FAILURE MODE EFFECTS ANALYSIS:

CONFIDENCE BY DESIGN

By BOB NUCKOLLS
EAA 205021
The AeroElectric Connection
6936 Bainbridge Rd.
Wichita, KS 67226-1008

I considered sub-titling this article, "Laughing in the Face of Adversity." Laughing? Well, at least smiling! In prior articles I mentioned failure mode effects analysis, a phrase which means exactly what you would deduce from four simple words: an analysis of the effects of failures. First, all possible failures of a product to do its intended task must be considered. This isn't difficult; virtually all failures are 100% predictable even if all possible effects are not clearly known. Each kind of failure must be considered weighing factors of: (1) making a part stronger or (2) reducing stresses in the part of (3) simply reducing its advertised service life. (Engines with TBOs on the order of 10,000 hours are possible, but they are a tad heavy for airplanes.) Changes made for reducing probability of failure always affect performance, weight and cost, sometimes in undesirable ways. Then comes the hard part. Manufacturers cannot control the manner in which a product is used; people have been known to ignore warnings, instructions and common sense. Fortunately, most user-induced product failures do not present hazards to life and limb; most simply cause a loss of product services and added repair or replacement costs to users.

Major manufacturer concerns arise when a failure induced by either end-of-life or user abuse creates a hazard. Such failures are fertile ground happily plowed by the plaintiff bar; "Well, Mr. Cessna, will you tell this court and jury why you didn't warn the owner of this twenty-five year old airplane that worn seat rails could cause a hazardous condition?" Who could have deduced 25 years ago that anyone would allow this part of their airplane to become so worn? Nowadays, whole teams of engineers study and theorize for every possible contingency. If a condition is perceived hazardous it must (1) be designed out of the product or (2) warnings clearly presented to current and future owners. This may result in a product having more surface area in warning placards than paint! However, woe to a company whose crystal ball is partially overcast the day a new product starts rolling off an assembly line. Obviously, had Cessna placed seat rail maintenance warning placards on those old birds, they would have saved millions! However, I suspect it would not have saved many lives.

Owner/operators who most often fall prey to end-of-life induced hazards have allowed themselves to be lulled into a sense of security knowing the airplane has performed very predictably for many years. Society's ills aside, what does this all mean to you as an owner/operator who has also built the airplane? Besides a benefit of freedom from lawsuit (I don't think anyone has ever sued himself!), it does put you into a position of having to consider the health and welfare of yourself and future passengers.

Nearly every aviation publication features articles under the general headings of "I Learned About Flying From That", or, "Never Again!" I note that these articles always deal with lapses in pilot attitude and/or poor decisions. But where are articles published for engineers (or amateur airplane builders) in which contrite survivors of bad decisions bare their transgressions for the benefit of those who ponder ways to avoid repeating the same mistake? Well, you won't see them in publications for John Q. Public pilot but you will find them in kit-type newsletters.

If you are not subscribing to any and all kit-type newsletters applicable to your construction project, then consider doing so. Order all back issues and comb them for notices from designers and builders alike. Even after your airplane is finished, continue to subscribe and read all published information. Kit-type newsletters are informal equivalents of FAA Airworthiness Directives (ADs). Staying vigilant to old and new developments about your project is a vital part of keeping your airplane airworthy (notice I didn't use the word "safe") and minimizing operating costs.

Further, be attentive to ways you can contribute to the knowledge base while working on your airplane. Publicizing your failures is just as important as talking about the successes; especially if the undiscovered failure creates a hazardous condition. Some other builder may make the same mistake you did and fail to correct it before it bites him!

SPORT AVIATION, February 1993, carried an article I wrote on the topic of designing for electrical system reliability. In that article, I introduced a concept that describes "reliability" as being able to comfortably complete a flight in spite of any single failure of an electrical system component. That may sound like a new oxymoron but consider that the word "reliability" applies to the flight system which includes airframe, pilot, powerplant and subordinate systems. The task is to produce a system design that is tolerant of certain kinds of failures.

Obviously, one expects to have some difficulty tolerating a failed wing spar but what about electrical systems? (Incidentally, I read recently that the FAA has awarded supplemental type certification for a ballistic chute on the C-150 series aircraft . . . more will undoubtedly follow. So maybe tolerance of failed spars and struts isn't a terribly absurd idea!) To my way of thinking, the most reliable electrical system design is achieved only after I have assumed that every single part in the system is going to fail in flight at some point in time. The trick is to apply the following questions to each case:

1. How many ways can this part fail?

2. How will each failure affect system operation?

3. How will I know it failed?

4. Is the failure pre-flight detectable?

5. Is failure of this part, in any failure mode, likely to create a hazard to flight?

6. Will failure of this part be likely to overtax my skills (as pilot) to comfortably terminate the flight?

Let's consider a simple example of an FMEA on a landing light system consisting of circuit breaker or fuse at the bus, interconnecting wires, landing light control switch, and a lamp bulb. First, what about wires? Nearly every wire has a terminal crimped or soldered on each end. If the crimp is improperly applied, the wire can slip out or break off under vibration. If a "hot" end of a wire slips out of the terminal, possible consequences are: (1) circuit is broken, lamp simply fails to illuminate or (2) wire falls against airframe and shorts out; fuse or breaker pops and lamp fails to illuminate. A wire can be damaged (cut) which has same result as (1) or insulation abraded which may duplicate the same effect as (2). The switch may (1) fail electrically such that connection becomes open or intermittent; the lamp may fail to light or (2) mechanically wherein otherwise good electrical contacts are simply not brought together inside. Again, the lamp fails to light. A similar set of conditions and effects apply to fuses and breakers. That leaves the lamp itself. You KNOW the lamp is going to fail; probably at some time when you would like to use it.

How does this example submit to the list of questions above? We've considered the failure modes. Some of the failures are related to design and workmanship; learn how to properly terminate wires and route them to preclude mechanical damage. Other failures are affected by quality issues; select switches and breakers with reasonable life expectancy in the proposed application. Inevitable failures occur at end-of-life. It makes no difference here if we're considering landing light bulbs or seat rails; we know that at some point in the future, these parts WILL

FAIL to perform their intended task.

Certainly, a landing light system is pre-flight testable. However, operation before flight cannot GUARANTEE availability a few hours later! Is system failure likely to create a flight hazard? Loss of landing light system doesn't result in immediate loss of control or structural integrity. But what about you as the pilot? Are you confident and skilled in landing without it? This is a fairly simple example but it illustrates some important points to be considered in designing, fabricating and using any airplane system: (1) Any system is no stronger than its weakest part. There's little point in purchasing other components built to NASA specs when you KNOW the bulb is going to fail anyhow! (2) If system failure can be detected in preflight, is it a part of your checklist? Most published checklists meet minimum requirements. You are certainly entitled to expand your list as appropriate. (3) Hazard potential in this case is a function of pilot skills. If you are not comfortable with landing in the dark, then do our wife and kids a favor, install a second light. How about an automotive head lamp with dual filaments? The low beam filament will not illuminate the same way as the high beam but it is adequate in a pinch.

FMEA becomes more significant as system complexity and failure effects escalate. Consider an electric trim system. Suppose a trim switch or relay sticks and the trim tab drives unexpectedly to a full up (or full down) limit. Is this likely to cause immediate airframe damage or loss of control? Can you still land the airplane with the trim tab driven to either limit? Even if YOU can land the airplane with a tab at limits, how about the guy you sell the airplane to? These are the kinds of things that can bite you years from now. Even if you know everything about your airplane and can deal with all its idiosyncrasies doesn't mean everyone can.

You cannot guarantee you or some future owner won't have a bad problem sometime in the future but you can greatly reduce the probability. Do FMEA studies on ALL systems, mechanical or electrical. Do tests (where practical) to determine how a failure stresses either the airplane or your skills (e.g. shoot touch and go landings at increasing out-of-trim settings to see if you can deal with a trim runaway). If any perceived failure is deemed intolerable, redesign the system to eliminate the failure or to provide some form of back-up. If you determine that some failure is personally tolerable, DOCUMENT it.

Future owners cannot assess their personal failure tolerance if they don't know what to test for.

EAAers are building some of the most advanced airplanes ever designed. Installed systems should rival, if not surpass the capability and quality of hardware installed on certified ships. FMEAs are useful tools for separating issues of perceived quality, convenience, reliability and safety. As I've illustrated in the landing light example, enhanced quality doesn't equate directly into enhanced reliability. ASSUME that every electrical system component WILL fail at some point in the future. Determine that (1) the system is not needed for comfortable completion of flight or (2) design in a backup. In either case, design your system for failure TOLERANCE.

A classic example of inappropriate attempts at simple repairs in flight: do you recall the L1011 that flew into the Everglades a few years back? The entire cockpit crew was working on a failed gear down indicator light. FMEA studies allow you to plan ahead - do all systems analysis and repairs on the ground AFTER YOU HAVE LANDED. There are cost benefits to be realized too. If any failure is tolerable by design, it matters not whether you bought high-dollar, mil-spec or plain vanilla parts . . . all failures have been reduced to simple maintenance issues. ◆

Bibliography

Written coverage plus real-time consulting services by the author on this and other electrical systems topics are available from the address listed above. $42 USD buys all materials in print (13 chapters, lots of illustrations, 5 appendices, 200 + pages) plus one year's subscription to newsletters and the next issue of chapters on specific topics. Overseas subscribers add $20 USD for airmail postage. MasterCard and Visa are accepted. The author may be contacted directly at 316/685-8617 or Compuserve 72770,552.