Designing out human error


Airbus Helicopters

DR HAZEL COURTENEY, DR SIMON GILL and **SCOTT CARMICHAEL*** explain how rotary-wing safety group HeliOffshore is exploring a new approach to identifying potential human error in maintenance.

HeliOffshore, the global safety-focused organisation for the offshore helicopter industry, is exploring a fresh approach to reducing safety risk from aircraft maintenance. Recent trials with Airbus Helicopters and HeliOne show that this new direction has promise. The approach is based on an analysis of the aircraft design to identify where 'error proofing' features or other mitigations are most needed to support the maintenance engineer during critical maintenance tasks. It is based on the engineering tools used to assure adequate technical reliability during the design phase of an aircraft, adapted and combined with established thinking around human factors in maintenance, to enable a design analysis which systematically considers human performance. The objective is to enable the aircraft designers to better support the human maintainers in the field, by realistic consideration of human performance reliability.

Against the backdrop of a depressed oil price and increased financial pressure on the sector, it is vital that maintenance standards are upheld and are not allowed to slip for budgetary reasons. Therefore, the need for a new approach is even more pertinent.

Maintenance error is not an unsolvable problem

Human error in aircraft maintenance has long been a hot topic. The industry has good, well-trained people, improved hangar 'human factors' and has reduced the number of maintenance errors to a low level. Yet, it is impossible to stop people from making mistakes occasionally and, depending on the nature of the error, this can result in an accident. However, for fatal accidents, 'rare' is still not rare enough. The goal is such an extraordinary level of safety with high volumes of flights that even extremely infrequent errors can create a risk if they affect safety critical functions.

Above: Airbus H175 helicopter.

* Scott Carmichael is a project manager overseeing HeliOffshore's System Reliability & Resilence workstream. He works closely with aviation human factors experts Dr Hazel Courteney and Dr Simon Gill.

Helicopters, in particular, have more systems that are critical to flight with more critical components to maintain and so there are more opportunities for error to result in a catastrophic situation. Helicopters have a higher rate of accidents than fixed-wing and the proportion caused by technical factors is higher.

So what can be done? One possibility is to design the aircraft systems to be error tolerant, impossible to mis-assemble, or with back-up mechanisms in case it should happen. Design is uniquely capable of fully preventing error and is unaffected by operational pressures. To what extent can aircraft designers be expected to anticipate errors or incorrect actions by professional engineers and crucially, how will they – the designers – know when they've done 'enough'?

Learning lessons from engineering

A good place to start could be to revisit how we assure technical reliability for an airworthy aircraft. We have developed comprehensive processes that allow this to be managed safely, such as the (CS25.1309) system safety analysis (SSA). This includes a high level top-down functional hazard analysis (FHA), then fault trees to identify which elements of the system are the safety critical parts.

These safety critical parts are subjected to a bottom-up failure modes and effects analysis (FMEA), a tabular format to systematically assess how the safety critical parts might fail, what the safety consequences could be, how and when that would be detected, and what (if anything) is required to mitigate this failure to achieve a target safety level.

The components that impact safety have a required reliability commensurate with their criticality and, if they do fail, the failure must be adequately mitigated with design features such as quadruplex systems, back-up modes or independent sources of key functionality. In some circumstances actions beyond the design, such as specific training, warnings or duplicate inspection requirements, are also used as mitigations. We know that components fail occasionally, so we account for that in the design and the type certification requirements ensure that this is achieved to a safe level. This recognition of realistic technical reliability and systematic management of failure potential has been very successful in achieving high standards of airworthiness and safety of the design of the aircraft.

The total system

In a total systems approach, the 'system' that achieves a function includes both machine and human elements. Both are reliable but can sometimes fail in service. For the human element a robust approach to design analysis is missing.

In assessment of the system, the human action is assumed to be fully reliable, although data on human performance (and accidents) clearly indicates that this is not the case. Limitations of human performance have been part of basic license training for maintenance engineers for over 20 years now, reflecting the fact that some errors are part of normal human performance.

> HELICOPTERS, IN PARTICULAR, HAVE MORE SYSTEMS THAT ARE CRITICAL TO FLIGHT WITH MORE CRITICAL COMPONENTS TO MAINTAIN, AND SO THERE ARE MORE OPPORTUNITIES FOR ERROR TO RESULT IN A CATASTROPHIC SITUATION

If the human action in the system is automated, it will then be considered within the system safety analysis (SSA) and, according to its level of safety criticality, it will be assigned a reliability requirement such as 10^{-7}. This is a lower reliability level than the assumed 100% reliable performance of the human operator, suggesting that automation reduces reliability, which we know is not the case. We also know that the reliability of the human action is unlikely to be as high as 10^{-7}.

Air Transport Association, maintenance steering group logic 3, Volume 2

The Air Transport Association (ATA) Maintenance Steering Group (MSG3) Volume 2, covering the development of maintenance programmes for rotorcraft, was approved by the European Aviation Safety Agency (EASA), Transport Canada Civil Aviation (TCCA) and Federal Aviation Administration (FAA) in 2015.

MSG3 has been used in fixed-wing aircraft design for many years and is a standardised process used to identify and schedule initial maintenance tasks, through analysis of failure mode and effects of aircraft design.

Great advances have been achieved using the methodology in fixed-wing (and can also be in rotorcraft if the manufacturers adopt it) but the process does not include a maintenance human performance consideration.

Airbus Helicopters

For example if, through the failure mode analysis, it is determined that to assure continuing airworthiness a maintenance task should take

Ronnie Robertson

A Bristow Helicopters Sikorsky S-92.

> THE CHALLENGE TO REDUCE HUMAN ERROR TO ABSOLUTE ZERO IS SIMPLY UNACHIEVABLE

place at a certain interval, there is no requirement in the MSG3 process to then analyse the proposed maintenance task versus the limitations and realities of human performance and known types of human errors.

This poses such questions as: does the frequency of the scheduled maintenance lend itself easily to be exposed to lapse type errors? Does the physical assembly of the component under the maintenance task support easy indication or prevention of incorrect assembly/installation?

We would propose that, by including the human performance analysis of key maintenance tasks and the associated design configurations in the MSG3 type approach, it would bring further safety enhancements to the industry and better support the maintenance professional in the field.

Practical design change

Design change sounds expensive but the changes can be relatively small. The figure below shows a design that was involved in an accident following a maintenance error where the bolt was not secured and dropped out; with an alternative concept for additional protective features.

The new design creates four locking features, where there were previously two. The two original locking features, a split pin and self-locking nut, meet the mechanical needs of systems securing the bolt in place and also meet the minimum certification standard of having two locking methods in the control system.

The ability of both the split pin and the nut to perform their safety function is entirely dependent on a human to correctly install them. On first consideration it would seem highly unlikely, maybe even fantasy, that a maintenance engineer could assemble these components incorrectly. However, the error of not installing the split pin and/or the nut, and failure of two experienced engineers to identify this, was the conclusion of the investigators report.

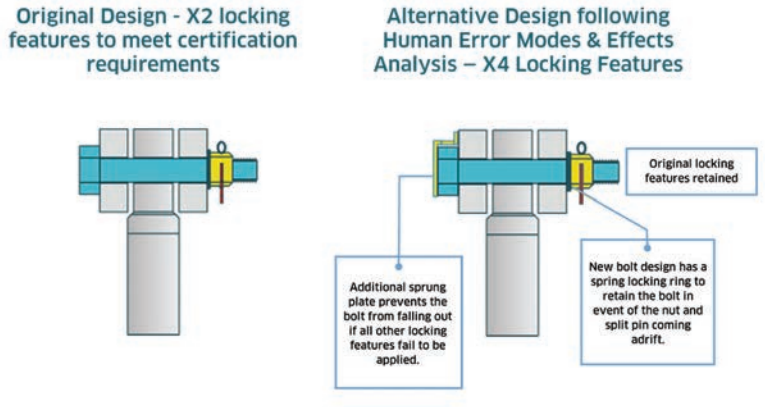
The main safety recommendation from the report was that better human factors training should be introduced. How much human factors training could ultimately prevent this error?

Instead we could consider, at the design stage, that this error could (and has) occurred and support the maintenance engineers and aircraft safety by including two additional safety design features.

The introduction of a locking ring on the bolt that prevents movement of the bolt if the split pin or nut fail (or are omitted) would prevent the aircraft having a catastrophic in-flight failure. The introduction of a retention plate over the head of the bolt would prevent the bolt moving if the split pin, nut and lock ring failed or were omitted during assembly.

The first two locking methods support the airworthiness of the system. The second two locking methods are introduced based on the knowledge of potential human performance errors, and protects the aircraft while supporting the maintenance engineers.

To achieve high aircraft utilisation and zero accidents, we either have to eradicate engineer errors completely, or accept that sometimes they may occur and prevent them from causing accidents. Maintenance engineer performance is generally highly reliable but the challenge to reduce human error to absolute zero is simply unachievable. Reacting after rare errors cause accidents means we have to wait until after the accident to fix it. We know better than that for technical failures; it's time to do better with human error, too.



Comparing the 'technical' and 'human' system design processes

Parts of the engineering assurance process have no direct parallel in assuring the human part of the system. It should be possible to tackle human error in maintenance by using similar methods to those used for technical reliability – a kind of human hazard analysis (HHA). The existing engineering process could help to determine the most safety critical maintenance tasks; then a process similar to the FMEA could assess whether an intervention was needed to reduce the risk. This could take each safety critical task and ask what maintenance errors are reasonably foreseeable, using expert judgement and human error data recorded by the maintenance error management systems (MEMS) from similar systems in common use. It could then assess the error for what the safety consequence would be, when/how it could be detected, what are the current protections, how well are they working and what additional protections – if any – are needed. In the table below, gaps for

additional activities on human functions are identified, where currently there is no equivalent to the technical assurance process.
Depending on the effect of the foreseeable errors

- Catastrophic – should be prevented by design, so that either the error could not occur, or it becomes less safety critical.
- Hazardous or major – prevented by design or mitigated by other methods,
- Minor – mitigated by low-cost actions or not at all.

This systematically determines which of the many components need an 'error protection' feature,

Functional Specification of system including all functions to be achieved	
Allocation of functions to technical/ machine or to human actions	
Process for technical functions of system	**Process for human functions of system**
Basic design	Basic operating procedures
Specification including required degree of resilience to uncontrolled factors outside system e.g. weather, temperature, birds, sand	No minimum requirements or specification for error tolerance of system design during production, maintenance or operations
Technical design of system	Recruitment & Training specification (may be incomplete e.r. engineer visual acuity standards)
Assess system for safety hazards from failures e.g. through FHA, fault trees, FMEA and SSA	System not assessed for safety hazards from foreseeable human errors
Assess spotential failures modes, likely effects and means of detection/recovery e.g. FMEA	Systematic consideration of likely error types and means of detection/ recovery not applied
Mitigate weak points that do not meet requirements e.g. 1309	Issues not identified, no standard set, therefore not proactively mitigated
Manufacture technical system	'Manufacture' suitable skilled humans through training of pilots, engineers and production staff
Check system work through testing/ certification	Check user competent through testing/licensing
Monitor in service	Monitor in service
Fix serious flaws after they occur	Fix serious flaws after they occur (or attribute blame to 'human error')

which maintenance tasks need other actions (such as improved documentation or duplicate inspections) and which do not need intervention because safety is adequately protected.

This is not a new idea. It was first explored by the UKCAA Design Human Factors in the late 1990s. The FMEA part of the process was successfully trialled in small internal research projects and postgraduate student theses. More substantial UKCAA funded research followed to conduct case studies with major companies such as Airbus, Rolls-Royce and Smiths.

Airbus immediately saw the potential for this approach. Having completed the research project, it further developed and implemented the method within Airbus where it was applied on projects such as A350, A400M and A380, including subcontractors and suppliers. The processes that evolved eventually became embedded in the Airbus Assurance procedures and normal working practices and was later refined through a dedicated PhD study. The concept has since been applied elsewhere (healthcare) and support software is commercially available. Yet, in aviation, it was not propagated beyond Airbus.

Technical Safety Assurance	Human Hazard Analysis (HHA)
Specification to meet SSA targets in CS25.1309	Specification to protect safety from single foreseeable errors
FUNCTIONAL HAZARD ANALYSIS (FHA)	
FAULT TREES that identify critical parts	
Failure Modes & Effects Analysis (FMEA)	Human Error Modes & Effects Analysis (HEMEA)

Airbus Helicopters

HeliOffshore awakens rotary interest

HeliOffshore is actively exploring this approach to reduce risk from maintenance error in helicopters. Working with Airbus Helicopters and HeliOne, a trial completed in December 2017 applied the HEMEA technique to helicopter system design to assess how it might work with their current processes. The full HHA includes a process for selecting the high priority maintenance tasks for the application of the HEMEA. For the trial a different process was used, as Airbus Helicopters had already identified a list of key maintenance tasks from expert judgement and had developed a method of rating five key criteria to assess the human factors sensitivity, to identify candidate tasks for the trial analysis using the HEMEA. The trial included rating all 200 tasks identified by Airbus Helicopters as a prioritisation exercise and working through selected HEMEAs with both Airbus and HeliOne engineers, with both groups finding value in the process. The trial identified the opportunity for some process improvements, and discussions facilitated by HeliOffshore are planned for early 2018.

This method could be attractive to the helicopter manufacturers in managing safety issues related to human error in aircraft maintenance. HeliOffshore would be pleased to hear from other volunteer organisations in the offshore helicopter community who would like to be involved in a trial application (support to the process is currently free!).

If you would like to participate in this debate, please contact scott.carmichael@helioffshore.org