Reliability Engineering and System Safety 124 (2014) 56–67

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Accounting for future redesign to balance performance and development costs

D. Villanueva [a,b,*], R.T. Haftka [a], B.V. Sankar [a]

[a] University of Florida, P.O. Box 116250, Gainesville, FL 32611, United States
[b] Ecole des Mines de Saint-Etienne, 158 cours Fauriel, 42023 Saint-Etienne cedex 2, France

ARTICLE INFO

Article history:
Received 23 December 2012
Received in revised form
24 November 2013
Accepted 28 November 2013
Available online 6 December 2013

Keywords:
Future test
Redesign
Two-stage stochastic
optimization

ABSTRACT

Most components undergo tests after they are designed and are redesigned if necessary. Tests help designers find unsafe and overly conservative designs, and redesign can restore safety or increase performance. In general, the expected changes to the performance and reliability of the design after the test and redesign are not considered. In this paper, we explore how modeling a future test and redesign provides a company an opportunity to balance development costs versus performance by simultaneously designing the design and the post-test redesign rules during the initial design stage. Due to regulations and tradition, safety margin and safety factor based design is a common practice in industry as opposed to probabilistic design. In this paper, we show that it is possible to continue to use safety margin based design, and employ probability solely to select safety margins and redesign criteria. In this study, we find the optimum safety margins and redesign criterion for an integrated thermal protection system. These are optimized in order to find a minimum mass design with minimal redesign costs. We observed that the optimum safety margin and redesign criterion call for an initially conservative design and use the redesign process to trim excess weight rather than restore safety. This would fit well with regulatory constraints, since regulations usually impose minimum safety margins.

1. Introduction

Traditionally, aerospace structures have been designed deterministically, employing safety margins and safety factors to protect against failure. After the design stage, most components undergo tests, whose purpose is to validate the model and catch unacceptable designs and redesign them. After production, inspection and manufacturing are done to ensure safety throughout the life cycle. In contrast, probabilistic design considers uncertainties to calculate the reliability, which allows the trade-off of cost and performance.

In recent years, there has been a movement to quantify the effect of uncertainty reduction measures, such as tests, inspection, maintenance, and health monitoring, on the safety of a product over its life cycle. Much work has been completed in the areas of inspection and maintenance for structures under fatigue [1–4]. A study reported by Acar et al. [5] investigated the effects of future tests and redesign on the final distribution of failure stress and structural design with varying numbers of tests at the coupon, element, and certification levels. Golden et al. [6] proposed a method to determine the optimal number of experiments required to reduce the variance of uncertain variables. Sankararaman et al. [7] proposed an optimization algorithm of test resource allocation for multi-level and coupled systems. A method to simultaneously design a structural component and the corresponding proof test considering the probability of failure and the probability of failing the proof test was introduced by Venter and Scotti [8].

Most aerospace components are designed using a computational modeling technique, such as finite element analysis. We expect some error, often labeled as epistemic uncertainty (associated with lack of knowledge), in the modeled behavior. The true value of this error is unknown, and thus we consider this lack of knowledge to lead to an uncertain future. Tests are performed to reduce the error, thus narrowing the range of possible futures through the knowledge gained and the correction of unacceptable futures by redesign.

Previously, Villanueva et al. [9] proposed a method to simulate these possible futures including test and redesign, and studied the effect of a single future thermal test followed by redesign on the initial reliability estimates of an integrated thermal protection system (ITPS). An ITPS is a structure on a reusable launch vehicle that simultaneously provides protection from aerodynamic heating during reentry, while working as a load bearing structure. Monte Carlo sampling of the assumed computational and

* Corresponding author at: University of Florida, P.O. Box 116250, Gainesville, FL 32611, United States. Tel.: +1 3523926780.
E-mail addresses: dvillanu@gmail.com (D. Villanueva), haftka@ufl.edu (R.T. Haftka), sankar@ufl.edu (B.V. Sankar).
URL: http://dianevillanueva.com (D. Villanueva).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.11.013

Nomenclature

d	design variable
e_c	computational error
e_x	experimental error
$f(T)$	probability distribution of the temperature
m	mass per unit area, kg/m^2
p_f	probability of failure, %
r	random variable
S	safety margin
ΔT	change in temperature, K
T	temperature, K

Subscripts

calc	calculated
corr	corrected
ini	initial
L	lower bound
nom	nominal
meas	measured
re	redesign
test	test article
true	true
U	upper bound

experimental errors was used to sample future test alternatives, or the possible outcomes of the future test. Using the future alternatives, the methodology included two methods of calibration and redesign. It was observed that the deterministic approach to calibration and redesign, which acted to restore the original (designed) safety margin, led to a greatly reduced probability of failure after the test and redesign, a reduction that usually is not quantified. A probabilistic approach was also presented, which provided a way to more accurately estimate the probability of failure after the test, while trading off weight against performing additional tests. Matsumura et al. [10] extended the methodology to include additional failure modes of the ITPS.

In this paper we use the reliability estimates of [9] as a building block to show that modeling future redesign provides a company with the opportunity to trade off development costs (test and redesign) and performance (mass) by designing the initial design criteria and the redesign rules. As regulations and tradition drive companies to use traditional deterministic design with safety margins and safety factors, we limit ourselves to deterministic design and redesign processes. The probabilistic approach can be limited to select safety margins and redesign criteria. This is a two-stage stochastic optimization problem [11], a type of problem which has been studied extensively in the area of process planning under uncertainty [12,13]. Here, in the first stage, a decision is made about the initial design before the test (i.e., an initial optimum design is found) and then decisions are taken based on the updated information from the test result (i.e., to redesign or not) in the second stage.

This research fits into a class of studies that have identified measures that are used to engineer safe designs and sought out ways to find an optimal set of safety policies or practices. Möller and Hansson [14] provided a review of safety practices (e.g., safety factor, safety margin, reliability) in engineering and how they increase safety. Aktas et al. [15] used cost and safety optimization to optimize load factors and safety indices considering the initial cost of design and future failure costs based on probability of failure for bridge specifications. Beck et al. [16] presented a method to optimize partial safety factors of the design of a steel beam under epistemic uncertainties in a robust optimization formulation considering costs of failure. In the same vein, we seek to optimize the design and redesign rules considering the outcome of a future test.

The following section of the paper will provide a description of the test problem, the integrated thermal protection system. Though the methods in this paper are focused on this particular example, they can be translated to any example problem in which the uncertainties in the computational model and experiment are quantifiable and the ranges of acceptable safety margins and safety factors are given. In Section 3, the process of test and redesign is described in detail. Section 4 provides a detailed description of the uncertainties considered in this study, and Section 5 describes how these uncertainties are used to obtain a distribution of the probability of failure. In Section 6, the process of simulating the future test and redesign for a single candidate design is described. An illustrative example is provided in Section 7.

2. Integrated thermal protection shield description

Fig. 1 shows the ITPS panel that is studied, which is a corrugated core sandwich panel concept.

The design consists of a top face sheet and webs made up of titanium alloy (Ti–6Al–4V), and a bottom face sheet made up of beryllium. Saffil® foam is used as insulation between the webs. The relevant geometric variables of the ITPS design are also shown on the unit cell in Fig. 1. These variables are the top face thickness (t_T), bottom face thickness (t_B), thickness of the foam (d_S), web thickness (t_w), corrugation angle (θ), and length of unit cell ($2p$). The mass per unit area is calculated using the below equation:

$$m=\rho_T t_T+\rho_B t_B+\frac{\rho_w t_w d_S}{p\ \sin\ \theta} \tag{1}$$

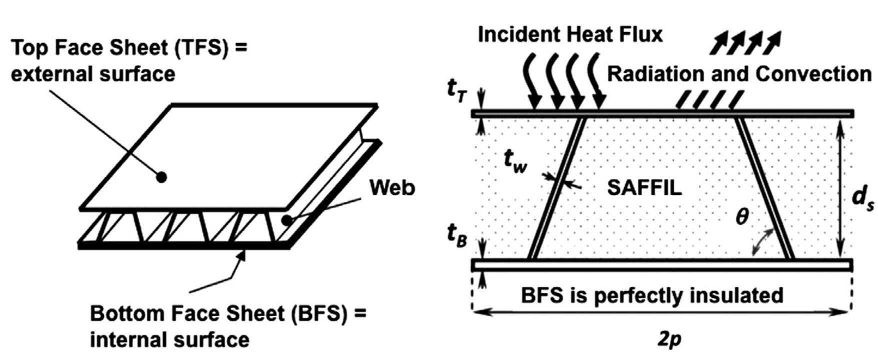

Fig. 1. Corrugated core sandwich panel ITPS concept.