

Human Centred Design for Maintenance

Hazel Courteney

Introduction

Civil aviation is safe but needs to be safer

Civil aviation currently enjoys a very high level of safety. However, due to increasing air traffic the standard needs to be further improved to avoid rising numbers of accidents. The much quoted Pareto Effect tells us that usually we will receive 80% of the benefit from the first 20% of the effort. This means that once a high level of safety has been reached, any further gains will cost relatively more effort. That is our situation today, so our target improvements need to be selected with care.

Human Error is the Leading Risk

It is already accepted that human error is the leading cause of aviation accidents [e.g. CAP 681 study of fatal accidents to large aircraft world-wide]. In fact, almost any risk could be traced back to human error if decisions in design, training, production, communications or weather forecasting and were to be included as 'errors'. The CAP 681 specifically identifies Maintenance Error as a contributory causal factor in 28 fatal accidents and in 10 of those it was the primary cause. The role of errors in maintenance has attracted increasing attention in recent years. It is difficult to obtain a comprehensive picture of risk trends world-wide but UK CAA statistics indicate a continuing rise in the number of reportable maintenance errors per million flights [see Fig. 1]. Such a rise will be compounded by increasing traffic to make absolute numbers of errors show an accelerating trend.

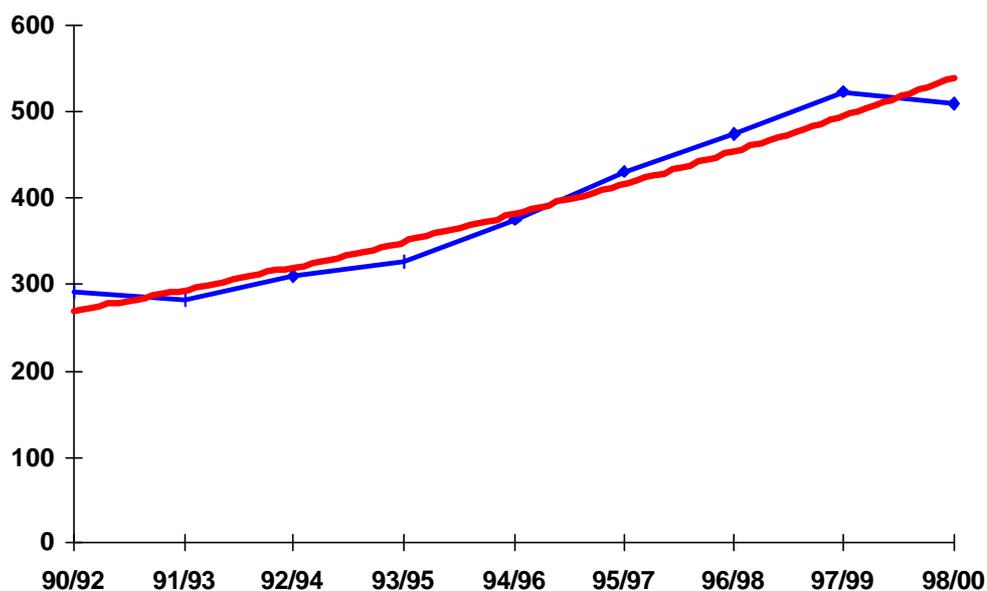


Fig. 1: Maintenance Error MORs to UK Registered Public Transport Aeroplanes >5700kg mtwa per Million Flights [shown as 3 year moving average]

Aircraft Design affects Likelihood and Consequences of Error

There is increasing awareness that the design of an aircraft affects its vulnerability to error during maintenance. The design will influence how easy it is to do the task, the likelihood that an error will occur, and the opportunities to detect the error and recover the situation before the aircraft returns to service. The design may also determine whether the error can be identified by the pilots before or during flight, and the final effect that it will have on flight safety. The opportunity for the regulatory authority to assess these aspects of the aircraft is during Type Certification [TC] of the basic design.

Documentation is Important

Maintenance manuals may also be viewed as an element of the 'aircraft' package. An aircraft design may be elegant but if the manual does not successfully communicate the task to the engineer, then the elegance is wasted and the 'total' design is poor. Documentation that is unclear leaves the aircraft vulnerable to maintenance error and reduces flight safety. Validation of a maintenance task should be conducted with representative maintenance engineers using the instructions as they would realistically be presented, including the realistic degree of cross referencing to other pages or sources, and translation to other languages where appropriate. This aspect may be missed in processes that evaluate the task using designers themselves, engineers who have received personal tuition or 'mannequins' computer simulations.

Whole Aircraft, not just Flight Deck

'Human Centred Design' refers to the practice of designing the machine to best suit the needs of the human user. The human in question might be the pilot, the cabin crew, maintenance engineer, production staff, ground crew, or anyone else who interacts with the aeroplane or its components. Historically, most of the discussion on these 'human centred' aspects of design have focused on the flight deck interface with the pilot. More recently, the maintenance engineer has begun to receive similar consideration as the potential importance of errors in maintenance are recognised. 'Design for Maintenance' across the whole aircraft is now recognised as a key area of Human Centred Design. 'Error resistance' is one of several considerations in a Human Centred approach.

What is Good 'Design for Maintenance'?

What Constitutes a 'Good' Design for Maintenance?

'Design for maintenance' as a concept is neither new nor mysterious. It embraces a range of characteristics, including tasks being error resistant, easy, quick and safe to do, visible and accessible, with space to manoeuvre for the full range of engineers physical sizes using the appropriate tools, a minimal training requirement, and appropriate supporting material.

Communication

The first priority in design for maintenance should be how the task is communicated to the engineer. This begins with understanding the training baseline that all qualified engineers would have and building from there through effective manuals, clear instructions and convenient data retrieval facilities. The tasks themselves have to be feasible, the procedures applicable and the data correct. Where problems are identified in service, the communication from the engineer to the manufacturer also

needs to be effective, so that information is corrected and redistributed in a reasonable timescale. These points may sound like obvious common sense, but consider whether they are always achieved by established aircraft manufacturers.

General Usability

Some manufacturers already have design guidelines to promote good practice. This directs design engineers to ensure that their design can be seen, reached and worked on in an appropriate way. 'Appropriate' will include sufficient clearance to turn a spanner without colliding with other components, to conduct manual manipulation without getting the hand stuck or skinning knuckles, on a part that can be seen without the necessity for the maintenance engineer to hold a torch with their third hand and have their head share a spatial position with an item of metal structure. There may be a policy to identify the most important tasks and ensure that particular guidelines are met for these, if not every maintenance task. Such priorities may also dictate which tasks [and associated data] are validated, which must be conducted independently, and which parts may not be disturbed to access others. If a safety critical part is repeatedly removed to allow routine maintenance on another item, then the risks of error in re-assembly, contamination or damage to that component rise considerably. Some of these concerns may be identified through the manufacturers Zonal Safety Analysis if it is done well.

Error Resistant Design

There may also be error resistant design features. This would ideally include 'designing out' safety critical tasks. It may also be supported by parts that are physically impossible to assemble or install incorrectly, cross connection prevented by different part numbers, staggered position of similar parts or by leads that are too short to stretch to the wrong fastener. Some designs remove the need for inspections, or other tasks, that may risk damaging delicate parts. Small apertures that invite tools to drop through may be avoided or at least a means provided to rescue stray items. Paint finish may be controlled due to the increased likelihood of flaw detection on shiny [rather than matt] surface finish, and certain colours may be favoured, or restricted to plain monochrome rather than patterned, to aid inspection reliability. Other simple devices to promote error resistance in design can include items in close proximity distinguished by colour coding or shaped switch tops, standardisation of display formats and direction of operation [always 'clockwise' to increase quantity] switches or dials that form a visual pattern when they are all in the correct position, convenient access panels, lids attached to chains [making it obvious that they have not been replaced], switches that lock, are physically separated or carefully positioned to avoid inadvertent operation, guarding of moving parts, even placards to some extent [although

MOR extract: "Loud bang & rapid depressurisation. P1 and cabin crew member lost consciousness. Emergency descent. Five injuries.

Cargo door cracked.....Evidence from the contamination of the cracks and the a/c records indicated that the cracks had been in existence some 17 years and not noticed during the embodiment of FAA AD 76-26-02 in Sept81 at 12000 flight cycles and 25000 hrs and the particularly relevant CAA AAD B737 001-06-89 'Frame and Beam Inspection Modification and Repair in Nov97 at 34460 flight cycles and 84772 hrs."

the use of placards should not proliferate as a 'sticking plaster' solution to all risks].

Use of these Principles is Variable

Manufacturers, even individual designers, may vary tremendously in their use of such design principles. There is no regulatory requirement to do so. This variation arises from at least three sources:

- the extent of their understanding of HCD principles
- level of confidence relative to task criticality
- competition from other priorities, such as cost, time, weight and space

These will be briefly discussed in turn.

Understanding of HCD

Design engineers are not a homogenous group in terms of their views on error resistance in design. Some regard the aircraft design as a self contained item that cannot be held responsible for the actions - or errors - of a human maintenance engineer. Those individuals feel that if the part they are designing meets the technical specification, and the published maintenance procedure is correct, then their task is done. They may feel no obligation to take preventative measures to deal with possible errors that could be made, or to accommodate the end users as they actually are [i.e. human] and not how the designer would like them to be [i.e. errorless]. In the case of manuals and procedures, they may believe that if the information they have written is clear to them as they have expressed it, then it must also be clear to someone else seeing the design for the first time. If not then it is that persons fault for not understanding. They may believe that provided that each element of information is factually true, their job is successfully completed. They may not feel it is their responsibility to ensure that information is presented in a way that is not only 'true' but is actually intelligible and convenient for the people who will use it. Such an approach would directly contravene the principles of HCD and Design for Maintenance. Manuals exist to communicate effectively to practising engineers and if they do not achieve that, they have failed.

Confidence Relative to Task Criticality

HCD and error resistant features improve the likelihood of good performance, but - depending on the mechanism chosen - cannot always guarantee it. Colour coding can be ignored, tasks performed incorrectly in even the best environments, parts that do not fit forced in to position regardless. For example, plates can be designed with one drill hole smaller than the rest to match a single smaller protrusion. This will 'ensure' that it can only be fitted in the correct orientation. Unfortunately, it has been known for the engineers to assume that the hole has been drilled under-size in error and conscientiously re-drill it to match the rest, before fitting the plate backwards. If the safety assessment cannot entirely rely upon the HCD method to avoid the risk, and other measures are needed anyway, some will question the benefit of doing it at all.

Competition from other Priorities

Within any design, there will be items where it is easy to introduce an error resistant feature with little or no penalty, and others where it is not. This may result in an implementation that does include some beneficial features but the policy is inconsistent and unrelated to safety priority. This leaves the possibility of high risk items being unprotected. It can also be unwise because the existence of some safety features may

lead engineers to a ‘false sense of security’ assuming that the same protection will be uniform across the whole aircraft and that anything that can be fitted must be right.

The Regulators Role

Good Practice Vs Minimum Standards

The CAA exists to set and enforce minimum baseline standards for aviation safety without creating an unduly restrictive environment or burden upon the industry. This means that the regulators role is confined in two important ways:

- Safety: the issue must be safety related
- Minimum Standards: the standard imposed must be the minimum acceptable, not the best theoretically achievable.

Safety Related Issues:

So far we have discussed some principles that may contribute to ‘good design for maintenance’ and in particular, resistance to error. These are all worthwhile goals. Clearly there are benefits to a design that offers minimal training burden, quick turnarounds and easy, convenient tasks that don’t result in dirty clothes or aching backs. However, whilst it may be universally acknowledged to be ‘a good thing’ this is not necessarily the business of the regulator. If manufacturers and operators are willing to tolerate a higher level of training and maintenance schedule time in order to buy aeroplanes at a lower price, that should not be prohibited unless it is unsafe. If errors can occur but the result only affects cost, rework or delay, then that is not a safety issue. Whilst good practice is acknowledged, the regulators focus remains on those elements of HCD that affect flight safety.

Defining a Minimum Standard for HCD

If the only criteria for aircraft design were optimised error resistance, then every part would be designed with additional features to achieve this, no two parts would be identical to avoid wrong fitting, every system operation would carry ‘are you sure?’ reminders, and the whole aircraft would be colour coded and jobs all inspected in triplicate. Of course, that can never happen. Aircraft also have to be affordable, parts have to fit into a certain space, tasks have to be conducted with limited resources of time and staff levels, operators push for parts standardisation. The simple advice to make aircraft design error tolerant is not very useful, because for any given part there will usually be a trade-off with other priorities such as cost, effort, weight, size, or task time. What is necessary is a clear definition of how we should decide which items *must* have error tolerant features, and for which it is optional.

Error Resistance is the Main Concern

The main safety related issue in HCD is the inherent error resistance of the design. Having said that, the easier maintenance tasks are to do, the less they are likely to incur error in the first place. Therefore there may be two parts to effective future regulation of design. The first task would be to effectively define a minimum acceptable level of error resistance. This could then form part of the design requirements for the aircraft. To support this it would be necessary to identify some methods that the manufacturer could use in order to achieve that goal, and to demonstrate that they have achieved it. These could be in the form of analytical techniques and form part of the compliance documentation for the Type Certificate. The development of such techniques will be discussed later. The second might be the requirement for a documented Design for

Maintenance Policy, that would identify the manufacturers selected principles [such as those outlined above] and their policy toward validation of maintenance tasks, ‘user testing’ of the instruction manuals, organisational methods for assuring documented procedures, and mechanisms for receiving and correcting incorrect data discovered in service.

MOR extract: “Nr2 engine contaminated by FOD (screwdriver).

Screwdriver found resting against leading edge of outlet guide vanes in 6 o'clock position behind fan blades. Screwdriver removed & engine inspected for damage but none found. Reporter confirms that a/c had flown one sector since recent overnight stop & RC1 check at foreign facility.”

Regulatory Action to Date

Regulatory action takes time. This can be frustrating but it is essential that all avenues are investigated, effects assessed, and relevant parties consulted. Before words become embedded as binding requirements, it is important to be sure that they are right, and the effects will be beneficial. There is already substantial efforts taking place on regulatory material for HCD aspects of the flight deck, as operated by the pilots. Design for Maintenance has received less attention to date, but that may soon change. UK CAA has already recognised the issues identified above and some proposed regulatory material forwarded to JAA Central as proposed new requirements. This material is designated JAA P-NPA 25.310 and it has had some preliminary circulation for comment. The proposal requires for example that:

“It must be shown by analysis, substantiated where necessary by test, that as far as reasonably practicable all design precautions have been taken to prevent human errors in production, maintenance and operation causing Hazardous or Catastrophic effect. Where the potential cannot realistically be eliminated, then the remaining safety critical tasks should be sufficiently understood and the potential for human error mitigated.”

Where industry resistance has been encountered, the main objection has been that compliance techniques are not readily available. Although there are various published approaches to the assessment of human error in the system, none appears directly suitable to the issues as they arise for aircraft certification in consideration of human error or design for maintenance in general.

Means of Compliance

Seeking a Mature Means of Compliance

A fully mature means of compliance has not yet been identified. It seems likely that it would involve systematic analysis of the design to identify the potential safety risks from maintenance error and show how they have been addressed. It might also include a manufacturers ‘Design for Maintenance’ manual with ‘good practice’ guidance. However, the existence of guidance may not provide adequate assurance of acceptable safety in all cases. Therefore a suitable method of analysis is currently being researched by UK CAA.

Existing HF Analysis Methods

Of course, there are already 'off the shelf' analysis techniques that are offered as potentially suitable for the purpose. Human Reliability Analysis [HRA], Hazard and Operability assessment [HAZOP], and others have been evaluated and considered. Many such methods have some merit, but none of these has been found entirely adequate for this specialised purpose.

HF Analysis Integrated with Engineering Methods

The CAA approach endeavours to integrate Human Factors considerations with current practice in engineering and design. At present designers conducting the System Safety Assessment [SSA] use techniques such as fault trees and Failure Modes and Effects Analysis [FMEA] to determine whether the design is acceptable in terms of safety and reliability. For technical components, the more severe the consequences of a failure, the more reliable it must be. If it cannot be made more reliable then the system must be revised to reduce the adverse consequences of a failure occurring. Depending on the task, it may not be possible to make the human 'component' more reliable. Training will not eradicate all routine errors in human performance. New techniques to incorporate human error into the evaluation build upon these existing methods, extending them to encompass risk from human error as well as technical failure. This is preferred to creating a completely separate parallel activity that the design would then have to accommodate in addition to technical concerns.

Methods Developed by CAA

The UK CAA has begun to develop procedures for augmentation of traditional engineering fault trees to include potential maintenance error alongside technical failure risks [see example produced for CAA by Ray Cherry Associates, Appendix 1 Section A1]. Once the potential errors that may impact safety are identified in the Fault Tree, then the relevant tasks in which those errors could occur would be subjected to a Human Hazard Analysis [HHA]. This method was first published to address direct operational tasks [Courteney, 1997, 1998, 1999] and was subsequently developed for application to maintenance tasks [Doherty, 1999] see adapted example, Appendix 1 Section A2. It is based upon the qualitative FMEA approach but assesses the result of a human error instead of a technical failure. Opportunities [both for maintenance engineers and pilots] to detect and recover from the error are considered, as are the potential hazard level of the consequences, both directly and through dormancy. For example, cross connected fire bottles have little immediate effect but in the event of an engine fire the result may be more serious. Having systematically considered the effects of the error should it occur, the selected means of mitigation is identified. This may range from design change, training / procedures or nothing at all, depending upon the result of the assessment. However, it is made clear that design change is usually preferred and that, in the case of risks from routine slips and lapses that training people is not acceptable as a claimed means to eradicate error. This method specifically aims to distinguish between items that must incorporate error resistant features for safety reasons, and those that can be tolerated without such features at the discretion of the manufacturer. It is intended that the analysis would form part of the aircraft documentation to demonstrate compliance with the requirements.

Which Errors are 'Foreseeable'?

Development of these techniques is more difficult than it might first appear, because defining exactly what human errors are 'foreseeable' by skilled maintenance personnel is not a simple matter. It is clearly 'foreseeable' that even highly competent and experienced people can make errors in data entry or drop a spanner. However, it is not reasonable to require aircraft manufacturers to design aircraft such that professional maintenance engineers can act in an almost random fashion without due care, knowledge or skill. It would be almost impossible to design such a machine and anyway unnecessary with a highly trained, carefully licensed population. So where should we draw the line in deciding which errors the manufacturer must identify as 'foreseeable' and thus be required to make the design resistant to the error occurring?

Defining Foreseeable Errors

The approach thus far has been to explicitly identify specific kinds of error that the manufacturer should regard as foreseeable [e.g. crossed connections] and those that would be referred to as 'slips and lapses' in the literature [e.g. data entry errors], plus any that are known to have occurred in service previously. In order to make progress, this has been accepted although it is probably a conservative set. However, if at least these can be accommodated, then this will be a significant improvement without introducing an unnecessary burden to address large numbers of errors that might never happen. The 'set' as defined above is not adequately addressed in current design and so the requirement would make a step improvement to existing standards. It would also provide an opportunity to gain experience and improve safety with the least effort and expense by industry. However, it is hoped that in the future this definition of 'foreseeable error' can be expanded.

MOR extract: "Fuel imbalance. "Pan" declared. Diversion. Fuel gauges cross-connected. Maintenance error.

Re-balancing procedures & QRH actions had no effect. Subsequent investigation revealed that flight deck fuel quantity gauges were cross-connected behind instrument panel during recent work carried out on a wiper motor that required the instrument panel to be removed."

Using Numerical Probabilities

Before leaving this subject it is worthwhile to mention the use of numerical probabilities for human error. It would be massively convenient if the human errors in a fault tree could be assigned a realistic probability value like the other, technical components in the System Safety Assessment [SSA]. The safety levels could then be mathematically computed and the problem solved. Again, it is unfortunately not so simple. Realistic probability numbers for human error are notoriously difficult to obtain. The reason is that they are very sensitive to small changes in the design, the task procedure, in fact almost anything including time of day, temperature, lighting levels and noise. Such factors can change the error rates from clearly within to far outside the line of acceptability for certification.

Difficulty of Collecting Probability Data

It could be argued that the actual design proposed could be subjected to experimental trials, but to obtain sufficient hours to establish statistical rates of these [actually very rare] errors in sufficiently representative circumstances [i.e., embedded realistically in

the task, and in context] for every relevant feature would be a mammoth program. Worse, it would have to wait until the design [and prototype build] was complete, to begin the data collection necessary for the analysis, to decide whether each feature was acceptable or had to be changed. Some people have proposed the use of generic 'coarse band' numbers for human errors in safety assessments in order to at least gain an approximate understanding of the human error risk in the system. That is not such a bad thing to do, for overall SSA. It is certainly better than the philosophy by some system designers today that the risk from human error is assumed to be less than 10^{-9} [one in a billion flight hours!] and therefore can be discounted from the safety assessment.

Motivating Best Design for High Risk Items

From a certification point of view, generic probability bands are only part of a solution. Suppose human errors are always assigned a certain value, let's say 10^{-3} per flight hour. There is then nothing to motivate a manufacturer to improve the design surrounding any task, not even the most vulnerable designs where an error seems obviously likely. If the Type Certification team will always give the same credit [10^{-3}] to that error risk, then what has the manufacturer to gain by making it less likely by a better design? Further, it does not allow a Certification Team to reject a design that carries a high risk of error in a vulnerable area if it meets the agreed SSA criteria with a 10^{-3} probability. This is then complicated by the introduction of equally approximate numbers for the reliability attributed to the detection of the error by the maintenance engineer, or the intervention of the pilot, and the cross checks provided by the other pilot. So, although it would be easy to be seduced by the numerical analyses, their contribution is at best incomplete. They need to be balanced by a motivation for best ergonomic design for highest risk items, as provided by the HHA.

Realistic Human Performance Levels in SSA

One possible way to use numerical probabilities may be to calculate, through the SSA, what the probability of a human error would have to be in order to meet the safety objective for its effect. So, if a technical failure were to be classified 'Major', it should not happen more often than 1×10^{-5} . If this were combined with a human error, [e.g., failed component, plus human does not detect the failure] then the result may be much more serious [e.g. it now has to survive take-off again], so the classification would have to be amended to accommodate this to, for example, 'Hazardous'. For a hazardous event the safety objective would be 1×10^{-7} , so that the 'implied' rate of human error to meet that target would be 1×10^{-2} . This could be seen as a realistic level of human performance. If however the 'implied' level of human performance would have to be 10^{-6} in order to meet the safety objective, that would be very optimistic. Parts where that was the case might be considered vulnerable to error and selected for improvement in terms of technical reliability and/or human factors aspects of design, in order to promote acceptable overall performance. These methods could be combined with the use of Fault Trees as described above to identify which maintenance tasks would need to be subjected to the full HHA treatment.

'Meta' Human Factors Issues

Assuring a Seamless System

Many problems that are labelled 'Human Factors Issues' arise from gaps or mismatches between different areas of the aviation system. In justifying a design as safe and workable designers may make assumptions about operational circumstance and practices that may not be a perfect match for reality. Where two areas of the overall aviation system do not match up in this way, there is a 'gap' between what designers expected and what is realistically provided operationally. When such a 'gap' arises, there is only one element of the overall industry system that is sufficiently adaptable, flexible and clever to stretch itself and compensate for the gap between areas. That element is the human engineer. When the engineer stretches to bridge the gap he may come under strain. We may refer to this as a 'meta' human factors issue: it arises not from the HF aspects of any individual element [ergonomics, good hangar conditions], but from the mismatch between elements. As the London Underground trains have said on the platform: 'Mind the Gap'!

Does the Training Assumed Match the Training Provided?

It could be that the demands of a design assume a certain depth of knowledge gained from a certain level of training. Yet that depth of training may not be provided for everyone who might do that task. The 'gap' between the expectations of the designer and the training by the operator will be covered by individual engineers being 'stretched'. They will 'stretch' by figuring it out, asking others, going in search of information. However, sometimes the stretch required is just too much, or they are overloaded by this stretching and make errors. These errors are called 'a human factors problem' because the engineer made an error, but they arise because of structural difficulties in the overall system, with gaps between different parts of the process.

Is the Time Allowed Realistic?

Another potential 'gap' might arise between the time allocated for a task and the time that it might realistically need, given contingencies that arise or problems that could be found. If the operation relies upon a faster turnaround time than can be comfortably achieved, the engineers will 'stretch' to achieve a solution. They may be proud of their 'can do' attitude and work innovatively to get the aircraft out on time. Unfortunately, their 'stretched' performance to bridge the gap between scheduled times and realistic times may encourage undetected errors.

Engineers May Assume 'Normal' Procedures

Designers may assume that if the instructions on a drawing or in a manual identify a certain technique to be used, then the engineer will read that and the prescribed method will be applied. However, it may be that if normal custom and practice is to do things a certain way. If this particular component is not obviously different from many others that are always treated in that conventional way, it may be unrealistic to assume that skilled experienced engineers will consult the instructions anew with every new job that arrives. Engineers may see a task that [they believe] belongs to a familiar category of tasks and proceed accordingly. Therefore in cases where a different technique is called up, it may be wise to assess the consequences of the traditional method being used. A good 'error resistant' system would provide clear flags to draw attention to items that depart from 'normal' procedures. A similar argument could apply to the inspection of parts where a small amount of surface damage would be acceptable on traditional constructions and might be [wrongly] assumed to be equally insignificant on modern materials. In this case a specific training requirement might be identified.

Adverse Field or Hangar Conditions

It would not be surprising if designers, located in light, clean and warm offices, did not give as much attention to real field conditions as engineers might like. They may consult JAR-145 and assume that during maintenance the activity will always be conducted within a narrow band of [relatively good] environmental conditions. This may not include consideration of manual strength or dexterity in biting cold; inspection of structures in shadowy illumination, scanning for damage on dust laden metallic or composite parts with multi-coloured paint patterns.

Quality of Documentation

There is ongoing discussion concerning the quality of maintenance documentation. There is a range of potential problems, from accuracy of information, clarity and feasibility of task descriptions, unworkable tasks that have not been validated, mechanisms to feed back incorrect data to manufacturers and [lack of] confidence in the likelihood and timescale of corrections. As with the other examples, if there is a gap between the quality of instructions needed and those actually supplied, it will be the engineer that has to stretch in order to bridge the gap - with varying degrees of success.

Modifications

Aircraft remain in service a long time and may incorporate many modifications over their lifetime. This can create a 'gap' between standards used for, e.g. the training notes for that Type and the actual standard found on the aircraft. Once again this must be bridged by the engineer. The best way to address this may be to create a mechanism that permanently links the design to the documentation and training such that a change in one necessarily causes a commensurate change in the other.

HF Characteristics of Maintenance Equipment

The equipment used by maintenance engineers is also beginning to receive attention in terms of usability, error tolerance and definition of training needs. This may take a little longer, but the principles are likely to be very similar to those applied to the aircraft. As with other areas, care must be taken that there is no 'gap' between the assumptions made by the design and the real context of use. There is little benefit to applying colour coding for good ergonomic reasons and easy use if we do not test licensed engineers for colour blindness - a common condition in male adults.

Supporting Activity

This topic is gaining attention from UK CAA design surveyors engaged in Type Certification, all of whom receive residential training in HF principles and some attend additional training specifically for Design for Maintenance. As described above new regulatory material has been proposed and supporting methods are being developed. This year, a research contract is being offered to encourage major constructors to bid for validation of these methods on full aircraft systems. Continued Airworthiness activity is ongoing to identify relevant issues from Mandatory Occurrence Reports [MORs] that may call for action on existing aircraft or improve our understanding of the issues. In addition, work in the flight deck area has begun to ask manufacturers to document any assumptions about maintenance that exceed normal baselines in an Operator Interface Document.

Conclusion

This paper has attempted to outline some of the UK CAA current thinking on Design for Maintenance. The Design approach fully recognises the value of error reporting and management but believes that the aircraft design can also make a strong contribution to reducing the vulnerability of aviation safety to errors during maintenance.

References

Courteney H.Y. & Earthy J.V. , 'Assessing System Safety To $10^{-\text{Joker}}$: Accounting for the Human Operator in Certification and Approval' Proceedings of the European Space Agency Conference 1997

Courteney, H.Y. 'Assessing System Design For Vulnerability To User Error', Proceedings of the Electronics Research Association Conference 1999

Courteney, H.Y., 'Project Requirements: The Silent Dictators' Proceeding of the Conference on Function Allocation, University of Galway 1998

Doherty, S. M., 'Development of a Human Hazard Analysis Method for Crossed Connection Incidents in Aircraft Maintenance.' Bournemouth University as an MSc Dissertation, 1999.

APPENDIX 1 EXAMPLES OF THE HUMAN HAZARD ANALYSIS METHOD

A1. FAULT TREE ANALYSIS

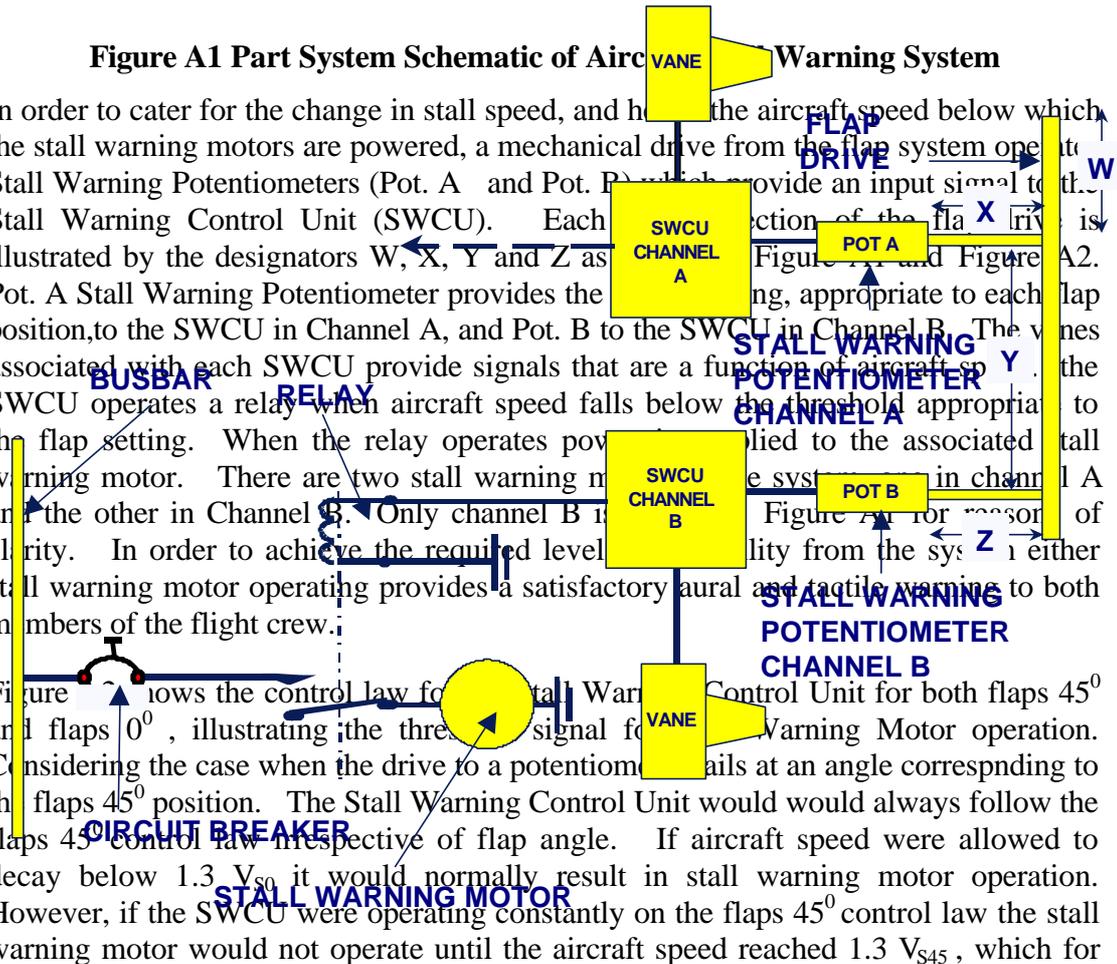
System Description

The sub-system shown in Figure A1 relates to that part of a stall warning system that provides the datum setting appropriate to each position of the trailing edge flap. The system does not relate to any particular aircraft but has been constructed to illustrate the proposed methodology.

Figure A1 Part System Schematic of Aircraft Stall Warning System

In order to cater for the change in stall speed, and hence the aircraft speed below which the stall warning motors are powered, a mechanical drive from the flap system operates two Stall Warning Potentiometers (Pot. A and Pot. B) which provide an input signal to the Stall Warning Control Unit (SWCU). Each channel of the flap drive is illustrated by the designators W, X, Y and Z as shown in Figure A1 and Figure A2. Pot. A Stall Warning Potentiometer provides the datum setting, appropriate to each flap position, to the SWCU in Channel A, and Pot. B to the SWCU in Channel B. The vanes associated with each SWCU provide signals that are a function of aircraft speed. The SWCU operates a relay when aircraft speed falls below the threshold appropriate to the flap setting. When the relay operates power is applied to the associated stall warning motor. There are two stall warning motors in the system, one in channel A and the other in Channel B. Only channel B is shown in Figure A1 for reasons of clarity. In order to achieve the required level of reliability from the system either stall warning motor operating provides a satisfactory aural and tactile warning to both members of the flight crew.

Figure A1 shows the control law for the Stall Warning Control Unit for both flaps 45° and flaps 0° , illustrating the threshold signal for Stall Warning Motor operation. Considering the case when the drive to a potentiometer fails at an angle corresponding to the flaps 45° position. The Stall Warning Control Unit would always follow the flaps 45° control law irrespective of flap angle. If aircraft speed were allowed to decay below $1.3 V_{S0}$ it would normally result in stall warning motor operation. However, if the SWCU were operating constantly on the flaps 45° control law the stall warning motor would not operate until the aircraft speed reached $1.3 V_{S45}$, which for the purposes of this exercise is assumed to be less than the stall speed at flaps 0° , V_{S0} .



THRESHOLD SIGNAL
FOR STALL
WARNING CONTROL
UNIT

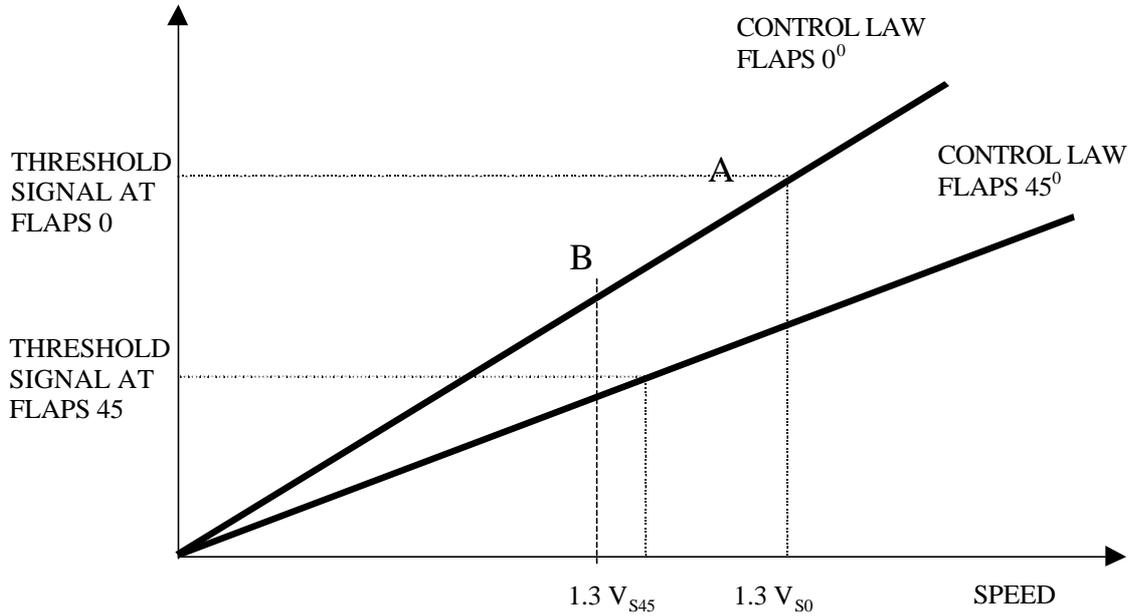


Figure A2 Graph Showing Relationship between Threshold Signal to Stall Warning Control Unit and Aircraft Speed

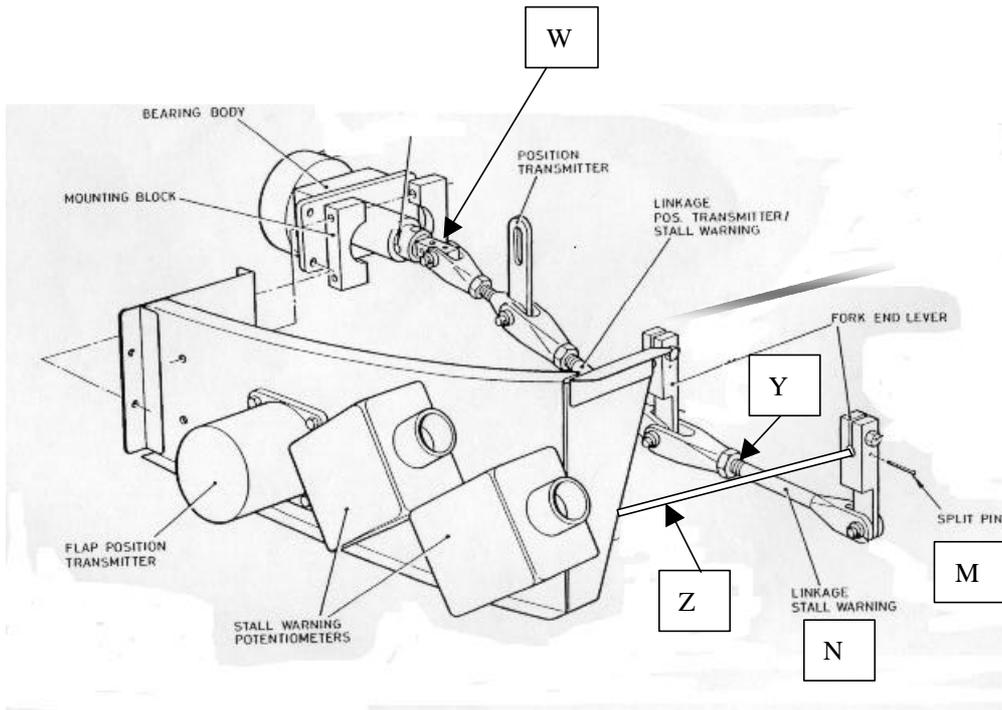


Figure A3 Mechanical Drive from Flap to Stall Warning Potentiometers

Explanation of The Fault Tree

The "Top Event" or undesirable System State considered in the Fault Tree is "Approach to the stall with no audible or tactile warning at Flaps 0". The symbology used in the Fault Tree is as defined in Table A1.



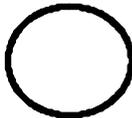
The rectangle identifies an event that results from the combination of fault or failure events through the input logic gate.



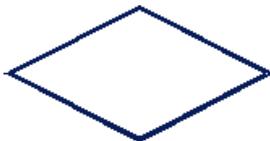
The 'OR' gate defines a situation whereby the output event will exist if one or more of the input events exist.



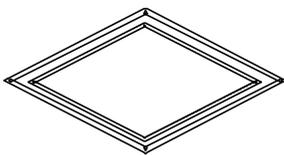
The 'AND' gate describes the logical operation whereby the coexistence of all input events is required to produce the output event.



The circle describes a primary failure event that requires no further development.



The diamond describes an event that is considered primary in a given fault tree. The possible causes of the event are not developed, because either the event is of insufficient consequence or the necessary information is unavailable.



The double diamond is similar to the normal diamond but is used to indicate a dormant or latent event.

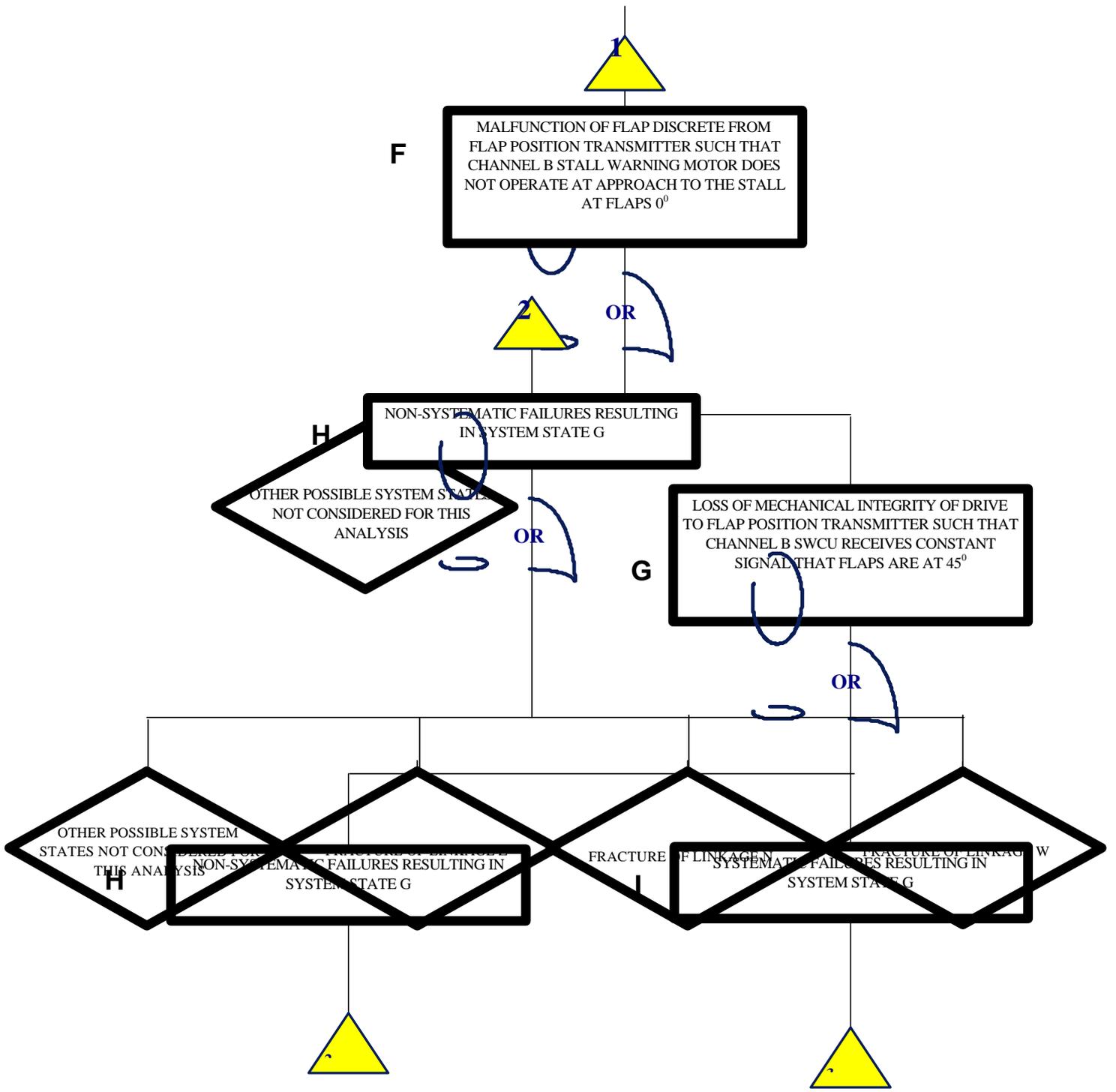


Triangles are used as transfer symbols. The inverted triangle is used where the sequence of events being transferred to another part of the fault tree is to have one or more different events in the second location but is to be identical in function. The upright triangle is used where the sequence of events being transferred to another part of the fault tree is to have all identical events in both locations.

Table A1 Fault Tree Symbology

The example Fault Tree is limited in the extent to which it has been developed. Its intention is simply to illustrate the manner in which Human Factors issues may be identified using this methodology.

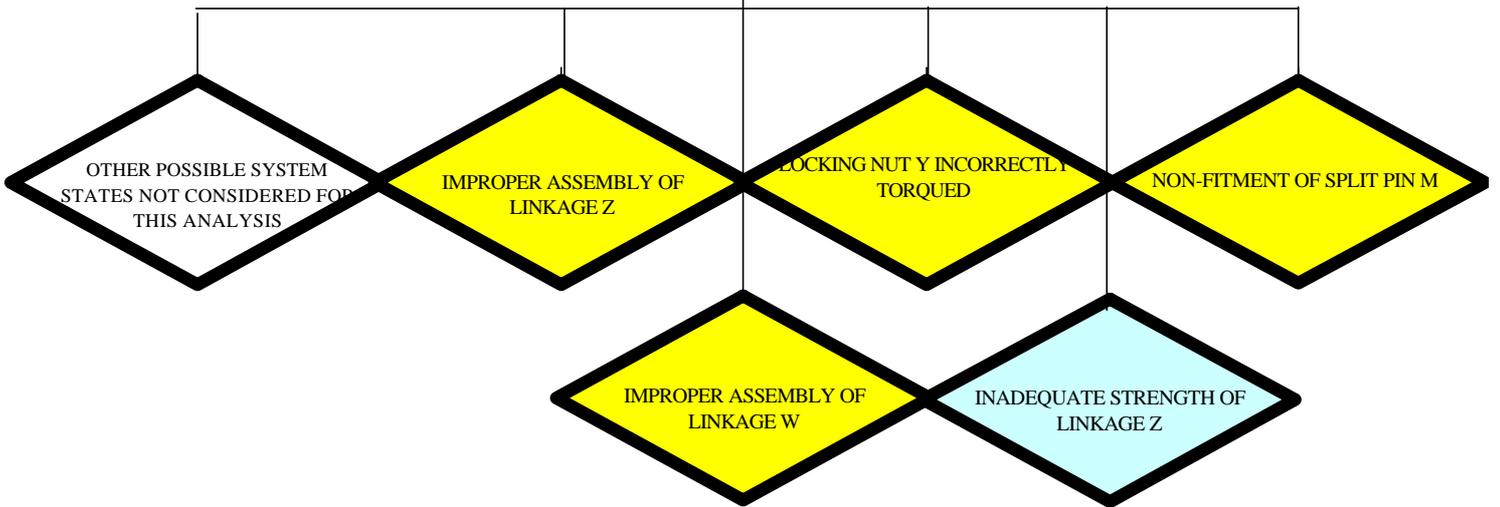
Of particular interest are the undeveloped events shown below transfer function 3. Those shaded yellow are maintenance or production faults and the "diamond" shaded blue is a design error. Of course if the Fault Tree were developed further many other faults would be identified that could possibly occur in production, maintenance or design. Whilst no examples are given in this particular fault tree Flight Deck Human Factors issues may also be identified. The Event Diamond "APPROACH TO THE STALL AT FLAPS 0°" could be developed further to identify possible problem areas. It should be noted that all of the failures below Transfer Function 3 are dormant. Hence they are of particular concern since they do not become evident until the aircraft approaches the stall or have been identified by a suitable maintenance or production inspection. Furthermore, the dormant failures of the flap drive system in that part of the system annotated W will affect both stall channels and hence could result in total loss of the stall warning system at flaps 0°. Therefore, particular attention should be directed toward this area.





SYSTEMATIC FAILURES RESULTING IN SYSTEM STATE G

Figure A4: Fault Tree Analysis from Errors in Maintenance, Design and Production. The yellow elements relate to possible maintenance errors and are used to select the maintenance tasks that would be subjected to the 'FMEA' part of the HHA [see Appendix 2]. For example, tasks may include 'Assemble Linkage Z', or 'Lock Nut Y to Correct Torque' or 'Fit Split Pin'. Other items such as 'Inadequate Strength of Linkage Z' may relate instead to vulnerability to human error in other areas such as Design activity. This would suggest that items such as 'Strength of linkage Z' identified in this way should receive particular attention during design checks and / or production processes.



A2: Example of FMEA Based HHA Conducted on Selected Tasks

| Maintenance task | Design Vulnerability | Possible wrong action | FT required? | Indication to maintenance crew if FT not performed? | Indication to flight crew before flight? | Subsequent indication to flight crew? | Immediate or direct consequence | Latent consequence (with second failure) | Comments | Mitigation required |
|---|--|--|--------------|---|---|---|---------------------------------|--|---|--|
| 1. Install fuel gauges | Same part numbers on gauges and connectors | Cross connect wing tank gauges | Yes | None | None | None unless fuel transfer required | MINOR | CATASTROPHIC When combined with fuel pump failure, it could lead to fuel transfer from the empty tank to the full tank, resulting in fuel imbalance and loss of control | No obvious visual clues unless wing tank fuel contents are considerably different | Physically different parts for the connectors and gauges Tagging system |
| | Same part numbers on gauges and connectors | Cross connect wing tank gauge with central tank gauge | Yes | None | Strange readings on fuel tank gauges in cockpit | More apparent if fuel transfer required | MINOR | CATASTROPHIC When combined with fuel pump failure, it could lead to fuel transfer from the empty tank to the full tank, resulting in fuel imbalance and loss of control | No obvious visual clues unless wing tank fuel contents are considerably different | Physically different parts for the connectors and gauges Tagging system |
| 2. Install PRSOV / fan air modulating valve | Pipe unions same part numbers CMM figure misleading - not in agreement with text | Cross connect PRSOV / FAMV pneumatic pipe unions | Yes | Pipes can be seen visually crossed | EICAS warning or message | Pneumatic duct pressure excessive at take-off power | MINOR | MAJOR Pneumatic system problems could result in high cockpit workload in the event of a second failure | Pipes found twisted inside pylon | Different unions Improve CMM figures |
| 3. Install navigation system | Same part numbers for cable connectors | Cross connect co-axial cables for VHF comms and VOR navigation | Yes | None | None | Poor range on VHF comms and intermittent VOR signal | MINOR | MAJOR In the event of failure of the secondary VOR or VHF comms system | Located on same rack | Physically different parts |

Fig. A5. HHA Applied to selected maintenance tasks on the B737 aircraft. Adapted from Doherty (1999).