Bob Nuckolls
6936 Bainbridge Road
Wichita, Kansas 67226-1008
Voice/Fax: 316-685-8617
E-mail: nuckolls@aeroelectric.com

What's all This "Failure Tolerance" Stuff Anyhow?

I participate in a few list-servers . . . a cybernetic party line for individuals with a common interest . . . usually in the construction and use of a particular amateur built airplane. A broad range of knowledge and skills is represented. An equally broad collection of ideas is brought forward for the sharing of information. It's not surprising that some ideas are not as well received as others . . . the discussions can be excited, perhaps a bit heated and occasionally folk's feelings get hurt. After observing a few "differences of opinion" some participants are increasingly reluctant to bring their own ideas forward . . . for a host of reasons.

Occasionally I receive private letters, off the list-server, from folk who really want to be heard but wish to steer around the more public discussions. I'll share one such exchange with you because it helps me to illustrate what I believe are the formidable strengths of list-servers for (1) the sharing of ideas knowledge and (2) the evolution of new ideas for advancing the art and science of airplane building. Importance of the "mission" aside, we're still people with aspirations and people's expectations for civil treatment cannot be ignored. More important than the mission, I'll suggest that list-servers offer another opportunity . . . to be the mechanism by which ideas are reviewed and nurtured or discarded as worthless or subordinate to a better one. Please consider the following comments from a list-server participant and my reply. . . .

It has taken a while for me to be able to put this in just the right words. I'm still afraid that I'm going to offend you. That's not what I'm trying to do here. I have a lot of respect for you and your experience .. .

Thank you sir and don't worry about upsetting me . . .

*. . . and please note that I chose to bring this up in a private E-mail message, and not in public on the list server. I want to *communicate with you*, not grandstand.*

Fair enough. . . .

First, the comment: While I have much respect for your opinions, I don't always agree with them. Too many times in my life, I've looked at someone's solution to some problem. (usually a well thought-out solution too) and my gut was uncomfortable with it. And I would say, "There's a problem with that solution. I don't know what it is right now, but my gut says it's gonna come back to bite us." Sometimes I was wrong, but in too many cases I was right. It DID come back to bite us. And when I said "There's a problem with that solution", the designer would always say, "show me where." Of course I never could.

My friend, here's where we differentiate between science and fiction. It doesn't take an "expert" to be a scientist. Further, people with any sort of authority are suspect because they get their authority from rule books and policies written by someone else and carved in stone. Problems with any design have explanations upon which judgments for change can be made. The definition of progress includes change. You and I are doing science here. The goal is to deduce answers for the "show me" questions. Anything short of that subordinates our freedoms to the experts and persons of authority. When someone proposes any sort of new concept for aircraft, there is an obligation to explain it terms of the physics with functionality filtered through what we know as technicians and pilots.

Anyone who proposes a new concept is **not entitled** to say, "do it my way because I'm an expert." Worse yet are the aviation legends circulated with words like, "I know this guy who has a friend who . . . ." We've all heard this kind of advice before. If one cannot sufficiently explain a concept to either dispel or confirm your reservations, then go with your gut feelings and keep the idea under suspicion. However, even after you're favorably convinced, the idea should be open to further review at any time.

So now to our particular disagreement: You advocate using automotive fuses in a location inaccessible to the pilot during

flight. My gut says, "There's a problem with that solution." Now, I'm sure you remember a few weeks ago when you posted a message to the list in which you describe that you discovered that under certain circumstances a 60-amp alternator could produce MORE than 70 amps, blowing the 70-amp fuse you were supplying. As a result, you said, you were switching to an 80-amp fuse.

I think we're really talking about two different situations here, with one being a sub-set of the first. First, the concept of using un-reachable fuses is a technique that encourages failure tolerant designs. The fact that any particular fuse nuisance trips is a different problem, with a different solution.

*Please understand that I'm *not* trying to say "I told you so". I'm too much of a gentleman for that. I'm just using this as a means of helping you see it from my side of the fence. This incident goes to show that "Even the best-laid plans of mice and men...", as the saying goes. There's not a doubt in my mind that the 70-amp rating was determined using good, sound, engineering principles.*

Several folk brought up the same thought and my question of them was, "have you never had a design evolve through several stages before it was complete?" The 70-amp choice was based on the observations of quite a number of systems. The value was chosen based on the observation that production variations in 60-amp alternators didn't go any higher than 70 amps in a current-limited mode. Only two of several hundred 70-amp kits flying have exhibited the phenomenon and then only in unusual circumstances. If I'd been working for one of the heavy iron bird factories, the phenomenon would have been administratively dubbed a "non problem" and summarily ignored. "Sound engineering principles?" Sure, but where is it written that sound engineering principles produce infallible, un-modifiable designs? Only "government certified" designs are un-modifiable and they're certainly not infallible.

Since our 70-amp fuse was subject to nuisance tripping under some, albeit rare conditions, an analysis of failure modes including an evaluation of wire-size already in place suggested we raise the value of the fuse to 80 amps. I expect this change will now cover ALL the 60-amp alternators out there. Up-sizing the fuse takes care of design decision #1, fix the nuisance trip.

But why should it be a **problem** when the nuisance trip occurs? Here's where There are dozens of ways that alternator can fail that won't pop a fuse. What are you going to do when one of those failures happens? What value is there in being able to handle a nuisance trip from the cockpit (i.e. leave the classic panel mounted breaker in place) when there are so many other failures that you can do nothing about?

We can stop nuisance tripping by up-sizing the fuse (or breaker). All other failure modes, need a "Plan-B". I would hope your answer to any failure is (or will become), "switch to plan-B and get on with my piloting business." A number of people latched onto the idea that the fuse sizing was some sort of "mistake" . . . well, I suppose it might be . . . we made a decision based on incomplete data; data that had to be gathered from the field in real operating environments.

Remember that we're striving to design and fabricate failure tolerant systems and pilots to go with them. The failure of that fuse or any other part of the alternator system should be no-big-deal . . . no single failure of any component should create a hazard to flight or a tense pilot. When that goal is achieved, we're free to experiment, adjust, consider and discard the less-than-useful in favor of advancing the design. Moving from 70 to 80 amps was a considered evolution of a design, no more, no less. Up-sizing the fuse avoids getting our hands greasy replacing it. If it causes you great concern perhaps you do not yet embrace the concept of failure tolerant design.

Failure tolerance is a weird concept in our society . . . *"whada mean you don't care if it breaks? You paid good money for that thing, it oughta work when you want it to."* Intuitively, we know it's a faulty concept. None-the-less, between the FTC, FDA, EPA, Trial Lawyers Association, FAA (you name 'em), we're encouraged to believe that's our due. Hmmm . . . what's that old saw about living in a perfect world? Well, suppose we relax our expectations a little and say, "some things breaking are okay . . ." That comes a bit closer to reality because in many circumstances things that break a lot are "certified". It matters not to people with authority that repeated failures are costing you your shirt just to keep your airplane operable.

I recently studied a downloaded list of service difficulty reports using the keyword "alternator". I found phrases like, "through-bolt broke, casting cracked, brushes burned, windings shorted, diodes shorted, etc. etc." Virtually everything that could happen to an alternator happens **routinely** on certified airplanes. None the less, each of those failures was sent to a shop sprinkled with Washington holy-water where it was returned to it's original, certified condition and bolted right back on somebody's airplane!

If these failures were deduced to cause crashes or risk of crashes, there would be the usual response in the form of airworthiness directives but consider this: Given that thou-

sands of alternators failures are documented every year with little or no AD activity, might we deduce that airframe systems are generally tolerant of alternator failure?

My personal goal is to make pilots equally tolerant of the failures, not because we're forced to fly with certified junk but just the opposite. If we're not concerned about individual failures of components, then we're **free to try any and all components** in a real life situation to deduce which are most suitable in terms of value received. Experimentation in certified aircraft is essentially impossible due to regulation fueled by bureaucratic ignorance and public fear. We'd like to apply simpler, lower cost and more reliable solutions but regulation all but eliminates real progress. So in certified ships, we struggle along with the status quo.

I'll suggest this environment tends to make us focus on things that we're expected to address in terms of response to failures . . . like fiddling with breakers or developing back-ups to back-ups, or getting on the radio for comfort and/or assistance. Instead of developing systems and pilot knowledge that tolerates any failure, we take comfort in being able to hammer on the few things we might fix in flight and try not to think about the things we cannot fix. Besides, it makes for good material when trading wing-and-a-prayer survival stories over a suds. Problem is, from time-to-time airplanes get bent and people get hurt . . .

In amateur-built airplanes, we have an opportunity to build better flight systems than our spam-can flying brethren can expect. I'll suggest that failure tolerance can help it happen. Instead of a cliff-hanger story the guy says, *"Yeah, as a matter of fact, I had that thing quit several times . . . had to flip a couple of switches and get out the toolbox when I got home. I've been thinking about upgrading that piece of junk . . . missed a good ball game once because I was hammer'n on that thing!"* . . . doesn't make for very exciting story telling, does it?

The public perception of airplanes is that they are fragile machines that come spiraling out of the sky when anything breaks. A problem I perceive is that a lot of pilots sign up to the idea too. After you get a few hundred hours in C-120s and J-3s you develop an appreciation for how little you need to go flying. Everything else is a convenience that should absolutely not be depended on to be working 100% of the time. That's why we embrace built-in or hand-carried backup systems for flight situations that may need them.

I'll suggest that specifications, certifications, STC's, PMA, qualifications and conformities don't mean squat with respect to absolute reliability. A study of service difficulty reports and/or interviews with a few mechanics will confirm the any suspicions you may have with respect to quality also. We should design, fabricate and test systems and develop procedures for operating them so it doesn't matter what parts get changed for any reason. Then we're free to evolve our designs into the best airplanes that have ever flown I've published a warranty statement for our parts catalog that reads something like this:

Warranty

If you have purchased any product from us which in your opinion was not a fair value, return it for a full refund.

"We absolutely guarantee that everything you purchase from us is going to fail. We spend a lot of time researching methods and technologies that perform well and give fair value. The vast majority of parts we sell you will still be in service the day your airplane is scrapped. However, if plan to use your airplane in a way that absolutely depends on any single component function 100% of the time, please don't buy the part from us. Our parts and design services are offered to individuals who architecture systems and possess a pilot's attitude that no single failure is more than a maintenance issue. By-the-way, should you locate a supplier that guarantees their parts will never fail, please let us know who they are, we'd sincerely like to license their technology."

Our friend continues, "*I hope by telling you this that we can maintain our cordial relationship, and that you'll have as much respect for my 'gut feelings' as I have for your experience and expertise."*

Your "gut" feelings are correct, because you do not yet possess the data and confidence to dispel them. It's foolish to embrace things I say because of any aura of expertise or authority I might project. Until you take personal possession of knowledge and tools to move ahead, you are better off working with things you know. When and if the day comes that you agree with anything I have to offer, please promote the idea to others because because YOU say it's good not because this guy Nuckolls sez so . . . and then be prepared to explain it to your audience in terms they too will understand.

So much of what's passed around as common wisdom is hearsay propagated by folk who don't understand the issues. When the idea is questioned, their only defense is to get hysterical. I try to avoid bringing any idea forward until I'm ready to address all the questions. If you don't embrace it by virtue of understanding, then let's continue to talk about it.

Perhaps my reasoning is faulty . . you can help me identify the error. But know that we need to behave like scientists. Let's work with facts. My friend, these are the kinds of discussions that build relationships, not tear them down.

I should mention that my own philosophies for engineering and design are evolving for having read some words by the late Carl Sagan. He introduced me to the idea that "doing science" was not the exclusive domain of experts and authoritarians; rather a simple tool wherein ordinary people pick, probe and inspect an idea looking for truth based on physics and not faith. I could stand on a soap box and preach the gospel according to Carl Sagan but after reading his words, I'm certain he would not want that. The man is gone but his ideas are still with us. I'm sure Carl Sagan would delight in the knowledge that his thoughts continue to be picked, probed, inspected and flourish (or become replaced) because the science is good, not because we read his beautifully illustrated book or saw him on television. It's important that you do good science to understand, embrace and then promote concepts because they've been adopted as your own, not because I or anyone else holds them forth.

There's nothing wrong with crediting your sources of inspiration as I have just done. The strength of your argument grows 10-fold if you say, "I read this book by ---------- and found some ideas that I think are really great." However, from that point on professor, it should be **your** classroom.