Version 1.0

HO-HHA-RP-v1.0

Human Hazard Analysis

Standardised Approach for Airframe Designers

Enter >

HeliOffshore
Safety Through Collaboration

Safety Through Collaboration

Collaboration empowers safety and is at the very heart of HeliOffshore. This Human Hazard Analysis is a great example of how our industry – from designers and maintainers, to pilots and passengers – works together and learns from each other to ensure no lives are lost in offshore flight.

I would like to thank the HeliOffshore Human Hazard Analysis Working Group, industry stakeholders and every HeliOffshore member who came together to deliver this guidance. Thank you for your commitment and contribution. Together, we will implement and sustain ever-higher levels of performance so those we are responsible for travel home safely every day.

Tim Rolfe
CEO, HeliOffshore

Publishing Details

Version: 1.0

Publication date: May 2021

Authors:
Dr Simon Gill – HeliOffshore
Dr Hazel Courteney – HeliOffshore

Contributors

The following individuals and their organisations have contributed to the collaborative effort of this Standardised Practise:

François Lassale	HeliOffshore
Steve Hazlehurst	HeliOffshore
Lee James	CHC Helicopter
Georges Devilliers	AIRBUS Helicopters
Raphaël Paquin	AIRBUS Helicopters
Fabien Bernard	AIRBUS Helicopters
Emanuele Bufano	LEONARDO Helicopters
Giorgio Dossena	LEONARDO Helicopters
Roberto Di Procolo	LEONARDO Helicopters
Francesca Barosio	LEONARDO Helicopters
Jamie Renna	Sikorsky Aircraft Corporation
Carlos Rios	Sikorsky Aircraft Corporation
Tony Randall	Bell
Neil Barton	Bell
Peggy Hardison	Bell

Table of Figures

Section 1 Description

Section 1
Description

1.1 Background

Throughout the design of a new helicopter the Original Equipment Manufacturer (OEM) undertakes a series of iterative analyses to ensure that the aircraft is meets certification requirements and best meets the needs of its customers. Once the aircraft type is in service, the OEM seeks feedback from the users, including maintenance engineers, on any potential sources of improvement. However, many studies illustrate that maintenance engineers are problem solvers and adapt to any issues they encounter, resulting in a general lack of feedback. Often feedback is limited to when there is a safety or economic consequence.

In the design a new aircraft, OEM design engineers, although guided by experience within the organisation and customer interaction, must make assumptions about the maintenance environment and how maintenance will be conducted (so called "work-as-imagined") and procedures are written accordingly ("work-as-prescribed"). Many studies have shown that how maintenance engineers actually conduct that maintenance can deviate from this ideal ("work-as-done"). The gap between these is the source of considerable value, identifying improvements to the design, procedures, tooling and training which could be made by either the OEM or the aircraft operators, often before experiencing any consequences. This philosophy of learning from everyday work is becoming established as an important technique in safety practice (Hollnagel, 2018).

The Human Hazard Analysis process, based on a process used in fixed wing aircraft design (Gill, 2009) and adapted by HeliOffshore, explores these gaps and the most appropriate way to manage them by bringing together relevant personnel in a workshop setting. This can be done during the design of a new aircraft or assessing an aircraft already in service. The process, facilitated by a Human Factors specialist, is a systematic method similar to the well-established Failure Mode and Effect Analysis. In an ideal world this is conducted across all systems in the aircraft but in reality, such a process must be focussed on the areas of greatest potential value. The process therefore focusses on critical components as identified by the OEM's existing safety processes. A structured approach supports the decision-making regarding the best way to manage the identified gaps, applying a uniform criterion across all aircraft systems.

1.2 Philosophy

This Industry Standard follows the principles of Performance Based Regulation, setting the high-level steps defining the target outcomes ("what needs to be achieved"), rather than prescribing the processes, techniques, or procedures ("how it should be achieved"). Best practice and workable alternative methods are provided to support the "how".

1.3 Scope

The Standard can be applied to the following scenarios. Where there are specific issues concerning each scenario, they are explained in the relevant section:
- development of new aircraft;
- the review of any updates to in-service aircraft (e.g. new design features or kits);
- proactive assessment of in-service aircraft (e.g. HHA workshops);

The basic steps in the process are the same in all cases. There are some differences in the detail of process, depending on whether it is a new aircraft design or an existing aircraft. For existing aircraft, full details are already known, and in-service experience is available. For new designs, a more speculative approach is needed, but it is more effective in terms of preventative action and product lifecycle cost. Differences in process are identified in the detail of each stage.

1.4 Intended Users

The intended users of this document include, but are not limited to, airframe manufacturers, system integrators and equipment suppliers who are involved in the design and the assurance of continued airworthiness of civil aircraft and the associated systems and equipment.

1.5 How To Use This Document

The intent of this document is to illustrate methods that may be used to assess the human factors of maintenance, and the contents may be considered at any point in the aircraft lifecycle.

This document supplements the Society of Automotive Engineers (SAE) Aerospace Recommended Practice 4761 (ARP4761) and ARP4754. These present guidelines for conducting an industry accepted safety assessment to show compliance with EASA and FAA 27/29.1309 and aid in the development processes which support certification of aircraft systems respectively.

The specific application of such activities needs to be established by the organisation conducting the assessment and the appropriate recipient. "Example of Use in Practice" sections are provided throughout the document with additional information on how the process has been adapted by a particular organisation.

1.6 Definitions

When the following terms are used in the Standard, they have the meanings indicated below:

Control Measures	Interventions which are designed to manage an identified error
Critical Component	A component identified during the design and certification process as one whose failure could result in hazardous or catastrophic consequence (related to terms already defined in Certification as “Important Parts” or “Critical Parts”)
Error Risk Rating	A numerical value given to an identified error according to the likelihood the control measures will fail and the consequence of the most credible outcome
Hazard	A condition or an object with the potential to cause or contribute to an aircraft incident or accident
Human Hazard Analysis	A process to identify gaps between the way in which the designer intended the component to be maintained, the way in which the procedure specifies how it should be carried out and the way in reality it is, or could be maintained (including potential errors) and the analysis of such gaps
Performance Influencing Factors	Factors that have the potential to influence the way in which a maintenance task is performed
Reasonably Foreseeable	An action which has been determined, according to the participants of the workshop, to have a fair and sensible chance of occurring
Work-As-Done	The way in which the maintenance engineer actually carries out the maintenance task
Work-As-Imagined	The way in which the maintenance task will be carried out, as imagined by the designer
Work-As-Prescribed	The way in which a maintenance task should be carried as prescribed by the author of the procedure

1.7 Abbreviations and Acronyms

ALARP	As Low As Reasonably Practicable
ARMS	Aviation Risk Management Solutions
ARP	Aerospace Recommended Practice
ATA	Air Transport Association
CAA	Civil Aviation Authority
EASA	European Aviation Safety Agency
ERCS	European Risk Classification Scheme
FC	Failure Condition
FMEA	Failure Modes and Effect Analysis
FMECA	Failure Modes, Effect and Criticality Analysis
FTA	Fault Tree Analysis
HEMEA	Human Error Mode and Effect Analysis
HF	Human Factors
HFIX	Human Factors Intervention Matrix
HHA	Human Hazard Analysis
ICAO	International Civil Aviation Organization
MEDA	Maintenance Error Decision Aid
MEMS	Maintenance Error Management System
OEM	Original Equipment Manufacturer
PIF	Performance Influencing Factor
PSSA	Preliminary System Safety Assessment
SAE	Society of Automotive Engineers
ZSA	Zonal Safety Analysis

Section 2 Human Hazard Analysis Overview

Section 2
Human Hazard Analysis Overview

Human Hazard Analysis (HHA) is a tool for engineers to use to influence the design of aircraft systems. It sets out a process owned by the Original Equipment Manufacturer (OEM) that may also consult the Operator's maintenance engineers for input. Aircraft design engineers already use tools such as Failure Modes & Effects Analysis (FMEA) to identify and manage any potential safety effects that could arise from technical failures. HHA is used in a similar way, to identify and manage any potential safety effects that could arise from human errors during aircraft maintenance activity, but also offers an opportunity to share and discuss actual maintenance practice. This supplements the existing practices used by some design teams to reduce vulnerability to human error. HHA provides the advantages that it:

- Offers a systematic, documented method that has industry wide recognition;
- Provides a common, consistent criteria for which issues do, or do not, require action;
- Creates a 'total system' approach to operational aviation safety.

2.1 Top Level Requirement

The top-level requirement can be set by the OEM to provide a uniform level of error risk tolerance across all systems. Examples of this could include the more abstract 'a single foreseeable human error should not be capable of causing a catastrophic loss' or, make specific reference to the HHA process, 'no risks rated 3 or above in the error risk matrix should remain without mitigation, whether by design, documentation or training'. This Standard allows the OEM the latitude to define their own requirement.

2.2 Process Summary

The HHA process overlaps with the System Safety and the Maintainability processes within an OEM. These processes can be used to identify critical components in Step 1 and capture the relevant information for Step 2. Steps 3 to 8 involve the sharing of ideas between OEM design engineers and operator maintenance engineers facilitated by human factors specialists. This can also utilize maintainability assessments, feedback from aircraft operators and accident/incident investigation results to develop insight into the real-life experience and challenges faced by maintenance engineers. Steps 9 and 10 identify error treatment solutions and their impact. Monitoring and measuring solutions is covered by Step 11. The HHA Process is summarised in Figure 1.

Figure 1 – Human Hazard Analysis Process Summary

Step 1.
Select Maintenance Tasks for Analysis.

Step 2.
Collect fundamental information regarding the critical component and maintenance task.

Step 3.
Identify and factors which could influence the performance of the maintenance engineer.

Step 4.
Identify any damage which this component could be subject to during maintenance.

Step 5.
Identify any foreseeable mainteance errors (including any damage identified previously).

Step 6.
Capture any notes regarding gaps between work-as-imagined, work-as-prescribed and work-as-done.

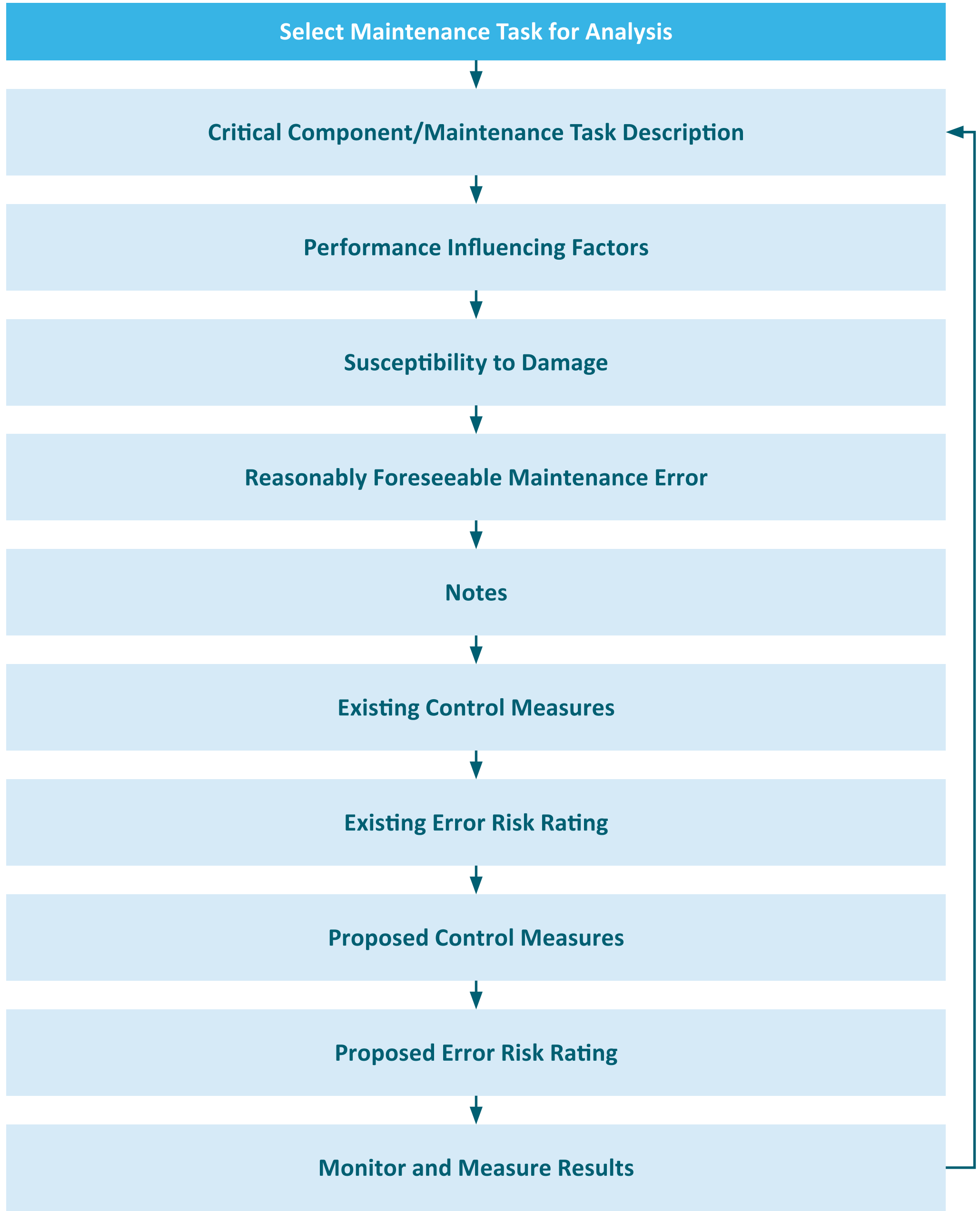
Step 7.
Explore what is already in place to manage the error (e.g. prevention, reduction, detection).

Step 8.
Agree the consequence of the identified error and the likelihood of the existing control measures failing to generate a risk rating.

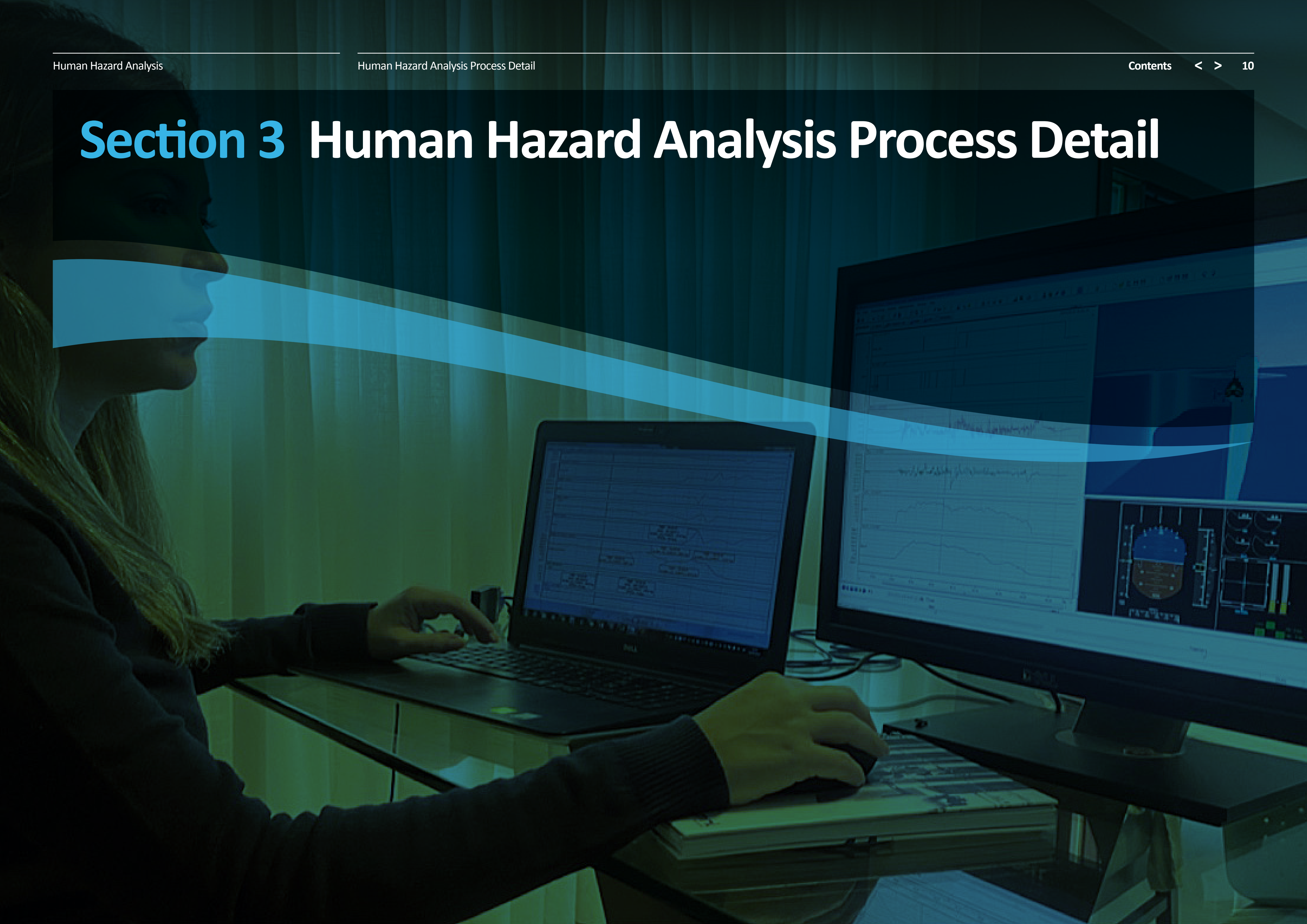
Step 9.
Identify the potential means to treat the error and the effect of these on the consequences of the error and the likelihood of their failure.

Step 10.
Agree the consequence of the identified error and the likelihood of the proposed control measures failing to generate a new risk rating.

Step 11.
Monitor the implemented solutions and measure its effectiveness to ensure the error treatment achieves its aim.



Section 3 Human Hazard Analysis Process Detail



Section 3
Human Hazard Analysis Process Detail

The process first identifies aircraft components to be analysed using existing safety processes, and then identifies the maintenance tasks related to those components. Then a Human Error Mode and Effects Analysis (HEMEA) develops the detail of the gaps existing between intent of design and procedures and the reality of maintenance. When a reasonably foreseeable maintenance error is identified, the process helps the participants to agree an Error Risk Rating based on the severity of potential safety consequences and the likelihood of existing control measures to fail. The HEMEA is a derivative of the Failure Mode and Effect Analysis (FMEA), a well-used analysis technique. It seeks to support the analysis of potential human errors and is a barrier risk model, similar to Bowtie and the Aviation Risk Management Solutions (ARMS) methodologies, both well-established safety techniques.

The HHA process is conducted using a workshop format. For a new design, this workshop would involve the system design engineers, maintainability engineers, one or more human factors specialists and any other relevant disciplines (possibly technical authors). For an existing design, this workshop would involve aircraft maintenance engineers.

The purpose of the workshop is to populate the HEMEA table by working through a standardised series of questions for the workshop attendees to consider, and agree the appropriate entry. These questions form the table column headings and address the subject areas listed in this Section.

3.1 Select Maintenance Tasks for Analysis (Workshop Preparation)

It is important to define the subset of tasks that will be subjected to analysis. It is neither necessary nor feasible to analyse the design features, procedures and documentation for every maintenance task on the aircraft. This first step selects those tasks that have the most potential for safety impact. This step is the same for new or existing designs. There are a number of possible approaches, including but not restricted to:

- All tasks that are performed on specific safety critical components (terms already defined in Certification as “Important Parts” or “Critical Parts”);
- All tasks that are performed in the proximity of specific safety critical components that may disturb that component when performed (e.g. identified from Zonal Safety Analysis);
- Certain types of task on critical components, such as installation, inspection and those tasks where there is a risk of damage during removal (i.e. either damage to, or by, the system);
- Within safety critical tasks, there may be a subset prioritized where tasks have characteristics that increase risk of error such as complexity, special tooling, non-standard procedure or access difficulty;
- Processes or installations identified as requiring attention by in service data or other processes or feedback obtained during in service or during development.

Analyses of maintenance error have consistently identified that errors made during installation represent the largest share (Graeber and Marx (1993); Courteney (2001), Hall (2003); Skinner (2003); Rankin and Sogg (2003); Gill (2007)). The UK CAA (2016) undertook an analysis of rotorcraft maintenance incidents and found that 43% of incidents related to installation error.

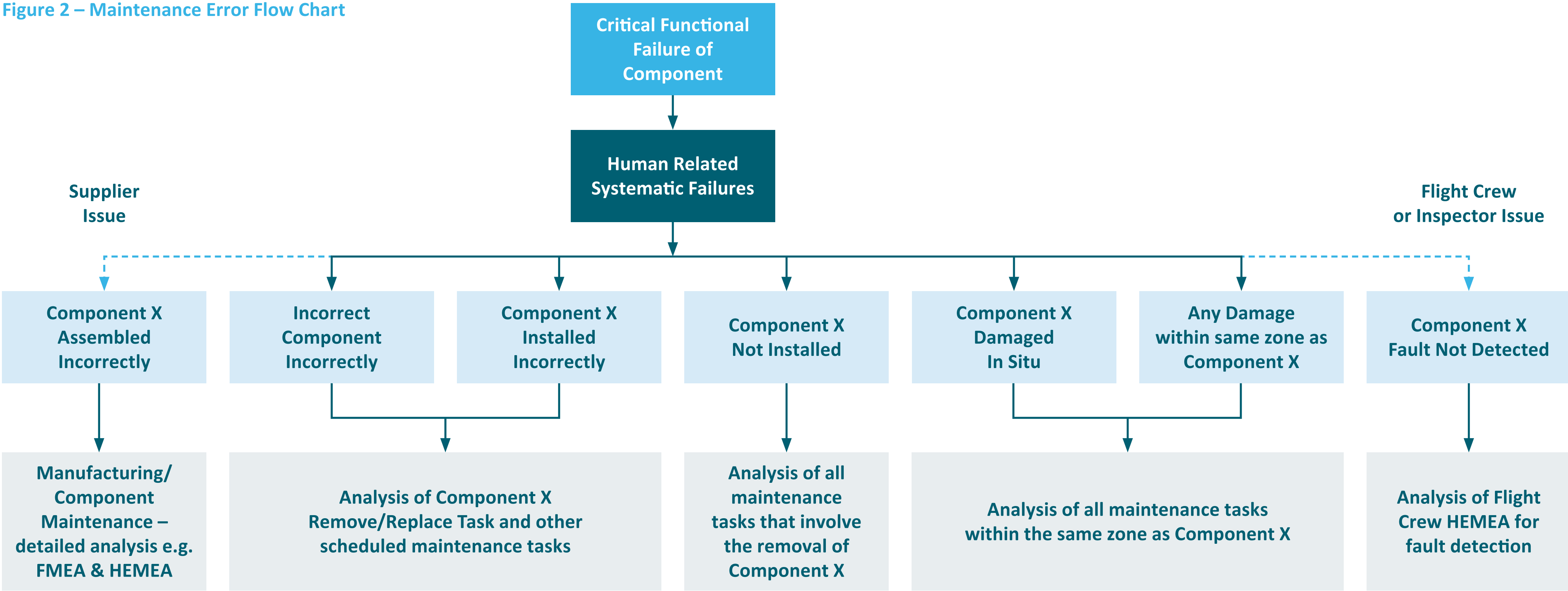
However, removal and inspection tasks are also relevant to safety and may therefore be included, albeit with additional or different criteria at some stages of the process.

3.1.1 Example of Use in Practice – Using Fault Tree Analysis (Fixed Wing)

The System Safety Process defines all functions required of the aircraft and identifies Failure Conditions (FC), the potential ways in which the aircraft may not be able to achieve such functions. These are cascaded from an aircraft-level to specific aircraft systems, and this is repeated to determine the FCs and their consequence at system level.

The Preliminary System Safety Assessment (PSSA) takes the FCs and determines the combinations of failures that would result in those undesirable system states. The so called “top-down” technique Fault Tree Analysis (FTA) is used to identify critical components and the critical ways in which they could fail. Components highlighted where one failure, or the combination of two failures, could result in a catastrophic FCs are chosen as candidates for HHA. Maintainability expertise is used to explore the maintenance tasks conducted on those components, or any other maintenance task that could result in the identified critical functional failure of the component. This is shown in Figure 2 (Gill, 2009).

Figure 2 – Maintenance Error Flow Chart



3.1.2 Example of Use in Practice – Using Design Assessment (Rotary Wing)

The Rotary and Rotor Drive System Design Assessment can be used to specify all critical components with the potential to cause Catastrophic effect, especially those which originate from Single Points of Failure. This is undertaken by the Safety and Reliability Department.

Once the critical components have been highlighted using the Design Assessment, any maintenance tasks associated with those components are identified by the customer support team (e.g. installation, removal or inspection). Input is also sought from feedback related to in-service experience and contribution to accidents/incidents.

3.1.3 Example of Use in Practice – Using Safety Input (Rotary Wing)

One OEM varies the process above. The list of maintenance tasks to which HHA is applied comes from:

- Design Office input (e.g. FMECA, stress analysis, safety analysis) to identify list of parts for which no maintenance error should occur, basically all dynamic system components (e.g. Rotor, transmission, suspension, flight control) or structural parts for which there is only one single load path.
  Those parts are classified as CRITICAL or IMPORTANT as per EASA regulation.
- In addition, a zonal analysis is performed to identify other parts on other system that could have an impact on CRITICAL or IMPORTANT parts during maintenance (using digital mock-up and maintainability specialist review of scheduled/ unscheduled maintenance in MSM Chapter 04/05)
  This list is called a "Sensitive Parts List" in this example.
- Once the complete part list is available, Support Engineers identify all related tasks. The list includes the inspection tasks AND their Installation/Removal
  This list is called a "Sensitive Task List" in this example.

3.2 Critical Component/ Maintenance Task Description (Workshop Preparation)

Once the list of tasks to be evaluated have been selected then more information must be gathered in advance of the HHA workshop. The additional information allows for the team to more accurately apply the error analysis during the workshop:

- Critical Component (P/N) – Reference or Part number of the component to be assessed;
- Critical Component (Description) – Description of the component to be assessed
- System – System of the component to be assessed;
- ATA – Air Transport Association (ATA) Chapter of the component to be assessed;
- Critical Maintenance Task – Maintenance task to be assessed;
- Documentation Reference – Reference within the maintenance manual;
- Maintenance Interval (Exposure) – Where applicable, the interval of scheduled maintenance, which defines the exposure to the error (i.e. if the interval is 15000 hours then the exposure to the error is small compared to a task which is undertaken every day).

3.3 Performance Influencing Factors

There are various factors that influence human performance and the likelihood of human error. Some residual level of human error will remain despite all Performance Influencing Factors (PIFs) being optimised, but the likelihood of error is lower. Of the PIFs that can increase the likelihood of error, some relate to the operational environment, ranging from engineer training to the physical environment in the hangar, but these are not considered here. Other PIFs relate to the system design and documentation; for the purpose of HHA for designers, these are the most relevant. It has been found useful to set the context for the analysis of each task by considering the presence of common design related PIFs.

The first stage of the HHA process conducted in the workshop is to assess the design related PIFs on a scale of 1-5 (according to the ratings described in Appendix A):

- Accessibility – Visual and/ or physical access to the component under assessment;
- Perceived task frequency – The perception of maintenance engineers of the frequency that the task must be undertaken. For example, if they believe it is undertaken too frequently engineers may omit the task or not refer to documentation;
- Demand on resource – The number of engineers needed to perform maintenance task or the amount of time is takes;
- Documentation – Documentation provided to guide the maintenance task. Note that in this section there is specific mention of the suitability of the documentation for inspection tasks (especially suggesting an assessment of the clarity of the pass/ fail criteria);
- Special tooling – Status of tooling required to undertake the maintenance task;
- Other – any other factor which could have a significant influence on maintenance engineer performance.

The review of PIFs in a new design is more complicated. Depending on the stage of design it may be difficult or impossible to review the PIFs, e.g. there may not yet be documentation in place, nor maintenance intervals defined. Review against comparable existing designs is important and consideration should be given to how its design is different and what impact that could have. This is an opportunity to guide those involved in the design to be considerate of these factors.

3.3.1 Example of Use in Practice – Use for Prioritisation of Tasks

In situations where the number of tasks identified in Step 1 is too great to be analysed in the time available, the Performance Influencing Factors have been used to prioritise maintenance tasks for more detailed analysis. In this case if any of the PIFs are rated by the workshop participants at a 3 or above then the analysis is continued. If none are rated at 3 or above the participants move to the next maintenance task.

3.4 Susceptibility to Damage

Any damage which the critical component could sustain due to any maintenance activities on this component, this system or an adjacent system or component, on- or off-aircraft. This is a free text field to allow an explanation of the issues identified.

3.5 Analysis of Reasonably Foreseeable Maintenance Error

It is not possible for designers to address every theoretically possible incorrect action that could occur whilst an engineer performs aircraft maintenance. Therefore, the potential errors addressed are restricted to those considered 'reasonably foreseeable'. For practical purposes, this should include errors that:

- Have been identified by the Safety Management system of the OEM and the Operators of this or other comparable aircraft, or by a Bowtie analysis, as being either errors that occur relatively frequently or errors that could directly contribute to the highest risk situations;
- Are errors of a type that have been identified through data analysis as common error types in aircraft maintenance and are considered by qualified aircraft maintenance engineers as a reasonable possibility;
- Other errors identified by qualified aircraft maintenance engineers as a reasonable possibility on this design (experience shows that engineers tend to be conservative in these judgements, so there should not be concern that this will produce too many possibilities).

The process then collates information relating to any maintenance errors identified as reasonably foreseeable:

- Type of Maintenance Error – the type of maintenance error which could be made during the Critical Maintenance Task according to a taxonomy, adapted from one developed by Airbus Helicopters who analysed all maintenance-related accidents and incidents on their helicopters up to 2005:
  - Incorrect component installed;
  - Component installed incorrectly;

- Component not installed;
- Damage not detected;
- Damage not properly assessed.
- Detail of Error – Free text explanation of the identified error.
- Frequency of Error – The assessment of the frequency of the identified error:
  - Has not happened before – a completely unknown error;
  - Has happened before on this aircraft type – an error known to have been made on this aircraft type;
  - Has happened before on other aircraft type – an error known to have been made on another aircraft type;
  - Has contributed to serious incident – an error known to have contributed to a serious incident.

3.5.1 Example of Use in Practice – On and Off Aircraft Review

In some cases, the participants of the workshop require more detailed investigation of the maintenance task. How this is achieved is dependent on the stage of design at which the analysis is performed. If the analysis is being conducted on an aircraft which is in-service then the options are to review an actual aircraft, the virtual design model (using Virtual or Augmented Reality) or an aircraft prototype. If the aircraft is in an earlier stage of design, assessment against comparable existing systems or the use of virtual reality is recommended.

3.6 Notes

Any relevant notes from the discussion of the maintenance task are detailed here. These notes capture the discussion between participants regarding any gaps between work-as-imagined, work-as-prescribed and work-as-done for future investigation by the OEM.

3.7 Existing Control Measures

Considering the identified error, it is important to explore what control measures are already in place to address this:

- Prevent Error – the most robust error management technique as it eliminates the possibility of the identified error and the resultant consequences (e.g. removing a maintenance task where an error is identified);
- Reduce the severity of the error and/ or its consequences – this does not eliminate the potential of the identified error, but reduces the severity of the error or its consequences (e.g. if an error occurs such a strategy ensures that the consequence is minor instead of catastrophic);
- Reduce Error Frequency – this strategy focuses on reducing the likelihood of the error occurring (e.g. increasing the maintenance interval to reduce exposure to the error);
- Ensure Timely Detection and Recovery (Maintenance) – enhancing the ability of the person who makes the error or another maintenance engineer finding and rectifying the error (e.g. an inspection focused on this particular error);
- Ensure Timely Detection and Recovery (Indication to Flight Crew) – enhancing the ability of the flight crew to find the error and allowing rectification (e.g. flight crew indication of an error).

3.8 Existing Error Risk Rating

The traditional way to classify risk is the product of severity and likelihood. This inevitably leads to two questions, the severity and likelihood of what? In 2010 the Aviation Risk Management Solutions (ARMS) working group proposed a new way of doing operational risk management (ARMS, 2010). This new way of assessing safety events has been adopted by EASA in the European Risk Classification Scheme (ERCS) (EASA, 2020). The HHA methodology applies this approach in the proactive assessment of risks associated with maintenance error.

To conduct the risk assessment two questions should be answered:

- Likelihood of control measures failing – the likelihood of the control measures identified in the previous stage failing:
  - Zero Likelihood
  - Very Unlikely
  - Unlikely
  - Possible
  - Likely
  - Almost certain
- Consequence of most credible accident scenario (Immediate or subsequent) – should the control measures fail what is the most credible accident scenario, which could occur immediately or at a subsequent time. These are defined according to the ICAO Safety Management Manual (ICAO, 2018):
  - No Consequence;
  - Negligible (“Few consequences”);
  - Minor (“Nuisance; Operating limitations; Use of emergency procedures; Minor incident”);
  - Major (“A significant reduction in safety margins, a reduction in the ability of operational personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency; Serious incident; Injury to persons”);
  - Hazardous (“A large reduction in safety margins, physical distress or a workload such that operational personnel cannot be relied upon to perform their tasks accurately or completely; Serious injury; Major equipment damage”);
  - Catastrophic (“Aircraft/ equipment destroyed; Multiple deaths”).

The combination of these answers defines the Existing Error Risk Rating according to the matrix shown in Figure 3 overleaf.

Figure 3 – Error Risk Rating Matrix

Consequence of most credible accident scenario →

Likelihood that control measures could fail ↓

	No Consequence	Negligible	Minor	Major	Hazardous	Catastrophic
Zero Likelihood	0	0	0	0	0	0
Very Unlikely	0	1	1	1	2	2
Unlikely	0	1	2	2	3	3
Possible	0	1	2	3	3	4
Likely	0	1	2	3	4	4
Almost Certain	0	1	3	4	4	5

This matrix identifies the risk related to the identified error in five levels which are summarized in Figure 4.

Figure 4 – Error Risk Levels

Risk Rating	Definition
1	No sensitivity to human error (easy to perform, no error risk, or errors cannot progress to significant safety risk)
2	Limited sensitivity to human error (less easy to perform, limited error risk, error could progress but very unlikely and/or limited safety risk in rare circumstances)
3	Moderate sensitivity to human error (not easy to perform, moderate error risk, error could progress but moderately unlikely and/or limited safety risk in unusual circumstances)
4	High sensitivity to human error (challenging to perform, high error risk, error could progress and/or safety risk is material in some circumstances)
5	Very High sensitivity to human error (interpretation difficult, risk to damage a/c while performing the maintenance, high error risk, error could easily progress and/or safety risk is significant in common circumstances)

These ratings allow the potential errors to be prioritised within the workshop, to assess whether new control measures should be introduced. It should be noted however, that this is just an indication of the sentiment of the attendees of the workshop, is not a definitive score, and should ideally be used as a relative measure of risk. Consideration should be given to the Strength of Knowledge, i.e. the confidence of the group in their assessment. Where significant assumptions have been made, the group should consider upgrading the risk to the next risk level.

If the Error Risk Rating is sufficiently high that it is decided that further action should be taken, then the process proceeds as described below; if not, then the process is considered complete, and provides a documented assessment to explain why further action was deemed unnecessary.

3.8.1 Example of Use in Practice – Operator Health and Safety

It is possible to adapt the levels of consequence to also consider the health and safety of maintenance personnel. Equivalent consequence ratings can be developed to enable issues which may not have an aircraft level consequence to still proceed in the analysis.

3.9 Proposed Control Measures

In the case where the Error Risk Rating is determined to be sufficiently high, the next stage of the process is to propose new control measures to treat the risk. Ideally this should be done within the workshop setting to elicit ideas from the group. A revised Error Risk Rating is then generated to assess whether the proposed solution is likely to create an acceptable level of error tolerance.

Cost inevitably becomes a significant factor in the decision and the solution should be evaluated according to the principle of “As Low As Reasonably Practicable” (ALARP). This allows risk to be managed to a point where the stakeholders accept the level of risk compared to the solution chosen.

The choice of error management strategy must proportionate and linked to the Error Risk Rating. In many cases it may be appropriate to use a combination of actions to achieve error management. These strategies have different levels of robustness as illustrated by Figure 5:

Figure 5 – Levels of Error Management Robustness

5	Prevent Error
4	Reduce Error Frequency and Reduce Error Magnitude and Improve Detection and Recovery
3	Reduce Error Frequency and Reduce Error Magnitude and Improve Detection and Recovery
2	Reduce Error Frequency and Reduce Error Magnitude
1	Reduce Error Frequency Improve Detection and Recovery

“Error Prevention” is the ideal error management strategy because it eliminates the error potential completely. Without prevention, there is an assumption that the error could occur at some time.

Proposals are made within the same categories as the Existing Control Measures:

- Prevent Error – Note that this strategy is highly recommended where a risk is identified with potentially Catastrophic effect;
- Reduce the severity of the error and/or its consequences;
- Reduce Error Frequency;
- Ensure Timely Detection and Recovery (Maintenance);
- Ensure Timely Detection and Recovery (Indication to Flight Crew).

3.9.1 Example of Use in Practice – Human Factors Intervention Matrix

There are alternative methods to support the choice of the most appropriate control measures. Once such example is the Shappell and Wiegmann (2006) Human Factors Intervention Matrix (HFIX) as shown in Figure 6. This requires a further, more detailed human factors analysis of the identified error which could be considered if the OEM has sufficient human factors resource available.

3.10 Proposed Error Risk Rating

Using the same process as the determination of the Existing Error Risk Rating outlined in Section 3.8, two questions should answered, assessing the design with the proposed control measures in place:

- Likelihood of the control measures failing:
  - Zero Likelihood;
  - Very Unlikely;
  - Unlikely;
  - Possible;
  - Likely;
  - Almost certain.

- Consequence of most credible accident scenario (Immediate or subsequent):
  - No Consequence;
  - Negligible;
  - Minor;
  - Moderate;
  - Hazardous;
  - Catastrophic.

The combination of these defines the Proposed Error Risk Rating according to Figure 3.

3.11 Monitor and Measure Results

Following the workshop it is critical that the error management proposal is assessed by the OEM, and its implementation measured and monitored. It is recommended that the following actions are undertaken by the OEM but internal processes will determine how this is achieved:

- Does the budget holder accept the proposed solution?
- Do all stakeholders agree with the proposed solution?
- Has the final proposal been implemented?
- What is the real impact of the implemented solution (including assessment of residual risks)?

It is also important to feed back the implemented solutions to the participants of the workshop, but also in the interest of safety, to the wider community (including where appropriate the HeliOffshore membership). This allows the loop to be closed as Operators will be able to feed back to the OEM the effectiveness of the implemented solutions.

3.11.1 Example of Use in Practice – Human Factors in Maintenance Safety Board

One way in which results have been measured and monitored is the establishment of a 'Human Factors in Maintenance Safety Board'. The purpose of this is to inform the safety department of identified issues, make sure each stakeholder is aware of the proposed interventions and to ensure that the organisation implements the agreed solutions.

Figure 6 – The Human Factors Intervention Matrix

	Organizational/ Administrative	Human/Crew	Technology/ Engineering	Task/Mission	Operational/ Physical Environment
Decision Errors					
Skill-based Errors					
Perceptual Errors					
Violations					

Section 4 Human Hazard Analysis Workshop

Section 4
Human Hazard Analysis Workshop

HHA is achieved in a workshop involving engineers with experience of maintenance and design engineers from the OEM, facilitated by a human factors specialist. There are a number of factors to consider regarding how the workshop is organised and run.

4.1 Participants

- Core Team:
  - Trained facilitator (with human factors expertise);
  - OEM Personnel with knowledge of the design and documented maintenance tasks of the specified components;
  - Operator Maintenance engineers, ideally from multiple operators in various regions (it is important to seek engineers with varied experience, involving both junior and experienced engineers and trainers). OEM maintenance personnel could also be invited but ideally in addition to the Operator engineers.
- Optional:
  - OEM safety specialists;
  - OEM accident investigators;
  - Customer support engineers;
  - Technical directors/ Chief Engineers.

For new designs, there will be no maintenance engineers with experience of the task. Therefore, maintainability engineers who have been involved in the process of design would be involved. They would use their experience of maintenance, their knowledge of the current state of design and the virtual prototype to anticipate the steps of the maintenance tasks to provide advice on best practice and suggestions on potential error.

4.2 Ground Rules

Setting the tone of the workshop is critical. The quality of the output depends on mutual trust within the group. Clear definition of the ground rules is therefore very important:

- Need for open, honest conversations;
- Need to actively change the way participants might historically have interacted;
- There must be:
  - An avoidance of defensive positions;
  - No rush to assign blame;
  - An acceptance of where improvements can be made;
  - Minimisation of protection of perceived reputations.

4.3 Briefing

All attendees should be briefed in advance on the following issues:

- What to expect;
- Definition of ground rules;
- What they will need to contribute;
- A request of maintenance engineers to bring MEMs Data, known gaps between procedures and practice and any relevant maintenance errors.

One the first day of the workshop a more advanced briefing is conducted including:

- Introduction to the HHA workshop;
- Human Factors in Design Process;
- Supporting Principles;
- Application to HHA;
- How Much is Enough?;
- Working Examples of HEMEA;
- Discussion.

4.4 Facilitation

The role of the facilitator is critical. First and foremost, the facilitator is required to guide the participants through the process, ensuring all are encouraged to contribute and the process proceeds at a pace balancing efficiency and effectiveness. They must be mindful of biases in the discussion and work to prevent these affecting the result.

The facilitator must also have detailed knowledge of human factors to offer help to the participants on the Performance Influencing Factors, the impact on error and to offer a human factors perspective on the task being considered. They are required to capture the discussions and conclusions in the HEMEA table (e.g. in a spreadsheet).

The facilitator should familiarise themselves with this guidance material, the specifics of the OEM and should ideally undertake the HeliOffshore training course on HHA. Where more than one facilitator is used, a session should be conducted in advance of the workshop to ensure consistency of approach.

4.5 Workshop Logistics

The host of the workshop should ensure the following is available:

- Meeting room/s of sufficient size;
- Good internet connectivity;
- Access to the maintenance manuals of the aircraft under review;
- A Projector to allow the maintenance task to be projected for all participants.

4.6 Workshop Process

In advance of the workshop, the OEM selects the maintenance tasks for analysis and collects fundamental information regarding the critical component and maintenance task (Steps 1 and 2 of Figure 1) to identify the focus of the analysis.

At the start of the first day of the workshop, following introductions, the facilitator sets the scene and outlines the ground rules. The detailed briefing and subsequent discussion ensures there is a common understanding before the analysis starts.

The analysis follows a set pattern. For each identified maintenance task:

- The facilitator will ask one of the participants to read the maintenance task instruction as if they were undertaking the task;
- All steps in the task, and all relevant figures should be reviewed;
- All participants reflect on their experience of the task, share any gaps or errors previously identified and discuss if any further issues can be identified by following the Steps of the HHA process.

Section 5 Conclusion

Section 5
Conclusion

This standardised process has been developed by an extraordinary collaboration in the helicopter industry. Major manufacturers have worked together and shared their best practice methods; design engineers, maintenance engineers and human factors specialists have exchanged their experiences and knowledge, and the initiative is driven and co-ordinated by an industry body in which all stakeholders have contributed, including the energy companies who have assisted with funding.

The resulting actions taken in the design and documentation are fed back to the maintenance engineers who provided their expertise, and this completes the loop.

Collaboration across boundaries is the way forward for safety, and HeliOffshore would like to thank everyone who has contributed to the delivery of this project.

Section 6 References

Section 6
References

ARMS Working Group (2010) The ARMS Methodology for Operational Risk Assessment in Aviation Organisations, www.Skybrary.com

COURTENEY, H. (2001) Human Centred Design for Maintenance, 15th Symposium Human Factors in Aviation Maintenance

EUROPEAN AVIATION SAFETY AGENCY (2020) COMMISSION DELEGATED REGULATION (EU) 2020/2034

GILL, S. (2009) Addressing Maintenance Human Factors During Aircraft Design, PhD Thesis, Nottingham University

GRAEBER R. & MARX D. (1993) Reduced Human Error in Aircraft Maintenance Operations, Flight Safety Foundation 46th Annual International Air Safety Seminar, Malaysia

HALL P. (2003) Monarch MEDA Experience, Maintenance Error Management Systems Conference, CAA Gatwick

HOLLNAGEL E. (2018), Safety-II in Practice. Developing the Resilience Potentials, Routledge, Taylor & Francis Group, New York

RANKIN W. & SOGG S. (2003) Update on the Maintenance Error Decision Aid (MEDA) Process, UK CAA MEDA/MEMS Workshop and Seminar

SKINNER M. (2003) CHIRP-MEMS Maintenance Error Data Sharing Project, Maintenance Error Management Systems Conference, CAA Gatwick

SHAPPELL S. & WIEGMANN, D. (2006) Developing A Methodology For Assessing Safety Programs Targeting Human Error In Aviation, Federal Aviation Administration

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (1996) Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Aerospace Recommended Practice 4761

UK CAA (2016) CAP 1367 Aircraft Maintenance Incident Analysis, CAA Gatwick

Section 7 Appendix A – Guidance on Performance Influencing Factor Ratings

Section 7
Appendix A – Guidance on Performance Influencing Factor Ratings

	0	1	2	3	4	5
Accessibility	n/a	Accessibility is good, negligible risk to initiate an incorrect maintenance action.	Accessibility is acceptable, minimal risk of it inducing an incorrect maintenance action.	Accessibility is poor, some risk of it inducing an incorrect maintenance action.	Accessibility is very poor, significant risk of it inducing an incorrect maintenance action.	Accessibility is extremely poor, it is very likely to induce an incorrect maintenance action.
Perceived Task Frequency	n/a	Frequency is very low, negligible risk to initiate an incorrect maintenance action.	Frequency is low, minimal risk of it inducing an incorrect maintenance action.	Frequency is high, some risk of it inducing an incorrect maintenance action.	Frequency is very high, significant risk of it inducing an incorrect maintenance action.	Frequency is extremely high, it is very likely to induce an incorrect maintenance action.
Demand on Resource	n/a	Negligible demand on resources (e.g. one person, 10 minutes), negligible risk to initiate an incorrect maintenance action.	Minimal demand on resources (e.g. one person, 2 hours), minimal risk of it inducing an incorrect maintenance action.	High demand on resources (e.g. two people, 5 hours), some risk of it inducing an incorrect maintenance action.	Very high demand on resources (e.g. two people, 15 hours), significant risk of it inducing an incorrect maintenance action.	Extremely high demand on resources (e.g. two people, 25 hours), it is very likely to induce an incorrect maintenance action.
Documentation	n/a	Documentation is good, negligible risk to initiate an incorrect maintenance action. **For inspection tasks, pass/fail criteria is very clear and objective.**	Documentation is acceptable, minimal risk of it inducing an incorrect maintenance action. **For inspection tasks, pass/fail criteria is quite clear.**	Documentation is poor, some risk of it inducing an incorrect maintenance action. **For inspection tasks, pass/fail criteria is not particularly clear.**	Documentation is very poor, significant risk of it inducing an incorrect maintenance action. **For inspection tasks, pass/fail criteria is not clear.**	Documentation is extremely poor, it is very likely to induce an incorrect maintenance action. **For inspection tasks, pass/fail criteria is very unclear/subjective.**
Special Tooling	n/a	No special tooling required, no risk to initiate an incorrect maintenance action.	Minimal special tooling required, minimal risk of it inducing an incorrect maintenance action.	Some special tooling required, some risk of it inducing an incorrect maintenance action.	Much special tooling required, significant risk of it inducing an incorrect maintenance action.	Too special tooling required, it is very likely to induce an incorrect maintenance action.
Susceptibility to Damage	n/a	Not susceptible to damage.	Minimal chance of damage to component.	Some chance of damage to component.	High chance of damage to component.	Very high chance of damage to component.

HHA specialists are encouraged to participate in our online, secure collaboration tool: HeliOffshore Space.

You can find out more about HeliOffshore, our safety plan, and the workstreams at
www.helioffshore.org

HeliOffshore
Safety Through Collaboration

This guidance will be updated regularly. If you have comments or suggested amendments, please email: **hha@helioffshore.org**