Apogee Components

PEAK OF FLIGHT

NEWSLETTER

In This Issue

Redundancy in Deployment Systems; Why 'More' Probably Isn't 'Better'

Cover Photo: Newway Rocketry's SquareOne Kit. Get one at:
www.ApogeeRockets.com/Rocket_Kits/Skill_Level_2_Kits/SquareOne

Apogee Components, Inc. — Your Source For Rocket Supplies That Will Take You To The "Peak-of-Flight"
3355 Fillmore Ridge Heights
Colorado Springs, Colorado 80907-9024 USA
www.ApogeeRockets.com e-mail: orders@apogeerockets.com
Phone: 719-535-9335 Fax: 719-534-9050

ISSUE 322 SEPTEMBER 25, 2012

Redundancy in Deployment Systems; Why 'More' Probably Isn't 'Better'

By Joseph Avins

In preparing for my HPR Level 2 certification attempt, and thinking ahead to Level 3, I was thinking about redundant recovery systems and considered going beyond simply having two altimeters and ejection systems to creating a system with multiple redundancy so that there would be virtually no chance of ejection failure. As I considered how best to do this I came to realize that it was actually a really bad idea. In this article I'll discuss the benefits – and limits – of redundancy.

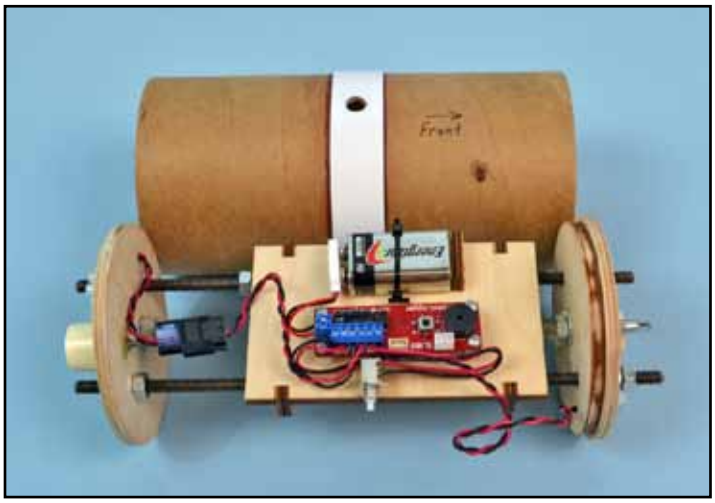
Definitions

We should start with some definitions. Redundancy is the use of more devices to do something than are strictly necessary, so that if any one (or possibly more) of them should fail, the overall system will still do what it's supposed to do. The obvious example for us rocketeers is using two altimeters or other devices, each able to operate an ejection actuator such as a black powder charge. If one doesn't work, the other (probably) will. But it is also redundancy if you use one ejection charge that is part of the engine and another that is activated by an altimeter or timer; the multiple devices do not have to be the same.

Apollo 13 lost one of its five first stage engines early in its ascent, but the mission was able to continue because those massive engines could complete the ascent with only four working.

Another interesting example is a five legged office chair. Assuming the load on a chair is well centered, it can stand just fine on three legs. (Though this would more often be a stool.) Four legs are more than enough, but interestingly, if one of those four breaks, the chair (or stool) will probably fall anyhow; the geometry of four legs is such that the remaining three would not function to keep the chair up. But with five legs, any one can fail and the chair will stay up. In fact, the chair might stay up even if two legs fail, but it might not. (This isn't the main reason that office chairs have five legs, but I digress.) But enough of furniture; we're hear to talk about rockets.

Our first two examples (dual altimeters and engine ejection plus altimeter) would be referred to as 2-for-1 redundancy, meaning that there are two devices and only one (either one) needs to work. The Saturn V first stage engines had 5-for-4 redundancy.



An ebay with only one altimeter installed is not redundant unless motor ejection is also used.

Why Redundancy?

The answer is fairly obvious: it makes the system more reliable. But just how much more reliable? For that, we need to do some math. Don't worry, I'll try to keep it to a minimum.

If we have two independent events, we can call the probability of one event occurring p_1 and the other p_2. In this case, we'll use p_1 for the chance that the first altimeter fails and p_2 for the chance that the second altimeter fails. The probability of two things both happening is the product of the two individual probabilities, if the two events are independent. (If one event influences the other then the math is more complicated, but we don't need to consider that situation.)

The only way that a 2-for-1 redundant system can fail is

Continued on page 3

About this Newsletter

You can subscribe to receive this e-zine FREE at the Apogee Components web site (www.ApogeeRockets.com), or by sending an e-mail to: ezine@apogeeRockets.com with "SUBSCRIBE" as the subject line of the message.

Newsletter Staff

Writer: Tim Van Milligan
Layout / Cover Artist: Tim Van Milligan
Proofreader: Michelle Mason

Continued from page 2

Redundancy In Deployment Systems

if both of its devices fail. In other words, the system succeeds if it does not occur that both devices fail. Now, that may seem like a strange way to say it, but there's a reason; saying it this way will help make the math more understandable. The chance of success, p_S, is:

$$p_s = 1-p_1 \times p_2$$

The product of p_1 and p_2 is the chance of both failing, and one minus the product is the chance that they won't both fail, that is, the chance that at least one will work.

For a more concrete example, suppose we have two altimeters, each with its own igniter and ejection can. The altimeters are different brands, so one has a probability of working of 85% and the other of 88%. (Of course, if some brand really had only an 88% chance of working, let alone 85%, you probably wouldn't buy it, but this is just an example.) That means that their chances of failing are 15% and 12% respectively. The probability that at least one of these will work is:

$$1-(0.15)\times(0.12)$$
$$= 1-0.018$$
$$= 98.2\%$$

So, even with rather poor altimeters, we have a very good change of overall success.

And that's why we use redundancy.

But What About Early Deployment?

Up untll now we've been talking only about an ejection system failing to operate. With many things this would be good enough; either it works or it doesn't. But with ejection systems there are two potential problems. They can fail to fire (or fire too late), *or they can fire too soon*. We say that they have two failure modes: firing early and firing late or not at all.

Now, it is really quite rare that a deployment system fires too early. And when it does happen, it's very likely caused by a mistake on the rocketeer's part rather than an intrinsic failure of the equipment (and that's true of non-fire failures, too.) But rare as it is, it does happen. Are some devices more prone to it than others? Are some devices more or less touchy than others, making them more or less prone failures due to human error? Well, at the moment we really don't have *ANY* data on this, so I'm going to have to make up some figures in order to illustrate why more redundancy isn't always better.

{Editor's Note: There is no evidence that altimeters fail

Continued on page 4

Continued from page 3

Redundancy In Deployment Systems

by ejecting early (except in the case of Mach flights which are compensated for by modern electronics). Therefore, don't get too concerned about the failure rates to follow. This is more of a thought-experiment about the process of failure prediction.}

In terms of the system's chance of success, the two failure modes, early firing and late firing, have to be considered differently. For late or non-firing, the system fails only if both fail, but for early firing, the system fails if either one fails. As shown above, redundancy reduces the chance of not firing, but it also increases the chance that one or the other will fire early. Time for some more math.

Let's call the chance of firing early for the two altimeters p_{E1} and p_{E2}, and the two chances of firing late (or not at all) p_{L1} and p_{L2}. The chance of not getting any deployment is what we discussed above, but deploying early (say, during the engine burn!) doesn't require that they both fail, since either one is bad enough. What we need in the early phase is for them to both succeed. The chance for each one to not fire early is one minus its p_E. So the chance of both not firing early is

$$(1-p_{E1})\times(1-p_{E2})$$

and the chance of failure because one or the other fires early is

$$1-(1-p_{E1})\times(1-p_{E2})$$

System failure comes when one of the altimeters fires early or both fire late. These two are mutually exclusive, which is to say that they can't both happen; if either one or the other fires early then it's not possible for both to fire late. When two possible events are mutually exclusive, their probabilities can simply be added together to get the probability of one or the other happening. So, the overall chance of failure is

$$[1-(1-p_{E1})\times(1-p_{E2})] + p_{L1}\times p_{L2}$$

and the overall chance of success is

$$(1-p_{E1})\times(1-p_{E2}) - p_{L1}\times p_{L2}$$

(That's as bad as the math is going to get.) Getting back to a concrete example, let's say that the figures for our two altimeters above represent their chances of firing too late, 15% and 12%, and that their chances of firing early are 1% and 2%. (Even these small numbers are very likely higher than would be found in actual data.) Then, individually they have chances of failure or 15% + 1% = 16% for one and 12% + 2% = 14% for the other. The redundant system has only a 1.8% chance of firing late (as shown earlier) and the chance of firing early is

$$1-(1-0.01)\times(1-0.02)$$
$$= 1-(0.99)\times(0.98)$$
$$= 1-0.9702$$
$$= 2.98\%$$

The overall chance of failure is the sum of this and the chance of late (or not) firing that we computed before

Continued on page 5

Continued from page 4

Redundancy In Deployment Systems

2.98% + 1.8% = 4.78%

This is better than either of those altimeters alone, but notice what happened with the chance of early firing. Where the two altimeters individually had 1% and 2% chances of firing early, together the chance is 2.98%, which is worse than either one alone.

Ah, there's the rub.

Using redundant altimeters can make the chance of failing to fire virtually disappear, but it increases the chance of early deployment. So how do we know when redundancy helps and when it doesn't? Let's try some more test cases with made up figures.

Let's say we have three different altimeters, and each one has a 4% chance of failure. One has equal chances of early and late firing, 2% each. Another has a 1% chance of firing early and 3% of firing late, and the third has a 3% chance of firing early and 1% of firing late. What we're going to do is combine two of each type and see the results. I've done the math, and the results are shown in Table 1. (Of course, these failure rates are probably unrealistically high. I've used somewhat large numbers in order to make the effects of redundancy also large and obvious.)

When the early and late firing chances are the same, redundancy doesn't make any difference at all; the redundant system still has a 4% failure chance. When the chance for one altimeter to fire early is less than its chance of firing late, the redundant system's chance of failure is better than for one unit alone. But, when the early firing chance is higher than the late firing chance redundancy actually makes matters worse!

The other important thing to notice is that in all three cases, the redundant system's chance of late firing is very small and *the overall chance of failure comes mostly from*

One Altimeter Chance of Failure			2-for-1 Chance of Failure		
Early	Late	Overall	Early	Late	Overall
2%	2%	4%	3.96%	0.04%	4.00%
1%	3%	4%	1.99%	0.09%	2.08%
3%	1%	4%	5.91%	0.01%	5.92%

Table 1 – Effects of 2-for-1 Redundancy

Continued on page 6

Wanted: Your Rocket Products

If you're a manufacturer of rocketry products, like kits, electronic payloads, parts, construction tools, motors, launch equipment, or something totally cool, we're interested in talking to you. We're always looking for new products to sell.

So why have Apogee sell your products?

- *We have the best customers that are looking for someting new.*
- *We provide the product support for the customers, so you don't have to.*
- *We take care of all of the hassles, so you can focus on what you do best.*
- *We are a volume seller - Our web traffic means buyers will find you easier.*
- *Our endorsement means you sell more and make more money!*

APOGEE COMPONENTS

www.ApogeeRockets.com

If you're not getting enough sales on your own, let's talk.

Continued from page 5

Redundancy In Deployment Systems

the chance of early firing.

To put that another way, these redundant systems have the same early and late firing chances as a single unit where the late firing chance is very, very small and the early firing chance is much larger (though still small.) It is surely unusual for a real altimeter to have a greater chance of firing early than of firing late, but a redundant pair acts just like that.

What happens if we add more redundancy?

The overall chance of failure gets worse, just as if we had added redundancy with a single unit that has a high early fire chance. If the single altimeter's late fire chance is much, much more than its early fire chance, then it is possible for two of them together to still have a greater late fire than early fire chance, but the numbers for that to happen would have to be pretty crazy.

Table 2 and Figure 1 illustrate this. Even though the failure chances for the devices are hypothetical (that is, I made them up) we can see the key results plainly:

# of Devices	1%/3%	2%/3%	3%/3%	1%/13%
1	96.00%	95.00%	94.00%	86.00%
2	97.92%	95.95%	94.00%	96.32%
3	97.03%	94.12%	91.26%	96.81%
4	96.06%	92.24%	88.53%	96.03%

Table 2 - Effect of Redundancy, p_S with Devices with $p_E/{}_pL$

If the early and late fire chances of the device are the same, then 2-for-1 redundancy makes no overall difference and any more makes matters worse.

If the early chance is greater than the late chance then any redundancy makes matters worse, although we expect this to be pretty rare.

If the late chance is greater than the early chance by a reasonable amount then 2-for-1 redundancy helps overall, but any more is worse.

And if the late chance is worse than the early chance by a very, very large amount then 3-for-1 might theoretically be optimal, but anything more will *still* make matters worse, and you'd really be better off spending your money on better altimeters (like the ones at Apogee Components) than on three bad ones! Well, actually, no one sells altimeters this bad, and that's just the point; you'll never find an altimeter so poor that 3-for-1 redundancy is beneficial.

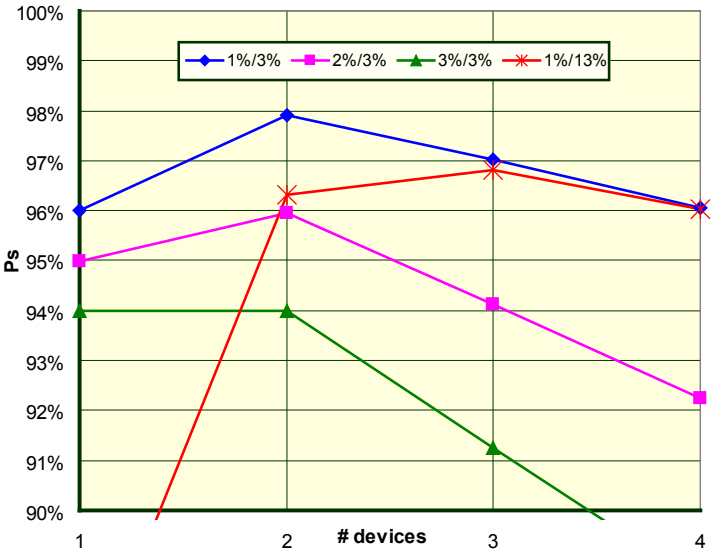


Figure 1: Effect of Redundancy, p_s with devices with $p_E/{}_pL$

Redundant deployment systems are useful with actuators that are more likely to fail by firing late (or not at all) than by firing early, which is believed to be the case with most if not all available devices. It is also required for Level

Continued on page 7

Continued from page 6

Redundancy In Deployment Systems

3 high power certification. However, more is not always better; redundancy should generally be limited to 2-for-1 or else it is liable to do more harm than good. This has been shown using arbitrary reliability figures for hypothetical deployment actuators.

It would be an interesting and useful project to gather data on launches, successes, early deployments, and late deployments for the common, commercially available devices. Since the majority of deployment failures, whether early or late, are caused by human error, collecting those would be useful as well. Calculations like those above could then be performed with real world reliability figures, producing practical results that would be useful for evaluating the benefits of redundancy and selection of devices. We can already see that, when designing a redundant system, all else being equal it is better to choose a device with a low early fire chance, even at the expense of an increased late or no fire chance (if only we knew which those were.)

About the Author

Joe Avins is a BAR who has been building and flying rockets for about four years now. He has worked his way up from skill level 1 kits to level 1 HPR certification, and is preparing for HPR level 2. He is a member of NAR, NARHAMS, and MDRA. In the real world he is an electrical systems engineer in the space industry, designing and building satellites for NASA, the US Air Force, and commercial customers. He currently lives with his family, dog, and cats in West Virginia.