **Low Complexity Zone:** A typical low complexity zone is shown in *Figure 4*. These are zones that contain one or two system components. The anticipated time to complete an inspection of such a zone is 1 to 2 hours;

Figure 4: Example of a Low Complexity Zone

- **Medium Complexity Zone:** A typical medium complexity zone is shown in *Figure 5*. These are zones that have several system components. The anticipated time to complete an inspection of such a zone is 2 to 4 hours;

Figure 5: Example of a Medium Complexity Zone

- **High Complexity Zone:** A typical high complexity zone is shown in *Figure 6*. These are zones that have a significant number of system components. The anticipated time to complete an inspection of such a zone is 4 to 8 hours.

Figure 6: Example of a High Complexity Zone

OTHER ISSUES

In addition to defining the scope of the interaction types that are to be covered in the ZHA, it is also important to establish the following

- Identify any dependencies to conduct the ZHA;
- Identify IT system access requirement to conduct ZHA, e.g. will the ZHA Team need access to online technical publications;
- Provide a ZHA Project Plan;
- Provide a detailed Statement of Work (SoW) for the scope of the overall ZHA task.

- Have all applicable requirements / policy been addressed during any initial meetings between with the ZHA Provider, the Platform PT and the Platform DO?

ZHA INSPECTION PREPARATION

ZHA INITIATION MEETING

Once the Initial Preparatory activities have been completed, the ZHA Provider, the Platform PT and other stakeholders should meet to finalise the arrangements for the completion of the ZHA. This will permit the ZHA Team Leader to confirm the boundaries of the ZHA with all stakeholders and ensure that all task dependencies will be addressed by the responsible owners. Examples of points which may need to be addressed during the meeting are:

- Will the necessary airframes and variants to ensure fleet coverage be available for inspection and will these aircraft be in an appropriate condition for inspection?
- Will the targeted aircraft be available for the entire period of the ZHA inspections?
- If systems need to be operated during the ZHA inspections, what arrangements are in place to enable these systems to be operated?
- What are the arrangements for reporting issues that may have a significant and immediate effect on safety and airworthiness of the aircraft?
- What processes are in place to allow identified hazards to be further investigated?
- What progress reporting requirements are required throughout the duration of the ZHA task, (e.g. written reports and meetings)?

The recommended attendees at the ZHA Initiation Meeting should include:

- The ZHA Team Leader;
- TAA and Platform PT representatives, including a nominated PT ZHA focal point, those who could be involved in the ZHA inspections and those who will be reviewing and acting upon the findings of the ZHA;
- Forward Support maintenance representatives; to include members of the squadron or maintenance organisation who could be involved in the ZHA inspections and an engineering officer;
- DO representatives, who may be required to provide technical information or respond to specific technical queries to support the identification of credible hazards.

Supplementary representation may be required by aircrew (perhaps from the Standards and Evaluation (STANEVAL) Flight) to help assess the criticality of hazardous system interactions identified. Experience gained from ZHA tasks completed to date has shown that a large amount of zonal information can be gained from having a cross-section of personnel; thereby having a broader competency can only add value to the overall ZHA process.

ZHA inspection preparation activities could be completed either within a dedicated meeting or could be done as Phase 1 progresses. The following sub-sections detail some of the topics that should be addressed.

COLLECTION OF AIRCRAFT TECHNICAL PUBLICATIONS AND PREVIOUS ZONAL ASSESSMENTS

The ZHA Team should also gather relevant technical publications, such as the Topic 1 AMM, the Topic 5A1 MMS and aircraft drawings (defining the aircraft configuration state) to give the ZHA Team sufficient information to identify accurately systems and system components during the zonal inspections.

If available, the ZHA Team should obtain any previous zonal assessment work undertaken on the subject platform. These can be reviewed to help the ZHA Team identify all particular zonal safety issues and system to system interactions in a given zone. Previous zonal assessments that may be referenced include:

- **'Green Aircraft' Zonal Assessments** - Some MOD platforms are derivatives of civilian aircraft and as such may have had Original Equipment Manufacturer (OEM) zonal safety assessments produced at the aircraft build or acceptance into service life cycle points. These are likely to have been completed iaw the ZSA principles defined in ARP 4761 [1].

- **Extant Zonal Safety Assessment(s**) - Other ZSA may have been completed at other life-cycle points, possibly as a consequence of a modification programme;

- **JAP(D)100C-22 'Guide to Developing and Sustaining Preventative Maintenance Programmes'** – This publication provides the MAA policy supporting MRP RA4203 (Preventive Maintenance, including Zonal Survey) and is hosted on the MAA web-site Home Page. This is an accessible and relatively uncomplicated guide, and Chapter 10 is dedicated to Zonal and External Surface Analyses. The Zonal Analysis worksheets contained within this JAP could be adapted and used during the ZHA Haz Id survey, if modified to include other relevant factors such as potential zonal interactions. However, the worksheets contained within JAP(D)100C-22 should not be taken verbatim as their purpose is to develop a General Visual Inspection (GVI) programme as part of scheduled maintenance, focusing heavily on generating an Environmental Damage (ED) and Accidental Damage (AD) 'score' for the zone in question. Experience has proven that many zonal hazards exist to poor design considerations or failure modes of equipment which bear no relation to the ED or AD condition, or 'score' of the zone.

However, when referencing earlier assessments, users should be aware that all of these assessments may no longer be accurate due to changes of use and configuration changes that may have occurred. Analysts should be careful that they are not led by these assessments and that any new ZHA should be entirely objective.

INSPECTION OF 'AS OPERATED' AIRCRAFT

To enable the Haz ID to be conducted efficiently and effectively, it is recommended that the ZHA Provider conduct a preliminary inspection of a subject aircraft. This will ensure that the Team are familiar with the aircraft zones, have identified the systems, components and other design features and are therefore in the best position to identify credible zonal hazards.

Using the technical information already gathered and, if necessary, assisted by a current maintenance or DO personnel, the ZHA Team should seek to identify in each zone:

- List of systems and components;
- List of equipment failure modes that could result in a zonal hazard cause or contribute to a zonal hazard;
- List of zone operating parameters such as temperatures, voltages, etc. that can result in a zonal hazard cause being created or facilitate the propagation of an accident sequence.

The ZHA Team should also confirm with the Platform PT the particular facility and aircraft tail numbers suitable for the ZHA inspections. The aircraft should preferably be in an 'as-operated' condition (i.e. not cleaned) to aid the identification of leakage or residue of fluids. Hazardous materials within the aircraft should also be highlighted to the ZHA Team Leader so that appropriate precautions can be taken. The ZHA Team Leader should ensure that adequate access can be gained to the targeted aircraft and that suitable staging is in place to enable the ZHA Team to effectively examine the chosen aircraft.

ZHA CHECKLIST GENERATION

A ZHA Checklist should be produced which identifies potential Zonal design features, potential hazards, component and hazard interactions and safety issues that the ZHA inspection team should take into consideration during its inspection. The ZHA Checklist helps ensure that each inspection is carried out in a consistent and controlled manner and that valuable experience from earlier analyses conducted is not lost. The ZHA Checklist can be generic, for use on multiple aircraft, with any aircraft specific aspects added for the aircraft on which the ZHA is being undertaken. The ZHA Checklist should be produced prior to the ZHA inspections and should be validated with respect to applicable platform design standards and installation guidelines.

ZHA WORKSHEET GENERATION

Standard ZHA Worksheets should be used by members of the inspection team to capture their observations in a consistent and controlled manner. The ZHA Worksheet should be produced during the Preparation Phase ahead of the Haz ID surveys and captured within the Project Documentation Set, for a project work instruction.

3.3 PHASE 2A: ZONAL HAZARD IDENTIFICATION

This section discusses how Zonal Haz ID inspections should be conducted and is based on practical experience of undertaking ZHA for several different MOD aircraft types.

ON-AIRCRAFT SURVEY

Before inspecting a zone, consideration should be given to the information obtained within Phase 1. The intention of this should be to ensure all members of the ZHA inspection team are familiar with the zone composition, operating parameters and boundaries. Maintenance access panels should be removed to enable access to the various zones to be gained by members of the ZHA inspection team. In addition, extra panels and Line Replaceable Units (LRU) may need to be removed to gain complete visual access to various zones. A list of panels and LRUs that are required to be removed should be agreed with the Platform PT during Phase 1.

The individual ZHA inspection team members should run methodically though the ZHA Checklist during the inspection of each zone. However, it is important to note that the ZHA Checklist should be used only as an ‘aid’ to stimulate the identification of potential zonal hazards types and should not be considered to be a complete list. In addition the ZHA inspection team should also systematically consider interactions between all equipment, components, pipe-work and wiring, and should not limit their attention to potential interactions between major systems. ZHA inspections should be carried out using a suitable light source, mirror and a camera; these are especially important when it is not possible to get right inside a zone.

Where a zone contains a system component which, due to the movement of the system during operation, means the physical disposition of items within the zone can alter, a zone may require inspections at various stages of component movement. Depending on health and safety implications, and if images can be taken during transition states, video recording may be used as a tool to establish possible sources of interaction that wouldn’t necessarily have been identified with the equipment in a static condition. The sweep of an aircraft landing gear is a typical example where 'stage inspections' may benefit from this type of recording.

ZHA Worksheets should be used to record the details of each zonal hazard identified during the inspection of each zone and the general ‘as-is’ condition of the zone. Zonal hazards and other contextual factors should be captured as soon as discovered to prevent them being forgotten, particularly if large numbers of zonal hazards are identified. It is important to ensure that a complete image of each zone and zonal hazard is clearly captured. All zones under assessment must have the worksheets completed accurately. If cursory notes are required, these should be recorded in a dedicated "Notes" section of the worksheets.

Many aircraft will have zones that appear to be symmetrical i.e. the configuration of the zones looks identical but they are situated on opposite sides of the aircraft (e.g. the wings). However lessons from previous ZHA suggest that the configuration of zones is rarely symmetrical and assumptions that the same zonal interactions between components will occur can be misplaced.

Any issues that are discovered during the inspection of a zone, which could have a significant and immediate impact on safety or airworthiness, should be reported straight away, by the ZHA Team Leader, to the Platform PT ZHA Focal Point.

Components that are missing from the aircraft at the time of the ZHA inspections must be recorded on the appropriate ZHA Worksheets and the zone in which they are located should be re-assessed when they are fitted. Additionally any parts of the zone that cannot be inspected should also be recorded on the ZHA Worksheets.

Once the zone inspection has been completed and the ZHA Worksheets populated, the individual ZHA Team members should put the information contained within the Worksheets and digital image references into a ZHA database for future interrogation. The no specific requirements as to what information should be captured or what software should be used to construct the database. However, sufficient information should be recorded to allow an assessor to work out how and in what circumstances the various systems might interact. All digital images taken should be clearly labelled and stored in a logical file structure to ease viewing during the risk assessment phase. When taking supporting digital images the orientation of the image must be clear to allow full understanding of system disposition within the zone.

After the information has been transferred to the ZHA Database, the database should be checked by the ZHA Team Leader to ensure that the results are credible and accurate, and that consistency of terminology and severity classification has been applied. The ZHA inspection conduct process is summarised in *Figure 7*.

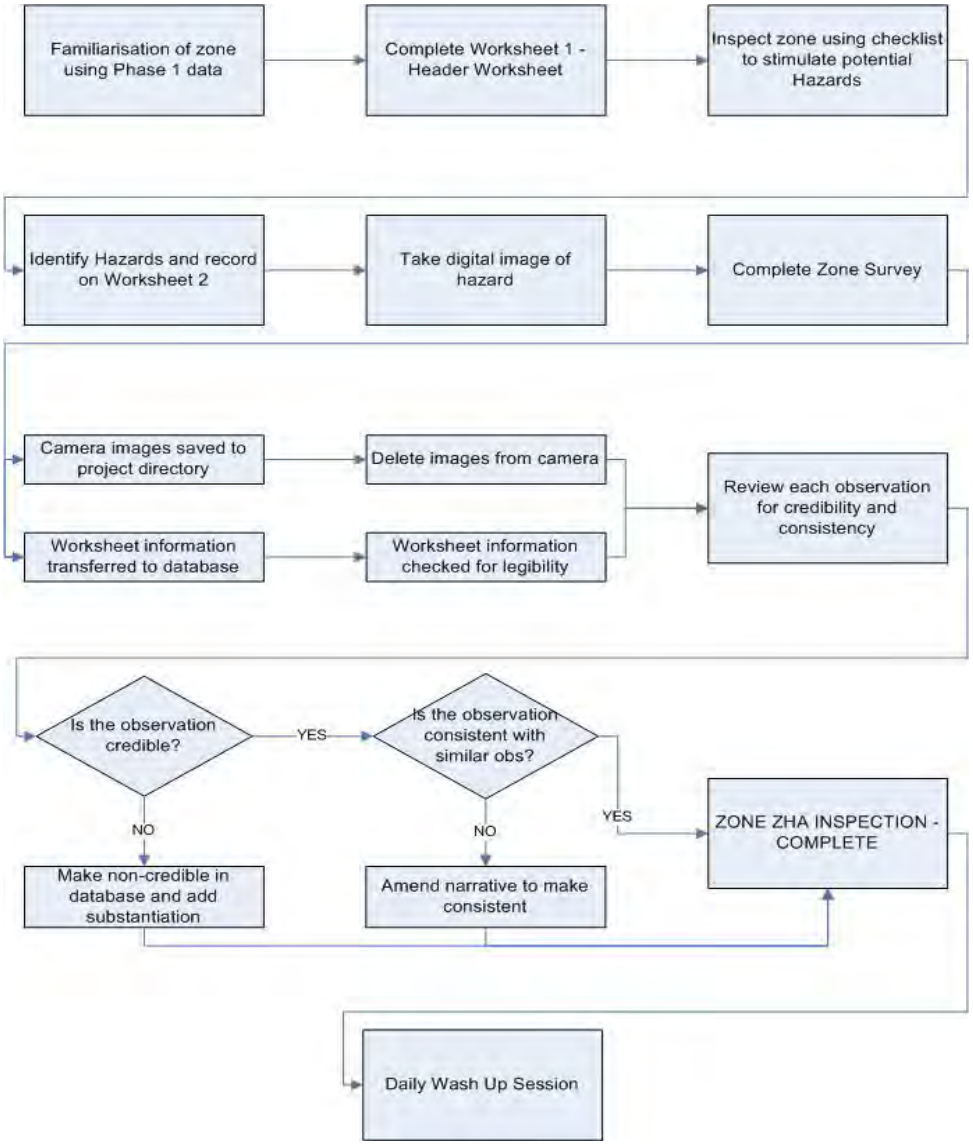


Figure 7: ZHA On-aircraft Inspection Conduct Process

IDENTIFICATION OF CROSS ZONAL HAZARDS

An element of a ZHA which can get over looked is the need to identify cross zonal hazards. The identification of all credible cross-zonal hazards requires a systematic review of how every possible hazard cause in each zone may interact with all systems in every other zone. Therefore, the optimum time to conduct this is after all the individual zonal hazard identification surveys have been conducted, when the analyst has identified the range of possible hazard causes and the potential vulnerability of affected systems and components. Depending on the aircraft size and complexity, a comprehensive cross-zonal hazard identification exercise can therefore be a significant undertaking.

A judgement on how to limit the scope of the identification of cross-zonal hazards is therefore necessary in order to ensure that resources are proportionally focused. The basis for this decision must be whether it can be shown that the possibility for the conditions for credible cross-zonal hazards to exist between two separate zones is reasonable. The factors that influence this include the: degree of spatial separation between zones; the nature of the boundary between

zones; and, the attributes of the initiating cause (e.g. does it involve the release of components or debris with a high kinetic energy that can span multiple zones) and potentially affected system or component. Whatever choice is made, these should be recorded as assumptions so that the results of the ZHA can be assessed in their proper context.

An area that can get overlooked within the Haz ID survey is the external surface of the aircraft. The external surface can facilitate the migration of system fluids from one zone to another, either from leaks within the aircraft or from components discharging fluids at the surface (e.g. blow off valves). Migrating fluids may hazardously interact with equipment located on the external surface, e.g. light fittings. This can be addressed by treating the external surface of aircraft as a distinct zone, subject to the same hazard identification process as the other zones.

Recording of Identified Hazards

ZHA Worksheets should be used to record the details of each zonal hazard that is identified during the inspection of each zone. A 'Header' ZHA Worksheet (referred to as 'Worksheet 1' in *Figure 7*) should be completed, which should contain the following information:

- Zone under inspection identification number;
- Name of inspector(s);
- Aircraft tail number;
- Aircraft Mk / variant;
- Zonal overview digital image identifier (ID);
- Inspection location;
- Date of inspection;
- Zone condition;
- Details of areas of the zone not covered in the survey;
- Visual impediments during the survey.

'Supplementary' ZHA Worksheets (referred to as 'Worksheet 2' in *Figure 7*) should then be completed, which should contain the following information:

- Details of each individual zonal hazard identified in the zone;
- The digital image ID of each identified zonal hazard image;
- Details of each accident that is associated with each of the individual zonal hazards;
- The severity classification of each accident.

3.4 PHASE 2B: ZONAL HAZARD RISK ASSESSMENT

The recommended approach to the risk assessment of each zonal hazard follows the principles described in RA1210 [5] and can be broken down into two main constituent parts:

- Probability data gathering - in which the evidence to underpin the probability values assigned to the identified hazard causes is collated and a probability figure for the identified hazard causes is derived;

- Risk assessment - in which the single risks arising from identified zonal hazards are assessed.

As this approach is common to all hazard analyses techniques it is therefore only covered in limited detail below.

PROBABILITY DATA GATHERING AND HAZARD CAUSE PROBABILITY DERIVATION

There are a number of different sources of in-service information that can be used to help derive a representative probability for each zonal cause. However, each source has different characteristics that influence how it can be used to help predict the future behaviour of a given component, system or platform. These information sources broadly can be divided into those which can be used to support a quantitative probability value and those which are better suited to supporting a qualitative probability assessment.

The information sources and their attributes that can be used to ultimately derive a qualitative probability figure are:

- **In-service Maintenance Data** – this includes general fault and failure information recorded on aircraft maintenance work order/Form 707 entries. These recorded faults and failures can, in some instances, be equated to one of the identified zonal hazard causes and by gathering fleet flying hours over an appropriate period, a historic arising rate for the given fault or cause per flying hour for the fleet can be produced. However, as this information does not capture the zone the fault or failure occurred in a zonal arising rate can only be approximated.

- **Safety Occurrence Reports** – these are raised on an aircraft fleet over its in-service life and can be gathered from the Air Safety Information Management System (ASIMS) network. Most relevant to determining a hazard cause probability are the occurrence reports raised via the Defence Air Safety Occurrence Report (DASOR) mechanism, as these capture accidents, hazard causes and other contributory factors. As with maintenance data, safety occurrence data can be used with fleet flying hours information to derive a historic event arising rate per flying hour.

However, for both these sources, not all arising events are noted by operating personnel and not all events are recorded. Moreover, there may also be errors in the codifying of maintenance

data within various databases that mask the true experienced rate of occurrence. These issues coupled with the recognition that the operating environment at the time of the data capture may be different to that which may occur in the future means that a hazard cause probability value derived from only these sources would not attract a high degree of confidence.

The qualitative sources of information that exist include:

- **Condition Survey Results** – CS results can be sorted, typically, by zone, system and observation and provide direct evidence of the scope of environmental and accidental damage that can arise on a platform and identify zones that are particularly subject to certain component or system failure modes or accidental or environmental damage.

- **Anecdotal Information** – this represents the experience of operating, maintenance and training personnel. It can be captured by conducting a series of interviews in which experienced personnel identify the frequency at which certain faults, failures and other operating events could be expected to occur for a given context.

There is no single approach to the identification of a hazard cause probability that is universally adopted; however, given the attributes of the data sources described above, the following approach has been found to be effective. For each hazard cause:

- A search of maintenance data and safety occurrence reports for instances which match the identified cause can be carried out. Using the identified number of instances in conjunction with the fleet flying hours over a given period will permit a basic quantitative fleet arising rate per flying hour to be produced for each cause.

- The basic probability figure should then be subject to a further review informed by the available qualitative sources and adjusted, as necessary, to ensure that probability figure represents all sources of information and, aided by the views of the operating community, represents as far as possible the future operating context. For example, if the anecdotal evidence suggests that arising rate of the event is more or less than the basic rate, then the analyst can use their judgement to adjust proportionately the basic rate to ensure that the resultant probability better reflects expected future behaviour.

Use of these diverse sources of information in concert should help reduce the likelihood of erroneous hazard cause probabilities being derived. Experience suggests that, in some instances, there will be notable discrepancies between the arising rates suggested by the anecdotal or condition survey evidence and the basic arising rate that will require careful consideration. Where no quantitative information is available to inform the probability derivation, then the analyst will have to make a solely qualitative judgement. In these latter circumstances, this may affect the confidence level associated with this probability value.

To determine the risk posed by individual zonal hazards representative accident sequences need to be created. Each accident sequence will include the constituent hazard causes and any other causal factors such as the effect of the spatial separation between applicable components or the properties of physical barriers between a failed and vulnerable component.

Once created, the probability derived for each hazard cause and that used for each causal factor can then be applied to each element of the accident sequence. Using the normal rules of probability theory an overall accident sequence probability can then be derived.

If the task requires the post-mitigation risk level to be assessed, then the fundamental accident sequence probability should be adjusted to account for each relevant mitigation or control. The degree of effect that a mitigation or control has on the accident sequence should be justified. As with the selection of probability of a hazard cause, it should not be assumed that mitigation performs as claimed by the design organisation is valid and, as appropriate, analysts should challenge quoted performance figures.

A judgement must also be made on the severity of the accident being considered and the resultant accident sequence probability and severity can then be classified using the definitions defined in the platform's safety management plan (SMP). These can then be used to derive a risk level using the hazard risk matrix defined in the SMP, although these risk levels should only be regarded as provisional until the results are sentenced by an appropriate Letter of Airworthiness Authority Holder.

In some circumstances, an assessment of risk using probability classifications derived only from fleet arising rates may be pessimistic. If a zonal hazard results from a potential interaction between two components in a single or a limited number of zones, then the use of fleet arising rates for each hazard cause will overstate the likelihood of that interaction occurring in the single zone. If the provisional risk from this is shown to be high, then further effort to derive a zone based probability figure will be necessary to determine the more realistic risk estimate.

3.5 PHASE 3: REPORTING

It is important to have in place an effective reporting framework for the ZHA undertaken. This will aid communication between the organisations involved in the ZHA, help manage identified project risks, enable any significant safety issues identified to be promptly dealt with and ensure that the ZHA product produced by the ZHA Delivery Organisation meets the TAA needs with respect to providing suitable evidence to argue that the ZHA Goal has been satisfied. To meet these objectives, experience has shown that once the preparation activity has been completed the following reporting framework is effective.

Routine Progress Meetings

The ZHA Task should include regular progress meetings. These provide a useful forum to inform stakeholders of the progress of the ZHA, to raise issues that could hinder the progress of the ZHA and to provide details of zonal hazards that have been identified during the inspections so far and review any Interim Reports produced to date (see below).

The Platform PT should organise these meetings, which should be held at regular intervals following contract award and throughout the Project. The Platform PT should provide a Chairman and Secretary for each meeting and should issue a full set of meeting minutes soon after the meeting. The suggested attendees for each progress meeting should be agreed during Phase 1; but should include the ZHA Team Leader, the ZHA Project Technical Lead and representatives from the Platform PT and the Platform DO.

Interim Reports

The ZHA Provider should produce a series of interim reports, at a frequency and depth agreed between the ZHA Provider and the Platform PT. These reports should detail the progress made on the ZHA to date, identify the main hazard trends identified so far and identify any risks to the successful completion of the ZHA.

Exception Reports

A mechanism should be put in place to ensure that any issue identified during the ZHA, which could have a significant and immediate impact on safety or airworthiness, should be reported straight away, by the ZHA Team Leader, to the Platform PT ZHA Focal Point. This should enable the Platform PT to undertake appropriate action as soon as possible. Such issues should initially be reported verbally and then followed up as soon as practicable with a written Exception Report.

Final Report

The ZHA Provider should also produce a Final Report for the Platform PT. The exact structure of a Final Report should be agreed between the ZHA Provider and the Platform PT and will vary from task to task depending on the needs of the PT and the results of the ZHA. However, to ensure that a judgement can be made on whether the ZHA has produced trustworthy and appropriate evidence to satisfactorily argue that the ZHA Goal has been met, it is recommended that the following issues are covered as a minimum:

- The Goal of the ZHA
- The ZHA Scope, Exclusions and the Assumptions used.
- A method statement, describing the hazard identification and analysis approach adopted.
- A list of the zonal hazards identified and the related risk assessments.

In addition, the ZHA can include details of other airworthiness of husbandry trends (e.g. instances of poor wiring husbandry) identified during the course of the Project. As a consequence of the hazards captured and other issues identified, a list of recommendations can also be captured at the end of the Final Report

4 RESULTS EXPLOITATION

4.1 OVERVIEW

The implementation of an effective ZHA Strategy undertaken by the TAA should ensure that a DH has sufficient evidence to support a safety case claim that the risk from zonal hazards on the aircraft they are responsible for is acceptable. However, if the results of ZHA are managed effectively they can be also be used to inform the overall understanding of risk present on an aircraft, initiate risk reduction measures and help sustain the airworthiness of that aircraft.

4.2 IMPROVING THE UNDERSTANDING AND MANAGEMENT OF RISK

INTEGRATING ZONAL HAZARDS INTO A HAZARD LOG

Following the process defined in RA1210 [5], once a list of zonal hazards has been identified for a given platform these need to be reconciled with and captured within the applicable platform hazard log. This step will identify any unmanaged hazards. It will help ensure that the hazard log is as representative as possible and it will help ensure that the identified zonal hazards are managed effectively throughout the life of the platform.

It is difficult to prescribe clear rules on how this should be done, as this depends on the attributes of the individual zonal hazards being considered and the structure of the existing platform hazard log. However, it is important to ensure that the zonal hazards are represented at the appropriate level in the platform hazard log. If this is not done effectively, then the inclusion of a large number of zonal hazards can make the hazard log disproportionately large and therefore difficult to manage.

For example, if we consider the example of the zonal hazard of ‘a leak of hydraulic fluid ignited by arcing and sparking EWIS’: This zonal hazard is likely to occur in many different zones on the aircraft. If each instance of this is captured as a discrete hazard in the hazard log, then the hazard log will grow significantly. Given that the accident sequence associated with this hazardous interaction is relatively short, it may be more appropriate to group together all the instances of this zonal hazard across the platform and to capture this as a single platform level hazard. Separate causes can then be identified to address the potential for hydraulic fluid to leak and for the EWIS to act as a source of ignition. Detail of where the individual zonal hazards occur and other relevant information could then be detailed within the text associated with the platform level hazard.

In other instances, the ZHA may identify zonal interactions that involve more complex or lengthy accident sequences, such as where a zonal interaction causes a loss of function of a single instrument or communications channel. In these cases, it is still likely to be appropriate to group together the zonal hazards that have the same accident sequence but occur in different zones.

However, given the longer accident sequence involved, this type of aggregate zonal hazard is more likely to be captured as a hazard cause in the platform hazard log.

If the platform hazard log is well structured and complete, it may be that its existing hazards and hazard causes are already linked together to create accident sequences that satisfactorily represent the zonal hazards identified in the ZHA. In these cases, a safety manager may only need to review the hazard log content and the associated probabilities used to ensure they remain appropriate and are not adversely affected by the presence of new identified zonal hazards.

In other cases, a suitable platform level hazard may exist to represent an aggregated zonal hazard, but the available hazard causes are not suitable or they are in place but are not linked to this hazard. In these cases, a safety manager may need to create new accident sequences and hazard-cause linkages to represent a particular zonal hazard. However, there may be a few instances in which the accident sequence associated with a particular identified zonal hazard is simply not captured in the hazard log and no suitable platform level hazards or causes are in place. In these cases a wholly new accident sequence, involving new hazard and cause entries will need to be created.

Where a new accident sequence is required to be created for the platform hazard log, a risk review process following the protocols defined in RA1210 [5] should be followed and confirmation of whether the resultant risk is ALARP or not should be established. The process for doing this for zonal hazards is the same as any other class of hazards and therefore this Paper will not examine this further.

IMPROVE UNDERSTANDING OF AGGREGATE RISK

The results of a ZHA can also be used to improve the level of understanding of the aggregate risk present on the subject aircraft type. RA1230 [15] introduces a design safety target criteria for all UK military aircraft. TAA are therefore required to show that the cumulative probability of the loss of the aircraft they are responsible for and the cumulative probability of a technical fault leading to the death of any aircrew or passengers should be of the order of at least $1x10^{-6}$ per flying hour (and $1x10^{-7}$ per flying hour for passenger carrying aircraft).

Commonly, a loss model, derived using FTA, is used to derive this cumulative probability figure. However, the trustworthiness of the loss model output is related to the degree to which it represents the credible accident sequences on the subject aircraft, including the influence of CCF. Therefore, a completed ZHA can be used to review the existing loss model to determine whether it correctly includes all the identified zonal hazards and hazard causes. If any differences are identified, then the loss model should be amended to include the missing hazard and/or cause. These actions should give TAA increased confidence that the loss model utilised to help determine if the requirement specified in RA1230 [15] is being met is realistic.

However, in many Project Teams, these loss models have been constructed by different organisations, at different times, to those conducting the hazard identification and analysis

techniques that inform it. The extant loss model and any subsequent analyses conducted may therefore have been constructed using different sets of assumptions and boundaries. Where it is identified that the loss model should be updated post the completion of a ZHA, care should be taken to ensure that the assumptions and context associated with the ZHA are coherent with those used in the loss model otherwise flaws may be introduced into the model.

4.3 SUSTAINING AIRWORTHINESS

ADDRESSING RISKS AND AIRWORTHINESS ISSUES IDENTIFIED

Once identified zonal hazards and the associated accident sequences have been reconciled with the relevant platform hazard log, as part of the ALARP evaluation process, TAAs may to seek to remove or mitigate individual zonal hazards. In addition, the conduct of a ZHA may identify other airworthiness issues that, if effectively addressed will help sustain the airworthiness of the platform. Examples of the type of follow-on action that a TAA may therefore initiate following a ZHA, to address risks and sustain airworthiness, are detailed below and further, more detailed examples of follow up action can be seen in Appendix A.

A TAA may issue a SI(T) pending more permanent preventative measures being taken. For example, during one ZHA undertaken by the authors, instances in which flying control cables were found to be chafing against structural features were observed. If unaddressed, this could result in a loss of flying control cable integrity and a subsequent loss of control accident. The TAA therefore issued a number of SI(T)s to address the lack of clearance between the cables and the structure and restore the aircraft to the correct design configuration, thereby removing the hazard initiating mechanism .

In another case, during the hazard identification activity on one aircraft, it was noted that an accelerant was leaking from a union and pooling within a zone. This pooling increased the probability of that fluid being ignited by a nearby electrical ignition source and the accumulation of debris that would encourage the erosion of the structure surface finish. An SI(T) was raised to periodically clean the affected area, in order to minimise the exposure of the leaked accelerant to ignition, whilst a more permanent solution was considered.

In addition, as a consequence of the detailed physical examination of an aircraft carried out as part of the zonal hazard identification activity and the accompanying use and scrutiny of the ADS carried out as part of the hazard analysis activity, a ZHA Team can identify other airworthiness issues that a TAA or other organisations should address in order to sustain airworthiness.

For example, a ZHA Team may identify trends, such as the prevalence of poor wiring husbandry in certain zones of an aircraft. This information can be used to inform awareness campaigns conducted by fleet Continuing Airworthiness Management Organisations and the scope of issues addressed in zonal survey training. The ZHA Team may also identify errors or weaknesses in the ADS that need to be corrected in order to reduce the risk of future maintenance error.

INFORM RELIABILITY CENTRED MAINTENANCE (RCM) DERIVED MAINTENANCE POLICY

A completed ZHA can also inform the development of a preventative maintenance policy derived by RCM and help ensure that the inputs to the RCM process are accurate and representative of current operations. The ZHA will consist of a list of independently identified system to system interactions, other condition based observations and revised probability assessments of hazard causes. Therefore, as part of a continuous review process, these can be used to:

- Ensure that the criteria used for determining significant candidates for RCM analysis is relevant. The selection process for determining what systems or assets are subject to RCM analysis uses a prioritisation process that includes consideration of safety If a given system or component is associated with a number of significant zonal risks, then this implies that the system or component should be scored highly in any subsequent prioritisation process.

- Validate that the extant RCM analysis has identified all the credible failure modes (including dormant failures) and effects for each asset being considered. This can be achieved by cross-checking against identified zonal hazards that involve the same system or asset components that the RCM analysis has accounted for the identified credible zonal hazard causes.

- Validate the extant probability of occurrence used for the individual asset failure modes considered in the RCM process. As the probability values derived for use in the ZHA will have utilised a wide variety of sources and the most results, these can be used to confirm that the qualitative probability values used in the extant RCM analysis remain appropriate.

There are similarities in some areas in RCM methodology and ZHA in that secondary effects of functional failures are considered. However, caution should be exercised if it is intended to use the analysis produced from RCM to support solely a safety case claim regarding zonal hazards. The DEF STAN 00-45 [9] RCM approach uses FMECA, which considers the effect of functional failure modes; however, zonal hazards can arise as a consequence of events other than functional failures and are significantly influenced by the relative separation between an initiating cause and a vulnerable component. Therefore, without further on-aircraft hazard identification and analysis activity to address these particular zonal hazard attributes, it is difficult to claim that a comprehensive identification of zonal hazards has been completed.

INFORM AGEING AIRCRAFT AUDIT (AAA) SCOPE

The results of a ZHA can also be used to inform the prioritisation of work in an AAA. At present, RA 5723 [10] requires a TAA to initiate an independent AAA for each ageing aircraft fleet under their control 15 years after a type's declared In Service
Date (ISD), or at the mid-point between the declared ISD and the initial planned Out of
Service Date (OSD), whichever is soonest. Repeat audits are conducted at 10-year intervals.

RA5723 requires that an ageing systems sub-audit should be carried out. It does not explicitly specify what systems should be audited but makes suggestions and offers criteria that the sub-

audit should cover "*systems…… that are critical to airworthiness*" and "*systems whose failure could affect another system*." As the scope of an AAA is very large, it is to be expected that the audit will prioritise those systems to be assessed according to the given criteria.

As the latter criterion is similar to the definition of a zonal hazard produced in Section 1 and a list of zonal hazards similarly will identify which systems are critical to airworthiness, an up-to-date ZHA can therefore inform a system prioritisation process in order to help ensure that the audit is focused effectively. Moreover, as the scope of the AAA includes a CS, the ZHA informed systems prioritisation process can highlight those systems that must be covered in detail in the CS. The identification of target areas for the CS can also be informed by the other opportunity evidence gathered during a ZHA, such as husbandry trends.

In addition, the completion of a ZHA may provide evidence to support other airworthiness decisions. For example, it has been argued that the conduct and sustainment of a ZHA will provide a TAA with: assurance that there are no unidentified and unmanaged zonal risks present on a subject aircraft; confidence that the probabilities used for defined hazard causes remain appropriate; and, give supporting evidence of the general condition of the aircraft.

Consideration of all these aspects will provide a degree of confidence that certain threats to the system integrity of the platform have been recently assessed. Therefore, where there is an evidence gap, possibly arising as a consequence of lost records or difficulty retrieving design information, a ZHA may provide sufficient relevant information to support a particular safety claim. This potential use of ZHA results is particularly relevant for supporting life extension decisions were a diverse range of evidence is required to underpin a component lifing decision.

4.4 MEASURES TO REDUCE ZONAL RISK

Over the numerous ZHAs that the authors have conducted, consistent issues and trends have been identified related to the condition of the aircraft examined that have increased the level of zonal risk present on the subject platform. For example:

- Where the examined zone is not clean and contains debris and detritus, this has encouraged the accumulation of any leaked accelerant within the zone.
- If wiring husbandry standards have deteriorated this has increased the probability of the wiring insulation breaking down and creating an electrical ignition source.
- If there are no appropriate system interconnecting pipe clearances or satisfactory pipe clearances are not maintained this has increased the probability of pipe rupture and the introduction of accelerant or corrosive fluid into the zone.
- Where there is evidence of leaked toilet chemical fluids and toilet effluent, this identifies that there are risks to health and threats to structural integrity within the zone.

In all the above instances, a valid mitigation to these is the timely and effective application of a zonal survey. Therefore, TAA should place emphasis on: ensuring that their personnel are appropriately trained to conduct zonal surveys; that the application of these surveys is thorough; and, that the interval between zonal surveys is not disproportionately weighted towards maximising aircraft availability.

A trend analysis of identified credible zonal hazards has also shown that a high proportion of hazards result in fire and explosion. Of these zonal hazards, many arise due to the potential for leaks of accelerant to arise from pipe unions etc. However, determining a representative probability for these failure modes is difficult as the manufacturer's claimed performance of these components seldom matches operational performance, not all leaks are recorded and identifying the exact location of the origin of a leak can be difficult. Similar issues also affect the determination of other hazard cause probabilities. Therefore, to help gather better and more relevant information to inform the derivation of hazard cause probabilities it may be appropriate for TAA personnel to issue targeted Mandatory Fault Reporting Instructions to gather accurate information about the performance of those systems and components that can create significant zonal risks.

4.5 THE HADDON-CAVE NIMROD REVIEW

The Haddon-Cave Nimrod Review [16] details the findings of an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. The scope of this Review was broad, but it made several references to ZHA and detailed shortfalls in the Nimrod ZHA produced in support of the Nimrod Safety Case (NSC) in the following sections:

- Section 10A Preparation of the NSC Phases 1 & 2.
- Section 11 NSC Analysis and Criticisms.
- Section 22 Best Practice for Safety Cases.

The main ZHA related issues from these Sections have been identified and confirmation of where each issue is addressed within this Paper is detailed in Appendix C. Consequently, it can be seen that if a ZHA is undertaken using the approach defined in this Paper, a user can be confident that they will have addressed the main ZHA issues identified in the Nimrod Review.

5 CONCLUSIONS

Experience has shown that there are tangible risks to the safe operation of UK military aircraft arising as a consequence of the presence of zonal hazards on those aircraft. In this environment, DH must satisfy RA1210 that requires them to show RtL are at least Tolerable and ALARP, and, under RA1230 that the aggregate probability of the loss of an aircraft or personnel is in the order of $1x10^{-6}$ per flying hour. As a consequence of this it is essential that all DH ensure that an adequate safety strategy with respect to the risk posed by zonal hazards is in place for the aircraft in their AoR.

Current MRP guidance refers personnel to the civil standard ARP4761 and the associated ZSA methodology. However, completion of a ZSA alone arguably will not provide sufficient evidence to satisfy the requirements of RA1210 and RA1230. Any approach to zonal risks adopted must be focused on the capture and assessment of articulated zonal hazards. A ZHA conducted in the systematic manner described in this Paper fulfils this criterion.

In those circumstances where the subject platform has been subject to a change of use since any original zonal safety assessment has been conducted, or, where doubt exists as to whether the original zonal safety assessment was comprehensive or the assumptions and probability values used in the risk assessment can be seen to be no longer be valid, then it is appropriate to initiate a ZHA to derive up to date and objective zonal risk assessments. This will permit DH and TAA personnel to more confidently determine if the requirements of RA1210 have been met and, post a reconciliation of the identified hazards against an existing loss model, provide a greater understanding of whether the RA1230 aggregate probability target can be met.

As the potential scope of a ZHA is large, decisions will have to be made about the type and extent of system to system interactions considered. It is important that these scoping decisions are clearly stated, so a judgement on whether the evidence produced can satisfy its intended goal can be made and be coherently linked with other evidence within the Air System Safety Case.

Confidence that the ZHA conducted has been effective and efficient will be improved if objective SQEP personnel are used to ensure impartiality. Furthermore, if a wide a range of sources (including fault and occurrence data and qualitative SME feedback) is used to help derive the probability values used in the risk assessment then this will ensure the risk assessments are as representative as possible.

The completion of a ZHA and an appropriate safety strategy that ensures the ZHA is kept up to date will provide sufficient through life evidence to meet all UK regulatory requirements with respect to the risk posed by zonal hazards. Such an undertaking may also provide evidence to support other airworthiness decisions and help sustain the subject platform's airworthiness.

6 REFERENCES

1. ARP 4761, issued 1996-12, Guidelines and Methods for conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

2. Dstl, Task Order Form Task AA1103 Zonal Hazard Assessment, FTS/1000059398 dated 21 July 2011

3. Ericson C.A, Hazard Analysis Techniques for System Safety, 2005, Wiley.

4. Acquisition System Guidance (ASG) - Safety and Environmental Protection Website, www.asg.dii.r.mil.uk/index.htm

5. MAA, RA1210, Issue 3, Management of Operating Risk (Risk to Life)

6. DEF-STAN 00-56, Issue 6, June 2007, Safety Management Requirements for Defence Systems

7. DEF-STAN 00-970, Issue 6, January 2010, Design and Airworthiness Requirements for Service Aircraft

8. MAA, RA1205, Issue 3, Air System Safety Cases

9. DEF STAN 00-45, Issue 2, Using Reliability Centred Maintenance to Manage Engineering Failures

10. MAA, RA 5723, Issue 3, Ageing Aircraft Audit

11. Leveson, N.G, Safeware – System Safety and Computers, Chapter 14.1, 5th Ed, 2001, Addison Wesley

12. MAA, Systems Integrity Handbook – Guidance in Support of RA5721, Version 6.0

13. Health & Safety Executive, Reducing risks, protecting people, 2001

14. MAA, RA 1002, Issue 3, Competent Persons

15. MAA, RA1230, Issue 3, Design Safety Targets

16. The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, Charles Haddon-Cave QC, 28 October 2009

APPENDIX A: ZHA EXAMPLES

A.1 EXAMPLES OF ZONAL HAZARD CAUSES

A1.1 Exposed Hot Surface – Accidental Damage or Maintenance Error

- **Situation:** During the zonal hazard identification activity, it was noted that the insulation covering a bleed air component had been torn.
- **Hazard Cause Analysis**:
  - The surface of the bleed air component can reach temperatures above the flash point and auto ignition temperature of accelerants in the zone due to the presence of hot gas in the pipe/component.
  - The exposed hot surface can therefore act as an ignition source in a fire and explosion accident sequence.
  - Normally, this potentially hazardous feature is mitigated by the use of insulation.
- **Hazard Cause Origin**. However, a hazard cause is created in this context, due to the occurrence of accidental damage to the insulation exposing the hot surfaces of the bleed air component.
- **Post ZHA Action.** By addressing this hazard cause, a TAA can mitigate the fire and explosion accident sequence identified. Applicable actions from the TAA could be:
  - The issue of an SI(T) to regain the design configuration of the insulation.
  - Reviewing the installation instructions in the platform AMM to ensure they are effective and not open to misinterpretation.
  - Reviewing the zonal inspection regime to ensure that the zone is being inspected at a suitable frequency to minimise the exposure of any defective insulation to a leaked accelerant.
  - Increasing awareness of the wider implications of exposed hot surfaces to maintenance personnel.

A1.2 Leakage of Fuel – Ageing Effects

- **Situation:** During the zonal hazard identification activity, fuel leaks were noted along the wing.
- **Hazard Cause Analysis**:
  - If the fuel migrates cross-zonally and combines with a source of ignition it can result in fire and explosion.
- **Hazard Cause Origin.** Ageing effects have degraded the effectiveness of the wing tank seals, enabling fuel to leak out.
- **Post ZHA Action.** To mitigate the potential for these leaks to act as a hazard cause, contributing to a cross-zonal hazard and resulting in fire and explosion, a TAA could:
  - Review the maintenance policy associated with the tank sealing.
  - Ensure the CAMO briefs maintenance personnel on the potential for this problem to occur, increasing the likelihood that any instances of occurrence are spotted

A.1.3 Leakage of Hydraulic Fluid – Design Issue

- **Situation:** During the zonal hazard identification activity on a helicopter, it was noted that the hydraulic pipes serving the tail rotor servo were chafing on adjacent P clips.
- **Hazard Cause Analysis**:
  - Continued chafing could cause a loss of pipe integrity and the loss of hydraulic system pressure and introduction of accelerant into the zone. There could also be functional implications associated with the loss of hydraulic supply.
  - A leak of hydraulic fluid can contribute to a fire and explosion accident sequence and a loss of control in the air accident
- **Hazard Cause Origin.** The existing design configuration of the hydraulic pipes was insufficient to ensure adequate clearance between the pipes and adjacent fittings.
- **Post ZHA Action.** To mitigate the two potential accident sequences that this hazard cause can contribute to a TAA could:
  - Initiate modification action to increase the spatial separation between the hydraulic pipe and adjacent components.
  - Review the zonal inspection regime to ensure that the zone is being inspected at a suitable frequency to minimise the exposure of any chafes.

A.2 EXAMPLES OF ZONAL HAZARDS

A2.1 Ignition of Fuel by Hot Surface

Fuel supply union

HP / LP Bleed air valve

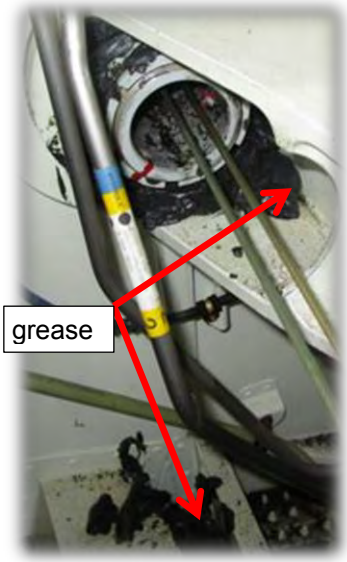
- **Situation**: During a zonal hazard identification activity it was noted that there was potential source of fuel leaks near to a hot surface.
- **Hazard Analysis**:
  - The fuel supply union has the potential to leak fuel. This is a zonal hazard cause.
  - The surface HP/LP bleed air valve can reach high temperatures, estimated to be above the AIT of fuel. This is a zonal hazard cause.
  - As the two hazard causes are in close proximity to one another, a leak of fuel could be ignited by the hot surface of the bleed air valve and result in fire and explosion.
- **Hazard Origin**: This hazard arose due to a design that does not mitigate the potential for fuel to leak downwards onto a hot surface that has the potential to ignite leaked fuel or vapour.
- **Post ZHA Action**: To mitigate this hazardous interaction, the TAA could initiate design modification action to shield the hot surface from any fuel leaks.

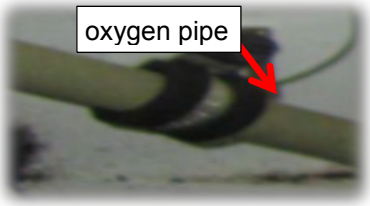
A.2 Control Restriction – Ageing & Design Issue

Cockpit trim becoming detached

- **Situation**: During a zonal hazard identification activity it was noted that the trim in the cockpit foot wells was loose.
- **Hazard Analysis**:
  - The trim in the foot wells is secured in place by Velcro strips.
  - Over time the effectiveness of the Velcro strips had degraded with the effect that the trim had become detached in places.
  - The detached trim could snag on the rudder pedals creating a control restriction hazard that could result in a loss of control accident.
- **Hazard Origin**: This hazard arose due to:
  - The application of the maintenance policy did not identify the failure of the Velcro and correct it.
  - Poor design that did not anticipate degradation of the Velcro
- **Post ZHA Action:** To address this hazard, a TAA could:
  - Initiate design action to remove the hazard. This could involve a modification that removes the Velcro and replaces it with a trim secured by a fastener.
  - Mitigate the hazard by issuing an SI(T) to replace the existing Velcro with new material and changing the maintenance policy to conduct directed inspections of the trim.

A2.3 Oxygen Enriched – Maintenance & Design Issue





- **Situation**: During a zonal hazard identification activity it was noted that grease had accumulated in the liquid oxygen compartments (LOX) of a large transport aircraft.
- **Hazard Analysis**:
  - The platform maintenance policy calls for the Nose Landing Gear (NLG) support beams to be lubricated with grease on a periodic basis. This activity resulted in grease extruding from the beam trunnions in the LOX zone(s). This creates a hazard cause.
  - The oxygen components in the zone(s) can leak from the system unions, valves or from damaged oxygen pipes. This creates a second hazard cause
  - A leak of oxygen could cause oxygen enrichment in the zone and the spontaneous combustion of the grease in the zone.
  - Mitigation features in place in this zone included caps that fitted over the trunnions and a warning notice telling maintenance personal to keep the zone free of grease and for the zone to be purged of oxygen before accessing the trunnion. However these were proven to be ineffective.
- **Hazard Origin**: This hazard arose due to:
  - A design that introduces a hazard in the zone without adequate mitigation.
  - A maintenance policy that is not sufficient to reduce the initiation of the grease hazard cause.
  - A lack of awareness amongst maintenance personnel of the hazard.

- **Post ZHA Action**: To mitigate this zonal hazard a TAA could:
  - Issue a SI(T) to ensure that grease has not accumulated in the LOX zone(s) on other aircraft in the Fleet.
  - Amend the existing maintenance policy in the platform AMM for the lubrication of the NLG support beam to include a specific requirement to remove extruded grease from the trunnion in the LOX zone(s).

APPENDIX B: ZHA TEAM ROLES AND RESPONSIBILITIES

Platform PT ZHA Focal Point

The ZHA Focal Point from the Platform PT should be responsible for:

- Liaising between the ZHA inspection team and the Platform PT;
- Ensuring the availability of appropriate aircraft, facilities and MOD personnel.

ZHA Project Manager

The ZHA Project Manager from the ZHA Provider should be responsible for:

- The day to day project management of the ZHA task;
- Ensuring that the ZHA task is completed on time, to cost and to the required standard;
- Reporting the progress of the ZHA to the Platform PT.

ZHA Project Technical Lead

The ZHA Project Technical Lead should be responsible for managing the overall technical aspects of the ZHA, including the provision of technical assurance of any ZHA output and also:

- Before commencing a ZHA ensure all team members are competent to conduct their role.
- Ensuring that processes and procedures are adhered to;
- Providing technical liaison with the Platform PT;
- Liaising with the Platform PT to arrange aircraft inspections and progress meetings;
- Ensuring that all ZHA inspections are undertaken by sufficient SQEP.

ZHA Team Leader

The ZHA Team Leader should provide the main point of contact between the inspection team and the Project Manager and ZHA Project Technical Lead. The ZHA Team Leader should also:

- Manage the technical aspects of the ZHA inspections;
- Direct the ZHA inspection team as required to undertake the inspections;
- Arrange for ZHA inspection support from aircrew or maintenance staff as required;
- Ensure that all ZHA inspection team members have undertaken appropriate ZHA training;
- Ensure that all team members comply with site Health and Safety requirements;
- Ensure that all technical ZHA information that is produced is accurate and consistent;
- Liaison with the Maintenance Organisation to determine aircraft and zone accessibility.

ZHA Database Administrator

The ZHA Database Administrator from the ZHA Provider should be responsible for:

- Ensuring that all ZHA Worksheets are legible;
- Controlling the configuration of the ZHA Database;

- Inputting data from the ZHA Worksheets into the ZHA Database;
- Ensuring that all ZHA Database entries have a supporting digital image;
- Ensuring that all digital images are saved in an appropriate secure ZHA Task folder;
- Converting all ZHA Worksheets to .pdf format for future audit purposes.

Safety Subject Matter Experts (Mechanical and Avionics Bias)

The inspection team should include Mechanical and Avionic Systems Safety SME who should:

- Inform the ZHA Team Leader of their progress;
- Identify and discuss zonal hazards with other members of the ZHA inspection team;
- Ensure that they methodically review the ZHA Checklist during the ZHA inspections;
- Ensure that they clearly and correctly complete the ZHA Worksheets;
- Encourage input and uninhibited 'hazard thinking' from all members of the ZHA team;
- Ensure they adhere to all onsite Health and Safety requirements.

Platform PT Representative (Senior Tradesman)

Platform PT Representatives, such as Senior Non-Commissioned Officers (SNCO) from various trade disciplines, may be required during the ZHA inspections to:

- Provide valuable specialist advice to the ZHA inspection team;
- Advise the ZHA inspection team of experiences gained from time spent within the Platform PT that may aid the inspections.

Squadron Representative (Junior Tradesman or above)

Squadron Representatives, such as Junior Non-Commissioned Officers (JNCO) from various trade disciplines, may be required during the ZHA inspections to:

- Assist with the identification of components;
- Advise the ZHA inspection team of valuable experience gained from time spent at squadron level that may aid the inspections.

Aircrew Representative (Part-time)

Aircrew representation is particularly useful during ZHA inspections within the cockpit zones and to identify operational issues that may have ZHA implications.

DO Representative

DO representation during the ZHA inspections is useful to:

- Assist with the determination of hazard 'credibility' using knowledge of specific items of equipment and operating parameters;
- Act as liaison with DO Design Office, as queries arise.

APPENDIX C: NIMROD REVIEW ASSESSMENT

Subject Area	Nimrod Review Reference(s)	Interpreted Issue	Discussed at SAAG Paper Section
Team Competency and Composition	10A.56	Consideration should be given for members to attend a ZHA induction session in order to meet the competency requirements. This should ensure that the team understand the techniques and worksheets and are familiar within the zones to be examined. Any course or dry run must include how inspection, recording and analysis should be carried out during the Haz ID.	• Sect 3.2, Identification of SQEP Team Roles (ensure team member briefed on their roles). • Sect 3.2, Inspection of As Operated Aircraft
	11.14[5]	It is important that team continuity is maintained throughout the ZHA task. Individuals that conduct the Haz ID survey should be the people that perform the subsequent risk assessment activity.	• Sect 3.2, Identification of SQEP Team (continuity)
Hazard Identification	10.A.174[2]	The 'as is' condition of the equipment must be recorded in the worksheet narrative, and if feasible in the associated digital image, should show the actual condition of the equipment. (For example torn insulation).	• Sect 3.2, Selection of Aircraft for Inspection • Sect 3.3, On-aircraft Survey, Recording of Identified Hazards,
	11.41	The Haz ID survey is more than just a physical survey of the zones. It should be considered a comprehensive inspection of the zone and adjacent zones which identifies undesirable interactions between systems, based on predicted failure modes and proximity of system equipment.	• Sect 1.3, zonal hazard definition, • Sect 3.3, Hazard Identification, • Sect 3.3, Cross-zonal hazard identification • Sect 3.4, Assessment of Risk
	10A.175	Technical assumptions regarding system operating conditions and parameters should be sought from the appropriate organisation, normally the DO. The ZHA analyst should not be afraid to challenge assumptions, or seek further 'sense check' advice from other sources, for example operators / maintenance	• Sect 3.2, Inspection of As-operated Aircraft

Subject Area	Nimrod Review Reference(s)	Interpreted Issue	Discussed at SAAG Paper Section
Assessment	10A.58	To ensure hazard cause probability values include operating experience, maintenance feedback must be included within any derived value. If nothing else it acts as a 'sense check; to any theoretical number.	• Sect 3.4, Probability Data Gathering and Hazard Cause Probability Derivation
	11.12[1]	Any quoting of design mitigation, such as fire detection / suppression systems should be fully supported. For example reference to AMM or correspondence from the DO. The ZHA analyst should not be afraid to challenge the validity of such mitigations.	• Sect 3.4, Assessment of Risk
	11.59	Extreme caution must be used if using generic probability data, particularly on legacy aircraft as the length in-service may invalidate initial probability values.	• Sect 3.4, Probability Data Gathering and Hazard Cause Probability Derivation
	22.42	The results of the ZHA should be used to generate new hazards or inform existing hazards with the Haz Log.	• Sect 4.2, Improving the Understanding of Risk

Report Documentation Form

1. Originators Report Number incl. Version No	QINETIQ/MS/AD/CR1200469	
2. Report Protective Markings UNCLASSIFIED		
3. Title of Report Guidance on the Conduct of Aircraft Zonal Hazard Analysis/Assessment		
4. Title Protective Markings incl. any Caveats	N/A	
5. Authors Jeff Jones, Mark Wilson		
6. Originator's Name and Address Mr. Mark Wilson MOD Boscombe Down, Salisbury, Wiltshire, SP4 0JF	7. Task Sponsor Name and Address Dr Steve Reed, Physical Sciences, Room 102-236, i-SAT-E, Bldg 5M [dstl] Porton Down, SP4 0JQ	
8. MOD Contract number and period covered		
9. Other Report Nos. N/A		
10. Date of Issue 28 September 2016	11. Pagination 47	12. No. of References 16

13. Abstract

This Paper describes the: requirement to conduct Zonal Hazard Analysis (ZHA); the different approaches to ZHA that a user might adopt depending on the position of the aircraft within its life cycle; and, describes a process for undertaking ZHA based on the Authors' own experiences. The Paper also details how the results of a ZHA may be exploited, including improving the Hazard Log, improving airworthiness standards and assisting the formation of the maintenance policy. Finally, the Paper demonstrates how issues raised in the Nimrod Review can be covered if the proposed ZHA method is carried out.

15. Keywords/Descriptors.

Ageing Aircraft Systems, Zonal Hazard Analysis, Zonal Safety Analysis, Zonal Safety, Zonal Survey, Condition Survey,