Deciding How Conservative a Designer Should Be: Simulating Future Tests and Redesign

Nathaniel B. Price[1], Taiki Matsumura[2], Raphael T. Haftka[3], Nam H. Kim[4]
University of Florida, Gainesville, Florida, 32601

Nomenclature

σ	=	true stress
σ_{meas}	=	measured stress
σ_{calc}	=	calculated stress
e_{meas}	=	error in measured stress
e_{calc}	=	error in calculated stress
σ_{calc}^{upd}	=	updated stress calculation based on measured stress
θ	=	calibration factor for calculation
S_{ini}	=	initial safety factor
S_{re}	=	redesign safety factor
S_L	=	lower limit for acceptable safety factor
S_U	=	upper limit for acceptable safety factor
A_1	=	initial cross sectional area (before redesign)
A_2	=	cross sectional area after redesign
$E(A)$	=	mean area after redesign
P_{re}	=	probability of redesign
$\bar{P}_{re}$	=	constraint on probability of redesign

I. Introduction

For structural design, it makes sense that designers want to have as small a safety factor as possible in order to save mass. However, since the regulatory bodies, such as the FAA, usually require certification tests to demonstrate that a structure satisfies the required level of safety, a small safety factor may increase the risk of failing certification tests. Because of the fact that the required safety factors are determined only on the basis of flight safety, it is manufacturers' responsibility to balance the performance and the risk of failing certification.

Probabilistic design is one way of assessing risks in a quantitative manner using probability of failure by modeling uncertainty as probability distributions [1-3]. There have been several studies on quantifying the effect of tests as a process of uncertainty reduction by using probabilistic approaches [4, 5]. Villanueva et al. [6] proposed a method that evaluates the risk of failing a certification test followed by redesign, i.e., probability of having redesign. In this study, they modeled an error in design calculation as a random variable and viewed different error realizations as corresponding to different possible futures. A remarkable feature is that the method works in conjunction with safety-factor based design as it can limit the use of a probabilistic approach only to assessing the reliability of the design that is obtained from safety-factor based approach.

Matsumura et al. [7] extended the method by incorporating it into a design optimization framework that enables us to tradeoff the expected performance of a structure in the future against the probability of having redesign. Furthermore, Villanueva et al. [8] introduced a framework that optimizes an initial design and redesign rules simultaneously to get an even better tradeoff solution. As a conclusion of the study in Ref. [8], it is observed that to minimize mass, the best strategy is to start with a conservative design (initially heavier structure) and redesign it to reduce the mass only when the test discovers that the design is overly conservative.

In this paper, we focus our efforts on investigating how different redesign strategies, such as redesign for performance as being a conservative design approach and redesign for safety as being an un-conservative design approach, influence the final design outcomes. We examine the effects of underlying uncertainties, including errors

---

[1] Graduate Research Assistant, Mechanical & Aerospace Engineering, AIAA Student Member
[2] Graduate Research Assistant, Mechanical & Aerospace Engineering, AIAA Student Member
[3] Distinguished Professor, Mechanical & Aerospace Engineering, AIAA Fellow
[4] Associate Professor, Mechanical & Aerospace Engineering, AIAA Associate Fellow

in design prediction and test observation. In addition, instead of the Monte Carlo method used for the previous studies, we demonstrate the use of analytical approaches for reducing the computational costs and increasing the accuracy of the tradeoff information.

II. Methods

A. Demonstration Problem Description

The example problem was reduced to the simplest form in order to clearly show the fundamental effects of different redesign strategies. The example is a solid bar with circular cross section subject to uniaxial tension. The design is subject to the aleatory uncertainty in loading and material properties. In addition, the design and testing process is subject to epistemic uncertainty in the calculated stress response and in the measured stress response. The uncertain parameters are defined as shown in Table 1. For simplicity we assume that an experiment is performed to measure stress in the bar rather than strain.

Table 1. Uncertain Parameters

Parameter	Classification	Symbol	Mean, μ	C.O.V	Range	Distribution
Applied Load	Aleatory	P (N)	100	0.20	[-∞, ∞]	Normal
Material Strength	Aleatory	σ_{allow} (MPa)	20	0.12	[-∞, ∞]	Normal
Calculation Error	Epistemic	e_{calc} (%)	0	Infinity	[-0.30, 0.30]	Uniform
Measurement Error	Epistemic	e_{meas} (%)	0	Infinity	[-0.10, 0.10]	Uniform

B. Deterministic Design & Redesign Procedure

Deterministic design optimization (DDO) is performed to minimize mass, or equivalently the cross sectional area, as shown in Eq. (1) where A_1 is the cross sectional area of the bar, σ_{allow} is the yield strength, S_{ini} is the safety factor for the initial design, and σ_{calc} is the calculated stress. The calculated stress is equal to P_{limit}/A_1, where P_{limit} is the limit load, and therefore we can calculate the cross sectional area of the minimum weight design explicitly as shown in Eq. (2).

$$\begin{aligned} \min \quad & A_1 \\ \text{s.t.} \quad & \frac{\sigma_{allow}}{S_{ini}} \geq \sigma_{calc} \end{aligned} \tag{1}$$

$$A_1 = \frac{P_{limit} S_{ini}}{\sigma_{allow}} \tag{2}$$

After DDO, a single test is performed and the test will be passed if the apparent safety factor, S_1, is within the upper and lower safety factor limits for redesign, S_L and S_U, as shown in Eq. (3).

$$S_L \leq S_1 \leq S_U \text{ where } \mathrm{S}_1 = \sigma_{allow} / \sigma_{meas} \tag{3}$$

If the test is failed then redesign must be performed. We consider two different redesign strategies. If the apparent safety factor is too high (i.e $S_1 > S_U$) then the design is too conservative and we redesign to reduce mass. On the other hand, if the apparent safety factor is too low (i.e. $S_1 < S_L$ then the design is unsafe and we redesign to improve safety. The measured stress response is more accurate than the calculated stress and therefore we can update our calculation using this new information before performing redesign. The simplest method is to update using the ratio of calculated to measured stress, θ, as shown in Eq. (4). If redesign is performed we calculate the cross sectional area of the design after redesign A_2 as shown in Eq. (5) where we introduce the safety factor for redesign S_{re} that may be different than our initial safety factor.

$$\sigma_{calc}^{upd} = \sigma_{calc,2}\theta \text{ where } \theta = \sigma_{meas} / \sigma_{calc} \tag{4}$$

$$A_2 = \frac{P_{limit} S_{re} \theta}{\sigma_{allow}} \tag{5}$$

C. Stochastic Simulation of Future Tests Followed by Possible Redesign

There is epistemic uncertainty (error) in the stress calculation and also in the stress measurement. If we assume we have some prior knowledge at the design stage of these errors then simulating future tests simply becomes an uncertainty propagation problem. The required knowledge of these error distributions or error ranges may be based on previous experience or expert opinion. The calculation and measurement errors are epistemic in nature in that they each have a single true value that is unknown. If we know the error, e_{calc}, in the calculated stress, σ_{calc}, then we can obtain the true stress before redesign, $\sigma_{true,1}$, as shown in Eq. (6). Similarly, if we know the error, e_{meas}, in the measured stress, σ_{meas}, we can also obtain the same true stress as shown in Eq. (7).

$$\sigma_{true,1} = \sigma_{calc}\left(1 - e_{calc}\right) \tag{6}$$

$$\sigma_{true,1} = \sigma_{meas}\left(1 - e_{meas}\right) \tag{7}$$

We can combine these two equations to predict the test result using the stress calculation and the errors as shown in Eq. (8).

$$\sigma_{meas} = \frac{\sigma_{true,1}}{1 - e_{meas}} = \sigma_{calc}\left(\frac{1 - e_{calc}}{1 - e_{meas}}\right) \tag{8}$$

We model the epistemic errors using uniform distributions as described in Table 1. Assuming we know the calculation and measurement error distributions we can simulate a future test by sampling each of the error distributions and substituting into Eq. (8). For n pairs of error samples we obtain n possible futures. In each possible future we determine if redesign will be performed and calculate the true probability of failure before and after redesign. The true reliability index before redesign can be calculated as shown in Eq. (9) where the expected value and variance of the true stress are calculated as shown in Eq. (10) and (11). The true probability of failure before redesign can be calculated from the reliability index as shown in Eq. (12). Similar expressions can be obtained for reliability index and probability of failure after redesign by substituting the true stress after redesign, $\sigma_{true,2}$, for the true stress before redesign. The expression for the true stress after redesign is given in Eq. (13). Note that if there is no measurement error then the calculated stress after redesign is equal to the true stress.

$$\beta_1 = \frac{E\left(\sigma_{allow}\right) - E\left(\sigma_{true,1}\right)}{\sqrt{\mathrm{Var}\left(\sigma_{allow}\right) + \mathrm{Var}\left(\sigma_{true,1}\right)}} \tag{9}$$

$$E\left(\sigma_{true,1}\right) = \frac{E\left(P\right)}{A_1}\left(1 - e_{calc}\right) \tag{10}$$

$$\mathrm{Var}\left(\sigma_{true,1}\right) = \frac{\mathrm{Var}\left(P\right)}{A_1^2}\left(1 - e_{calc}\right)^2 \tag{11}$$

$$P_{f,1} = \Phi\left(-\beta_1\right) \tag{12}$$

$$\sigma_{true,2} = \sigma_{calc,2}\left(1-e_{calc}\right) = \frac{\sigma_{calc}^{upd}}{\theta}\left(1-e_{calc}\right) = \sigma_{calc}^{upd}\left(1-e_{meas}\right) \tag{13}$$

We can model the redesign process analytically by introducing an indicator function I that is equal to one if redesign is performed and equal to zero otherwise. The equation for the indicator function is given in Eq. (14) where we use Heaviside step functions H. Using the indicator function we can combine the expressions from before and after redesign into single expressions for cross sectional area and probability of failure as shown in Eq. (15) and (16) where we use the subscript 1 to indicate values before redesign and subscript 2 to indicate values after redesign. These expressions have both deterministic and stochastic inputs. The deterministic inputs are the initial safety factor S_{ini}, the lower and upper limits for acceptable safety factors S_L and S_U, and the redesign safety factor S_{re}. The stochastic inputs are the calculation error e_{calc} and the measurement error e_{meas}. We can calculate the expected values for area and probability of failure as a function of the deterministic inputs by multiplying by the joint pdf of the errors and integrating over the range of possible errors. Since the errors in calculation and errors in measurement are independent we calculate the joint pdf as shown in Eq. (17). For given design and redesign rules (deterministic inputs) we calculate the probability of redesign, expected area (mass) after redesign, and expected probability of failure after redesign as shown in Eq. (18), (19), and (20).

$$I = \mathcal{H}\left(S_L - S_1\right) + \mathcal{H}\left(S_1 - S_U\right) \tag{14}$$

$$A = \left(1-I\right)A_1 + IA_2 \tag{15}$$

$$P_f = \left(1-I\right)P_{f,1} + IP_{f,2} \tag{16}$$

$$p\left(e_{calc}, e_{meas}\right) = p\left(e_{calc}\right)p\left(e_{meas}\right) \tag{17}$$

$$P_{re} = E\left(I\right) = \iint I\left(e_{calc}, e_{meas}\right)p\left(e_{calc}, e_{meas}\right)de_{calc}de_{meas} \tag{18}$$

$$E\left(A\right) = \iint A\left(e_{calc}, e_{meas}\right)p\left(e_{calc}, e_{meas}\right)de_{calc}de_{meas} \tag{19}$$

$$E\left(P_f\right) = \iint P_f\left(e_{calc}, e_{meas}\right)p\left(e_{calc}, e_{meas}\right)de_{calc}de_{meas} \tag{20}$$

D. Optimization of Safety factors & Redesign Rules

For an individual designer, the design problem is deterministic and safety factors are determined by regulations and additional company safety margins. However, a design group may want to select design and redesign rules while complying with regulations for a group of structural components so as to balance performance against the probability of redesign and the additional development costs. Here we illustrate this with a multiobjective optimization problem of selecting the safety factors and redesign window to minimize the mean mass after redesign while also minimizing probability (risk) of redesign. The constraint on probability of redesign is varied to capture the Pareto front for performance (mass) versus risk of redesign. A constraint is placed on the mean probability of failure to ensure all design strategies on the Pareto front will achieve a target reliability. This leads to the optimization problem in Eq. (21). In practice we optimize the variables S_{ini}, S_L/S_{ini}, S_U/S_{ini}, and S_{re}/S_{ini} because it is convenient to set the upper bound S_L/S_{ini}=1 and lower bound S_U/S_{ini}=1 to ensure the initial safety factor satisfies our redesign criteria.

$$
\begin{aligned}
\min \quad & E(A) \\
\text{s.t.} \quad & E(P_f) \le 1\times10^{-5} \\
& P_{re} \le \overline{P} \\
& 0.80 \le S_{ini} \le 1.60 \\
& 0.50 \le S_L / S_{ini} \le 1.00 \\
& 1.00 \le S_U / S_{ini} \le 1.50 \\
& 0.75 \le S_{re} / S_{ini} \le 1.75
\end{aligned}
\tag{21}
$$

III. Results

A. Discrete Error Simulation: 2 Possible Futures

To compare the fundamental differences between redesign for safety and redesign for performance we consider the trivial example where we have only 2 possible futures: e_{calc}=+30%, e_{meas}=0% and e_{calc}=-30%, e_{meas}=0%. From a designers perspective this scenario could correspond to a situation where we know the magnitude of the error in our calculation or simulation but can't determine, or are missing information related to, the sign of the error. We assume the error in our test is negligible in comparison to our calculation error. Furthermore, for this illustrative example we assume we are willing to accept a 50% risk of redesign. In this situation we must make a decision to start with a conservative initial design (high S_{ini}) and redesign if the test reveals we have been too conservative (S_I>S_U) or to start with an un-conservative initial design (low S_{ini}) and redesign if the test reveals our design is unsafe (S_I<S_L). For this comparison we consider two optimization problems. In the first problem we redesign for performance to correct a design that is too conservative and therefore we set $S_L/S_{ini}=-\infty$ and set $S_U/S_{ini}=1$ to fix the probability of redesign at 50%. In the second optimization problem we redesign to improve a design that is unsafe and therefore we set $S_L/S_{ini}=1$ and set $S_U/S_{ini}=\infty$.

In each problem we must perform optimization to determine the initial safety factor S_{ini} and the redesign safety factor S_{re}. Since we have simplified the optimization to only two variables we can visualize the solution as shown in Figure 1. We can see that when we redesign for performance the constraint becomes nearly vertical around S_{ini}=1.45 because without redesigning to improve safety we will not be able to satisfy our constraint on mean probability of failure if we start with a safety factor below this threshold. This value of S_{ini} corresponds to a probability of failure that is very close to our constraint of 1e-5 as shown in Figure 3. We note that the mean probabilities of failure before and after redesign are very close in the figure because the mean changes by about a factor of 2 which is barely visible on the log scale. On the other hand when we redesign to improve safety we can continue to decrease S_{ini} as long as we increase S_{re} as shown in the plot of the constraint contour in Figure 1. Since we are redesigning a design with a high probability of failure it is very influential on the mean as shown in Figure 3. Based on the histogram of the probability of failure we can determine that the optimum strategy in both cases is to select S_{ini} and S_{re} so that the one design that is not redesigned remains near the constraint and the other design is corrected so as to achieve the same reliability.

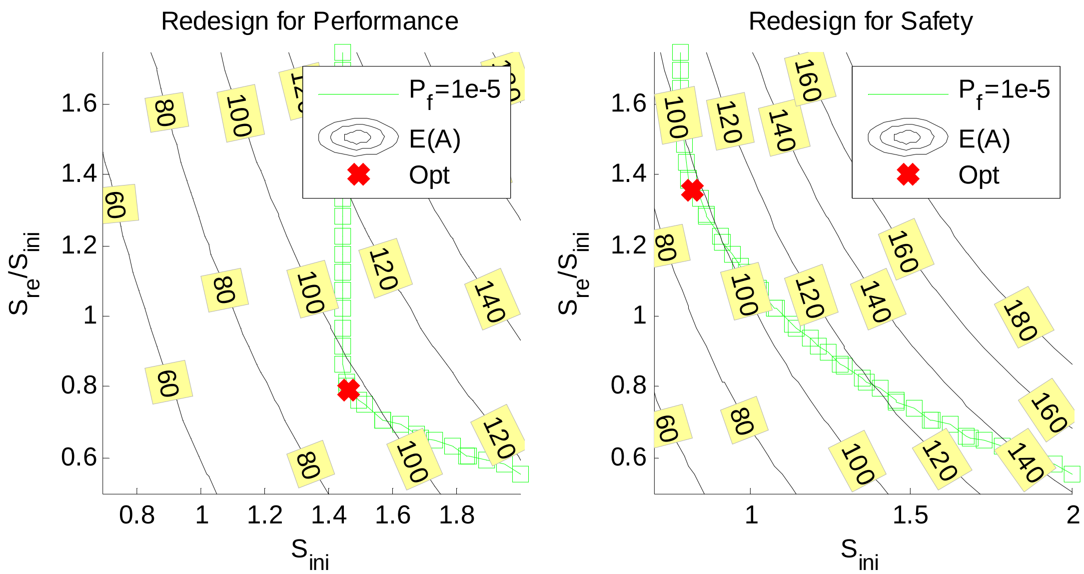

Figure 1. Visualization of optimization problem for simulation of 2 possible futures: +30% calculation error and -30% calculation error. The optimum initial safety factor and redesign safety factor corresponding to minimum mean mass in the future are shown by red x. Left: Redesign for performance; Right: Redesign for safety

The fundamental question we would like to answer is whether one redesign strategy will result in a lower mean mass (area) in the future. However, as shown in Figure 2 the mass distributions after redesign appear identical. The comparison in Table 2 shows that both redesign strategies achieve the same mean mass after redesign. Based on this simplified example we might incorrectly conclude that both redesign strategies are always equivalent. However, if we consider a continuous error distribution then the mean area after redesign for redesign for safety is about 0.6% higher. A much larger difference in mean mass can be seen if we introduce measurement error as shown in the next example.

Table 2. Comparison of redesign strategies for simulation of 2 possible futures

Purpose of Redesign	Mean Area After Redesign (mm^2)	Mean Probability of Failure	Probability of Redesign
Reduce Mass	96.09	1e-5	0.50
Improve Safety	96.09	1e-5	0.50

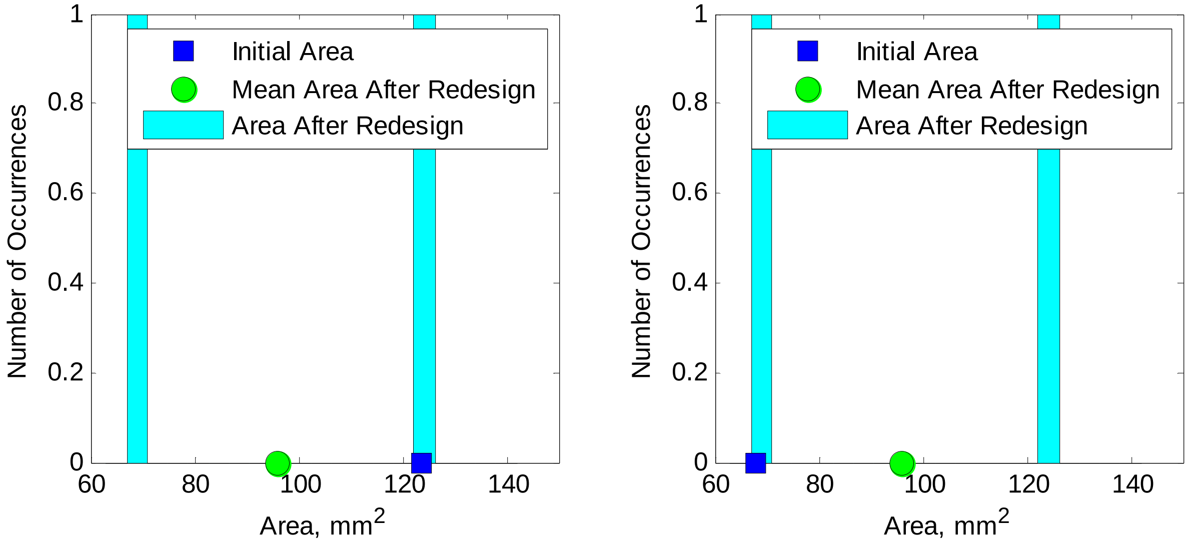

Figure 2. Mass distribution for simulation of 2 possible futures. Left: Redesign for performance; Right: Redesign for safety

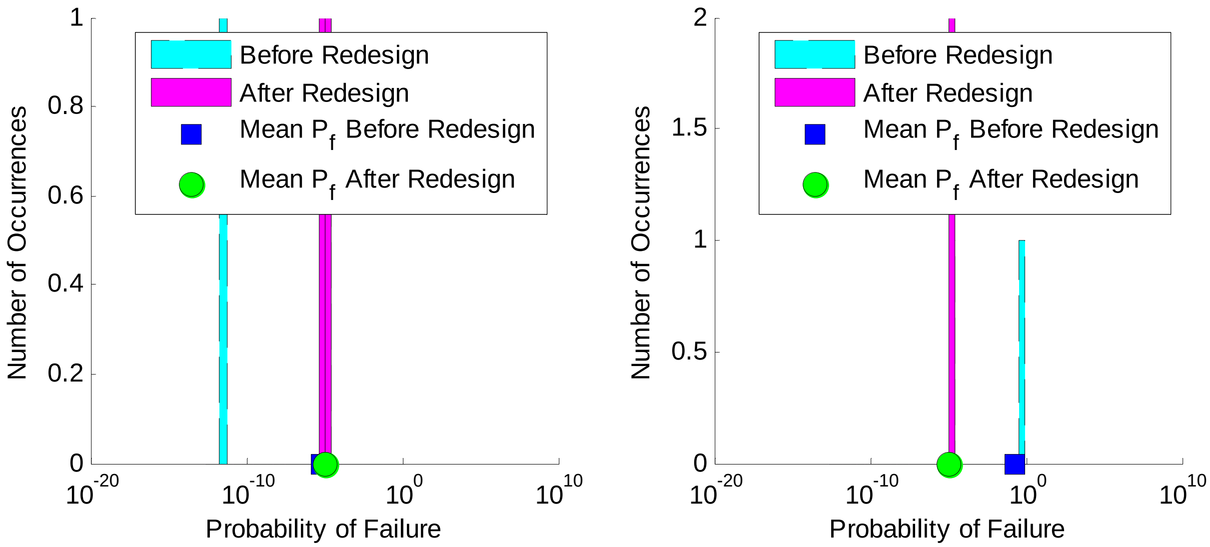

Figure 3. Probability of failure distribution for simulation of 2 possible futures. Left: Redesign for performance; Right: Redesign for safety

B. Discrete Error Simulation: 4 Possible Futures

In this example we extend the problem from the previous example to include 4 possible futures. We consider two levels of calculation error, +30% or -30%, and two levels of measurement error, +10% and -10%, for a total of four possible futures. When we introduce measurement error the updated (calibrated) model after redesign is no longer free from error. After redesign the calculation error is replaced with the smaller measurement error. Under these conditions there is a clear benefit to starting with a conservative initial design and redesigning to reduce mass rather than redesigning to improve safety. As shown in Table 3 the mean mass after redesign is approximately 2% higher if we start with a less conservative initial design and redesign to improve safety. In Table 4 we compare the mass and probability of failure in each of the four possible futures. We can see that the initial reduction in area by starting with an unconservative design (55.5mm^2) is outweighed by the required increase in mass to restore safety.

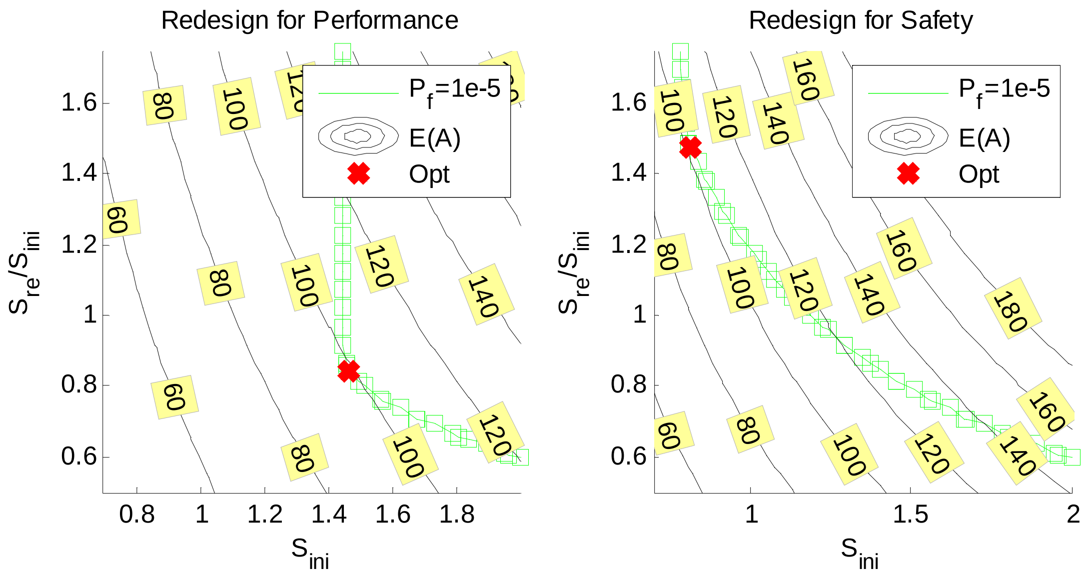

Figure 4. Visualization of optimization problem for simulation of 4 possible futures. The optimum initial safety factor and redesign safety factor corresponding to minimum mean mass in the future are shown by red x. Left: Redesign for performance; Right: Redesign for safety

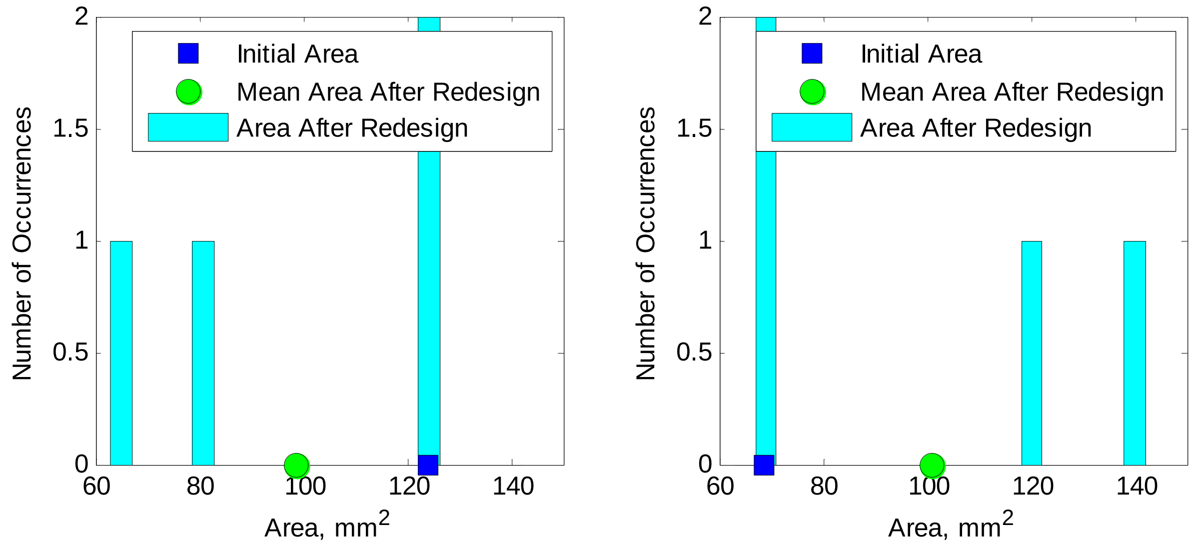

Figure 5. Mass distribution for simulation of 4 possible futures. Left: Redesign for performance; Right: Redesign for safety

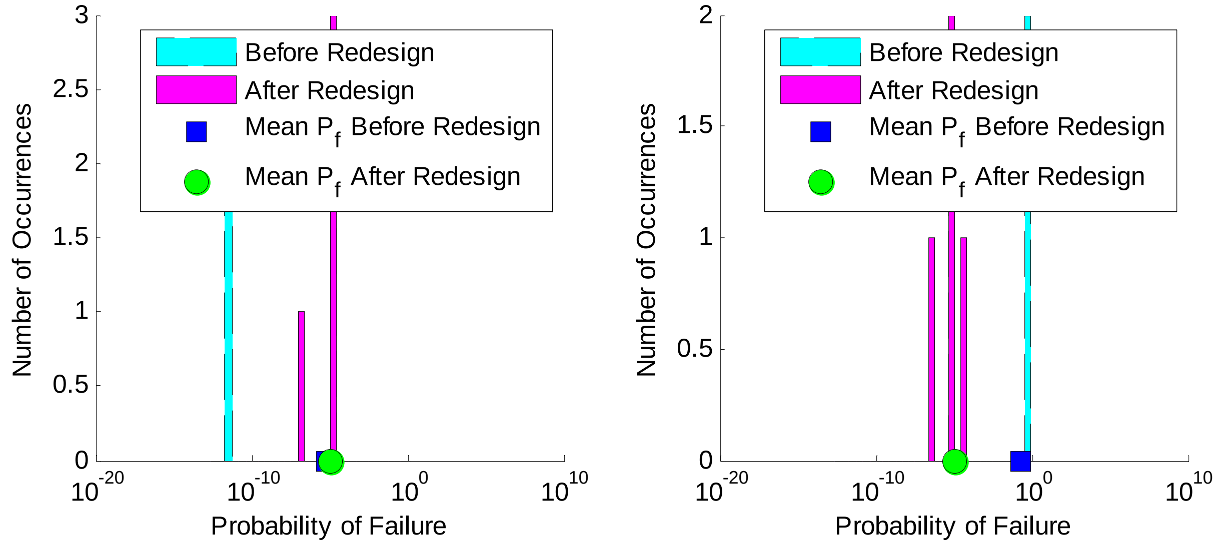

Figure 6. Probability of failure distribution for simulation of 4 possible futures. Left: Redesign for performance; Right: Redesign for safety

Table 3. Comparison of redesign strategies for simulation of 4 possible futures

Purpose of Redesign	Mean Area After Redesign (mm^2)	Mean Probability of Failure	Probability of Redesign
Reduce Mass	98.84	1e-5	0.50
Improve Safety	101.05	1e-5	0.50

Table 4. Comparison of change in area and probability of failure for each of the four possible futures under different redesign strategies

Error [e_{calc}, e_{meas}]	Area Before Redesign (mm^2)		Area After Redesign (mm^2)		Probability of Failure Before Redesign		Probability of Failure After Redesign	
	Reduce Mass	Improve Safety	Reduce Mass	Improve Safety	Reduce Mass	Improve Safety	Reduce Mass	Improve Safety
[-30,-10]	124.00	68.50	124.00	120.24	1.25e-5	0.355	1.25e-5	2.65e-5
[30,-10]	124.00	68.50	66.31	68.50	2.47e-12	6.65e-6	1.49e-5	6.65e-6
[-30, 10]	124.00	68.50	124.00	146.96	1.25e-5	0.355	1.25e-5	1.69e-7
[30, 10]	124.00	68.50	81.04	68.50	2.47e-12	6.65e-6	9.16e-8	6.65e-6
Mean	**124.00**	**68.50**	**98.84**	**101.05**	**6.27e-6**	**0.178**	**1.00e-5**	**1.00e-5**

C. Continuous Error Distribution Simulation

In a typical design scenario it is often more reasonable to model the error distributions as continuous distributions. A comparison of the tradeoff curves with calculation and measurement error for both redesign strategies indicates it is better to redesign for performance in order to achieve a smaller mean mass as shown in Figure 7. To better understand this result we consider the points on the tradeoff curve corresponding to 20% redesign. For these points the difference in mean mass after redesign is about 3% (109.6mm^2 vs. 106.4mm^2). Plots of the area distributions and probability of failure distributions for points on the tradeoff curves corresponding to a probability of redesign of 20% are shown in Figure 8 and Figure 9. From the histograms of the mass distributions we can see that when redesign is performed to reduce mass the designs that are redesigned are revealed to be very conservative and a large reduction in mass can be achieved. This reduction can be as large as reducing the cross sectional area from 114mm^2 before redesign to 65mm^2 after redesign. On the other hand, when we redesign to improve safety the redesign the maximum change in area due to redesign is from 108mm^2 to 138mm^2. This change in mass is related to the change in probability of failure required under the different redesign strategies. As can be seen from the probability of failure distributions, redesign for performance increases the probability of failure for a single design by about five orders of magnitude (10^{-10} to 10^{-5}). However, when we redesign to improve safety the change in probability of failure for a single design is about one order of magnitude and the change in mass is therefore also much smaller.

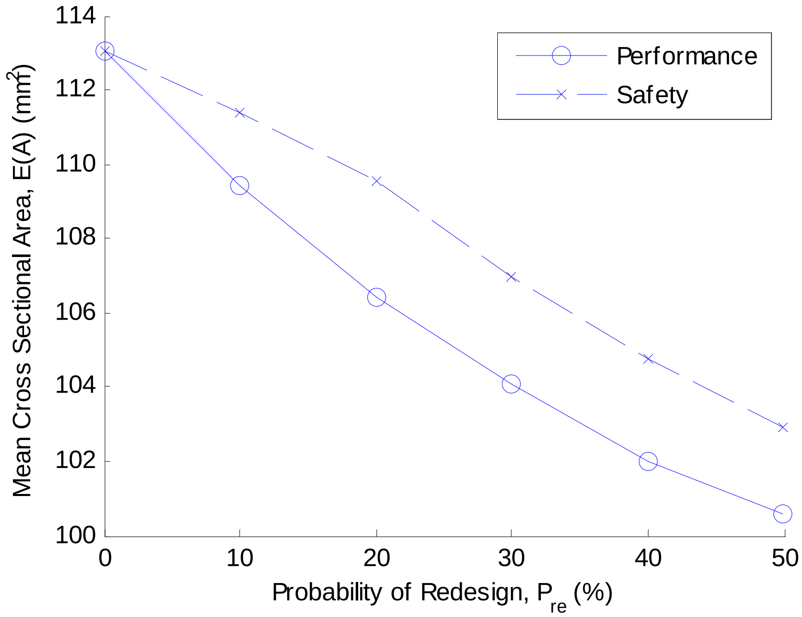

Figure 7. Tradeoff curve for mean mass versus probability of redesign

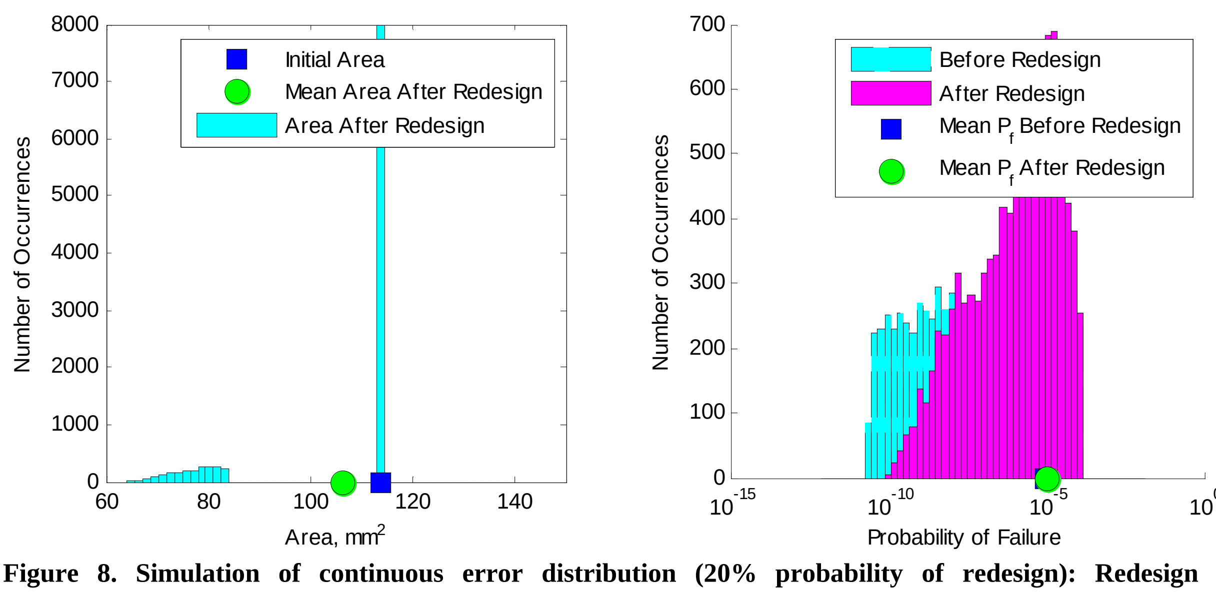

Figure 8. Simulation of continuous error distribution (20% probability of redesign): Redesign for performance

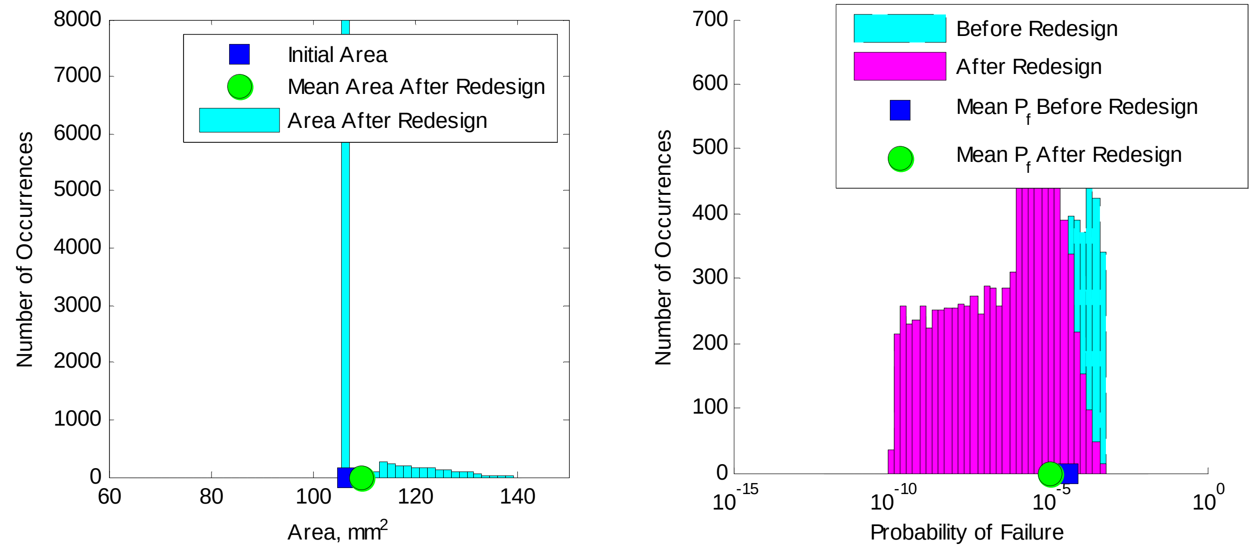

Figure 9. Simulation of continuous error distribution (20% probability of redesign): Redesign for safety

IV. Discussion & Conclusion

When considering the tradeoff between performance increases from mass reduction and the substantial costs that can be associated with redesign, a company wishes to select the design and redesign rules in order to achieve the best performance on average for an acceptable risk of redesign. In this situation the company should select design and redesign rules that start with a conservative design and redesign if the design is revealed by the test to be too conservative. This redesign strategy will result in better performance on average (lower mean mass) and will meet the same reliability constraint on mean probability of failure as other redesign strategies.

It is interesting to consider that this same decision of whether to start with a conservative design or a less conservative initial design may result in a different conclusion if considered from the designer's perspective. If we consider the modes of the mass distributions after redesign for redesign for performance versus redesign for safety then the designer will most likely be stuck with a heavier design if he chooses to start with a conservative initial design. In addition, in some instances the test will reveal that the designer has been much too conservative and the design after redesign will have substantial mass reduction. This result may reflect badly on a designer because the test has revealed his initial design to be very poor. On the other hand, if the designer chooses to start with a less conservative design the most likely outcome as indicated by the mode is that he will have a lighter design. This strategy of redesign for safety has the added benefit that if his design fails the test he may only have to slightly modify the design which would result in a slight increase in mass and reliability. Under this scenario the design may fail the test by being unsafe but the required change in his or her design would be smaller which one may consider to indicate his design was very good because it only needed a minor change. However, over many different designs this strategy will not be in the company's best interest because the average performance of designs will be worse.

References

[1] Youn, B. D., and Choi, K. K., "Selecting probabilistic approaches for reliability-based design optimization," *AIAA Journal,* Vol. 42, No. 1, 2004, pp. 124-131.

[2] Acar, E., Haftka, R. T., and Johnson, T. F., "Tradeoff of uncertainty reduction mechanisms for reducing weight of composite laminates," *Journal of Mechanical Design,* Vol. 129, No. 3, 2007, pp. 266-274. doi: Doi 10.1115/1.2406097

[3] Yao, W., Chen, X. Q., Luo, W. C., van Tooren, M., and Guo, J., "Review of uncertainty-based multidisciplinary design optimization methods for aerospace vehicles," *Progress in Aerospace Sciences,* Vol. 47, No. 6, 2011, pp. 450-479.
doi: DOI 10.1016/j.paerosci.2011.05.001

[4] Acar, E., Haftka, R. T., and Kim, N. H., "Effects of Structural Tests on Aircraft Safety," *AIAA Journal,* Vol. 48, No. 10, 2010, pp. 2235-2248.

[5] Sankararaman, S., McLemore, K., Mahadevan, S., Bradford, S. C., and Peterson, L. D., "Test Resource Allocation in Hierarchical Systems using Bayesian Networks," *AIAA Journal,* Vol. 51, No. 3, 2013, pp. 537-550.

[6] Villanueva, D., Haftka, R. T., and Sankar, B. V., "Including the Effect of a Future Test and Redesign in Reliability Calculations," *AIAA Journal,* Vol. 49, No. 12, 2011, pp. 2760-2769.
doi: Doi 10.2514/1.J051150

[7] Matsumura, T., and Haftka, R. T., "Reliability Based Design Optimization Considering Future Redesign With Different Epistemic Uncertainty Treatments," *Journal of Mechanical Design,* Vol. 135, No. 9, 2013, pp. 091006-091014.
doi: 10.1115/1.4024726

[8] Villanueva, D., Haftka, R.T. , Sankar, B.V., "Accounting for Future Redesign in the Optimization of an Integrated Thermal Protection System," *14th AIAA Non-Deterministic Approaches Conference*, Honolulu, Hawaii, 2012.