Application of Commercial Aircraft Reliability and Maintainability Philosophy to Reusable Space Vehicles

Harold W. Adams
Chief Designer, Douglas Aircraft Company, McDonnell Douglas Corporation

Follow this and additional works at: https://commons.erau.edu/space-congress-proceedings

Scholarly Commons Citation
https://commons.erau.edu/space-congress-proceedings/proceedings-1971-8th/session-13/3

This Event is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in The Space Congress® Proceedings by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.
APPLICATION OF COMMERCIAL AIRCRAFT RELIABILITY AND MAINTAINABILITY PHILOSOPHY TO REUSABLE SPACE VEHICLES

Harold W. Adams
Chief Designer
Douglas Aircraft Company
McDonnell Douglas Corporation
Long Beach, California

ABSTRACT

Reliability and maintainability requirements for reusable space vehicles are more nearly those for an airplane than for a single-use missile or space vehicle.

Commercial aircraft philosophies of optimum redundancy, dispatch with components inoperative, in-flight fault isolation, and on-condition maintenance, and the considerations necessary in applying them to reusable space vehicles are presented.

A reliability and maintainability design philosophy for reusable space vehicles is developed, based on trade-offs that are a function of the vehicle mission parameters.

GENERAL

From a reliability and maintainability viewpoint, the design and support of a reusable space vehicle is in many ways comparable to those of a transport aircraft. Before discussing these comparisons, I feel it necessary to review the reliability and maintainability program as applied to the aircraft.

The principal measures of reliability and maintainability on commercial transport aircraft are the mechanical delay rate, or "dispatch reliability," and the maintenance cost. A transport airplane reliability and maintainability program aimed at reducing both of these factors is summarized in Figure I. The application of such programs to transport aircraft design will first be outlined, and then their applicability to reusable space vehicles will be discussed.

<table>
<thead>
<tr>
<th>Reliability - Systems and Components</th>
<th>Reduce Maintenance Requirements</th>
<th>Reduce Departure Delays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition - Monitored Maintenance</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dispatch Inoperative - Postponable Maintenance</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Improved Fault Isolation</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Maintainability - Access/Removal - Quick Repair</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Struct Reliability and Accessibility</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

FIGURE I. DC-10 R&M - PROGRAM

RELIABILITY OF COMPONENTS

Component reliability can be expressed as MTBF (Mean Time Between Failure), but a more realistic measure is MTBUR (Mean Time Between Unscheduled Removal) which, in addition to removals for actual failures, includes erroneous removals usually resulting from inaccurate fault isolation.

The most successful component reliability program uses improved versions of proven equipment, unless some new technological breakthrough such as the substitution of transistors for vacuum tubes, promises a major improvement in reliability. When new technology is available, a very thorough test program including simulated service is absolutely mandatory if the new component, even given the advantages of the new technology, is to be as reliable as the older component. This takes time and money.

In using a proven component, its service record is examined in detail, and improvements are made in each area where an increase in reliability appears possible. The use of an in-service component has a further advantage in that the man-machine relationship has been determined in actual operation, and failures resulting from the mechanics' misunderstanding of the maintenance requirements of the equipment are minimized.

Experience has shown that taking a fresh sheet of paper and designing a brand new piece of equipment, no matter how good the designer's intentions, simply results in a new and different set of in-service problems, and 99 times out of 100, a new piece of equipment is not as good when initially introduced into service, and possibly may never be as good as an improved version of an older component. Incidentally, one of the most difficult problems in this approach is that of enforcing this philosophy on the inventive engineer who always feels that he can design something better than anything in service if he is given a free hand.
RELIABILITY OF SYSTEMS

The reliability of transport aircraft functional subsystems can also be expressed as MTBF, but this is over-simplification, since single component failures often produce only degraded operation rather than complete system failure. Systems whose reliability is critical to the safety of the airplane must be redundant to some degree. This redundancy need not take the form of direct duplication, as sometimes other systems can be substituted for the failed or degraded system. If redundancy is employed only to the minimum degree required for safety, all systems must be operating when the flight is dispatched. However, with additional redundancy, the flight can be safely dispatched with some components inoperative, thus avoiding dispatch delays for maintenance and permitting repair at main support bases. Modern transports take full advantage of this philosophy, and many systems incorporate added redundancy for this purpose. Since the flight is dispatched only rarely with equipment inoperative, the aircraft designed to this philosophy is actually safer on the great majority of its flights.

There is a penalty for this increased redundancy, but in transport aircraft design, the penalty has been small and the benefits large. Nevertheless, even in transport aircraft, the cost in dollars, weight and complexity of providing sufficient redundancy to permit dispatch with a major system totally inoperative would be too great to be borne. However, many systems can be operated in a safe but degraded condition at the cost of slightly reduced performance, or a slight increase in cockpit workload. For example, an airplane can be safely dispatched with the fuel quantity gaging system inoperative, but the flight engineer must occasionally compute the fuel remaining by subtracting fuel used, as shown by the fuel flow totalizer, from the fuel initially loaded.

RELIABILITY OF STRUCTURE

The reliability of the structure of an airplane is measured by the number and magnitude of structural repairs required. Two design philosophies are possible: safe-life and fail-safe.

In the safe-life philosophy, the critical structure is analyzed and tested to determine its safe-life. If this safe-life does not exceed the life of the airplane, replacement of the affected structure at safe intervals is made a part of the maintenance program.

Fail-safe in contrast to safe-life implies that the structural parts of the airplane are sufficiently redundant that failure of a single piece of metal will not cause catastrophic failure of the airplane.

Although both approaches have resulted in safe transport aircraft, the leaning in transport design today is toward the fail-safe approach because of the possibility of manufacturing errors, undetected corrosion, unsuspected problems with new materials, etc., causing failures that are not predicted by the tests that determine the safe-life. Of course, the fail-safe philosophy depends on inspection to determine the failure of one member of the fail-safe assembly, but such inspection is standard practice in transport aircraft maintenance.

MAINTAINABILITY AND RUAPID REPAIR

Rapid repair is that aspect of maintainability which deals with maintenance after a failure has occurred. Ideally, we would try to predict an impending failure and perform maintenance before the failure had occurred; however, there are many kinds of equipment, particularly electronic equipment, whose failure is completely unpredictable and the safety of the airplane must be based on the provision of adequate redundancy.

When it is possible to dispatch with the part inoperative, the maintenance can be accomplished at a major support base. In some cases, however, a part whose failure is completely unpredictable is still required for dispatch. In these cases, the capability for rapid repair is mandatory for successful airline operation. Not only does rapid repair increase dispatch reliability, but it also reduces maintenance cost directly.

MAINTAINABILITY AND FAULT ISOLATION

In today's complicated systems, rapid repair does not consist solely of repairing or removing and replacing the part. It is first necessary to go through a fault isolation procedure to identify the failed item. Good fault isolation in transport aircraft results from individual analysis of each system. Ground test, BITE (Built-In Test Equipment), and PCI® (Pattern of Cockpit Indication) are all used; whichever is best for the system being designed. In-flight fault isolation by BITE or PCI has advantages in permitting ground personnel to prepare for maintenance before the flight lands. It is also advantageous for use on systems whose failure cannot easily be checked in a ground environment. In transport airplanes, PCI, fault isolation by analysis of the pattern of cockpit instrumentation, has advantages over BITE in that it adds no complexity or weight to the vehicle.

Once the fault has been isolated to the failed component, then maintainability in the sense of rapid access, repair or removal and replacement comes into play.
MAINTAINABILITY AND MOCKUPS

Provisions for rapid access usually increase structural weight, so a trade-off is required, taking into account weight versus time saved. However, both access and replacement or repair time can be optimized within the cost-weight constraints by the proper use of mockups during design. An engineer designing a system on a flat piece of paper cannot visualize the path of a man’s arm carrying a wrench, passing around a hydraulic line or an air conditioning duct and tightening a bolt. This can only be done in three dimensions. At the very beginning of design, a rough mockup should be made and the equipment requiring maintenance installed and hooked up before the final drawings are released. This permits rearrangement for improved maintenance. In the case of the DC-10, mockups preceded the release of drawings for manufacture by approximately six months. During this period, as many as seven complete rearrangements of some areas were made. In the avionics compartment, below the cockpit floor, these rearrangements changed an original arrangement with work space for one man, no access to the back of racks, poor access to the controls protruding through the bottom of the cockpit floor, etc., into a compartment permitting working space for seven mechanics and very good access to all installations in the area. This required no increase in weight or manufacturing cost but was made possible through the ability to rearrange all of the equipment in the area before freezing the design.

MAINTAINABILITY AND CONDITION MONITORED MAINTENANCE

While many parts, including most electronic parts, have unpredictable failure modes, there still remain many parts of the airplane that have wear-out modes and whose failure it may be possible to predict. In the traditional “preventative maintenance” scheme used during the last decade, parts were removed, replaced and overhauled after a fixed number of flight hours. Statistical examination of the results of this method of maintenance shows that in the great majority of aircraft system components, this philosophy does more harm than good. The wear rate with time varies so greatly for the same component that some parts fail before the fixed interval arrives and other parts are overhauled with only a fraction of their useful life used up. Overhauling a part also introduces problems which increase the failure rate during the period just after overhaul.

Modern transport designs incorporate provisions for monitoring the condition of components while installed, to permit removing parts for overhaul only when the monitoring trends show failure to be impending. As an example, consider transport aircraft hydraulic systems which deteriorate principally by an increase in internal leakage. In the DC-10, flow meters strategically placed throughout the hydraulic system enable a complete internal leak check to be run on the three hydraulic systems in about an hour. If high internal leakage or a trend toward increased leakage is found in one of the systems, the flow meters within that system can be used to pinpoint the deteriorated component. This approach makes for safer airplanes and reduces maintenance cost as compared with maintenance at fixed intervals. The monitoring equipment in the DC-10 hydraulic system weighs thirteen pounds, but cost analyses show that it far more than pays its way in maintenance cost savings alone.

COMPARISONS OF TRANSPORT AIRCRAFT AND REUSABLE SPACE VEHICLE RELIABILITY AND MAINTAINABILITY PROGRAMS

In applying transport aircraft reliability and maintainability programs to manned reusable space vehicles such as the space shuttle, we must examine the operational differences and reexamine the relationship between the cost of maintaining and reliability versus cost, weight and other factors.

COMPONENT RELIABILITY

Component reliability has the same advantages in reduction of maintenance manhours and the same requirements as they affect safety for both aircraft and space vehicle programs; however, at least three factors that could cause differences in the reliability weight-cost trade-off should be considered:

1. Higher component reliability may reduce the number of redundant systems required for equal safety: For average (5-1/2 hour) flights, three systems with 1000 hour components have the same probability of total failure as four systems with 300 hour components. For longer flights, three systems are better. The reduction in the number of systems has obvious weight and maintenance advantages, so we can afford both pounds and dollars for improved component reliability. If the vehicle safety policy requires a fixed level of redundancy, advantage cannot be taken of high component reliability to reduce the degree of redundancy. A more realistic view of the safety of the vehicle than simply counting failures is to estimate failure rates in various modes and express the safety of the vehicle in terms of minimum number of flights between catastrophic accidents. This approach will optimize the vehicle from a safety standpoint and permit advantage to be taken of high reliability components. There is a psychological problem, however, in making the initial assumption that any catastrophic failure rate is tolerable. We all recognize it, but no one speaks of it, and until this is overcome, we will probably continue with the present approach.
2. Failure rates cannot simply be measured in flight hours or cycles. Several flight phases may have greatly different failure rates, as; subsonic flight versus non-powered orbital flight; and cyclic effects at takeoff and re-entry may assume more importance in determining component failure rates.

3. In early reusable space vehicle programs, maintenance cost will probably be a lower percentage of total system cost than is the case for transport aircraft, and weight will be of greater importance, especially in two stage vehicles.

The advantage of dispatch with components inoperative will depend on the operational requirements of the particular space system. One advantage is the ability to dispatch within a launch time "window" even though a minor failure is discovered shortly before launch time. If we make the assumptions (1) that all electronic gear will be turned on two hours before launch, with no repair permitted during this period; (2) that the vehicle will incorporate 100,000 transistors or equivalent; and (3) that each transistor has a MTBF of 1,000,000 hours, then it can be seen that launch reliability will be only about 80% if all transistors must be operative at launch.

STRUCTURAL RELIABILITY

Structural reliability design in space vehicles may be forced more toward the safe-life philosophy by the importance of weight and the short life and few cycles at high loads relative to transport aircraft. The greater uncertainty surrounding the loading criteria does not necessarily favor fail-safe since ultimate strength is the same for structures designed to either philosophy.

RAPID REPAIR

Since the on-ground interval between flights of manned reusable space vehicles will almost certainly be longer than for transport aircraft, rapid repair will be of less importance. Current space shuttle planning allows five days between flights, while commercial transport aircraft have only about 45 minutes between flights, with an eight hour period available two or three nights a week.

The advantages of in-flight fault isolation will lie more in the areas of increased safety by aiding to crew decisions on action to be taken when failures occur, and in isolation of faults that occur only in the flight environment and thus are difficult to isolate on the ground. As in transport aircraft, PCI versus BITE versus ground test must be evaluated to find the best method of fault isolation for each individual system, but using the criteria of crew decision and flight environment isolation rather than the criteria of reduction in repair time. For some vehicle applications, it will be worthwhile to design for in-flight repair, which of course will require in-flight fault isolation, access, spares, and tools.

Rapid access provisions usually require weight increases, whether they are cost effective for a space vehicle will depend on the minimum interval planned between landing and subsequent takeoff. With a five day interval, the trade-off of weight versus maintenance cost is not likely to permit the addition of appreciable weight for rapid access.

MOCKUPS

The use of early mockup for maintenance improvement by permitting three dimensional rearrangement will be of equal importance for space vehicles as for transport aircraft, since by this means maintainability can be improved with no increase in weight.

SIMILARITIES AND DIFFERENCES

In reviewing these similarities and differences between reliability and maintainability programs for transport aircraft and for manned reusable space vehicles, it is apparent that the programs require the same elements, but that the trade-off factors and their emphasis will vary; greatly in some portions of the program, little in others. Variations in trade-off factors is not new to the aircraft designer who is confronted by major changes in emphasis when working on such varied transport aircraft programs as large long range commercial transports, small short range executive aircraft, and VSTOL aircraft.

CONCLUSION

Application of commercial aircraft reliability and maintainability philosophy to reusable space vehicles will be beneficial to the program and will pose no problem to a commercial aircraft design department if the differences are recognized at the beginning of the program, and design policies based on trade-off studies are established by design management.