

Design Verification as a Key Deliverable of Function Failure Avoidance

2010-01-0708

Published
04/12/2010Ed Henshall and Felician Campean
University of Bradford, UK

Copyright © 2010 SAE International

ABSTRACT

This paper presents an approach to product design verification in which efficient and effective design verification is a key deliverable of a function failure avoidance approach to engineering. The traditional approach to design verification is discussed. The relative advantages of conducting design verification at different levels within the system hierarchy are identified and the manner in which component level testing can be made representative of usage in the field is illustrated within an automotive case study. The use of small samples sizes, a reduced number of tests and a reduction of testing complexity as a part of effective design verification is explained. The role of computer based models as the basis of virtual testing within design verification is discussed.

INTRODUCTION

When the design of a product is released for production it is important that the design is stable and is not subjected to further change. However, the launch of a complex product like a vehicle is often associated with hectic activity focused on problem resolution as one problem with the product is discovered after another (1). Design changes discovered during the launch phase of a product often result in costly changes to production tools and equipment. It is also often the case that a late design change associated with one product function has a detrimental knock-on effect to other product functions necessitating further design change.

Confidence in a design prior to its release is gained through successful verification of the design in which the design is tested to ensure that it meets its requirements. The late discovery of failure modes despite 'successful' design verification points to an inadequate design verification process. An inadequate design verification is one in which the

design is not subjected fully to the conditions it will meet in customer usage.

The Failure Mode Avoidance (FMA) strategy adopted in recent years by Ford Motor Company (2, 3) ensures efficient design verification. In simple terms FMA is a pragmatic approach influenced by Clausings's (4) definition "reliability is failure mode avoidance" in which potential failure modes are systematically identified and robust countermeasures implemented and verified early in the design process

The detection and elimination of failure modes during product design is a key strategy within Design for Six Sigma (DFSS) (5) i.e. FMA facilitates a DFSS approach to product design and development. The importance of design verification within DFSS can be seen from the fact that almost all of the numerous acronyms that different organisations use to describe their particular 'brand' of DFSS end with 'V' recognising verification as the conclusion of the DFSS process.

The fact that an FMA approach to product design and development can both be used to identify all potential failure modes, establish effective countermeasures and facilitate efficient design verification is not coincidental. The factor effects that can lead to failure and require countermeasures are the very same factor effects that need to be included within an effective design verification regime if it is to demonstrate the effectiveness of the countermeasures through the absence of failure. The information flow in FMA relating to failure modes and their countermeasures can also help to drive such verification lower down the systems hierarchy. This paper will look how efficient and effective design verification is a key deliverable of a function failure avoidance approach to engineering.

CRITIQUE OF THE TRADITIONAL APPROACH TO DESIGN VERIFICATION

Traditionally design verification has been conducted through a series of hardware tests and in conducting such tests two questions drive the manner of the verification. These questions are:

- How many parts do I have to test?
- How long do I have to test them for?

The answer to the first question is usually determined by the required level of statistical confidence and reliability with the answer to the second question determined by the time taken to achieve failure of the system given the test conditions. Generally the answers to both questions are not welcome.

A reasonable level of statistical confidence and reliability necessitates a relatively large sample size, usually several tens of sample parts (6). Large sample sizes are required because a random sample that is representative of the population is required i.e. one where the effect of all sources of variation in the population are present in the sample. For reasons of cost and time, particularly when testing is focused at the vehicle level or subsystem level, it is generally the case that only a small number of samples are available and the statistical basis of the sample size is compromised.

The length of a verification test is generally dependent on the type of testing that is conducted. Testing can be conducted for a predetermined time (the bogey), until failure occurs or until the performance of the item being tested degrades such that it falls below a predetermined level. The measure of success in bogey testing is that, either all samples do not fail, or less than a predefined percentage of failures occur. In testing to failure the test is conducted for a sufficient length of time such that as many of the samples fail as possible. In degradation testing the test is conducted for a sufficient length of time so that the performance falls below the predetermined level or the time when this level will be reached can be reliably predicted. Generally speaking testing to failure and degradation testing requires considerably longer test lengths than bogey testing. Test length typically tends to be based on experience, for example, relating it to what has been done historically or how long a similar design has survived in the field before failing. In testing to failure and degradation testing it is important that the conditions under which failure will occur are represented in the test.

Given that large sample sizes and long tests are often expensive a number of strategies have been adopted to reduce sample size and/or test length (7). These include:

Extended/Reduced Bogey Testing: Trading off sample size and test length with either smaller sample sizes being used

with a longer test length or a smaller test length being employed with a larger sample size.

Bayesian Testing: Allowing a smaller sample size to be used by the inclusion in the test data of information from previous tests or field failure data.

Accelerated Testing: Subjecting a design to stresses higher than those it will experience in the field to cause the system to fail earlier than it would in the field thereby reducing test length.

Tail Testing: Using knowledge of the failure distribution to select samples that are more likely to fail to allow a reduction in both sample size and test time.

Generally speaking the approach that is taken in devising strategies to increase the efficiency of design verification testing focuses on the statistical basis of the test rather than on the engineering of the system under test (6, 7). While this allows reduction in sample size and/or test length it may compromise the test from an engineering perspective with, for example, the 'more efficient' test conditions being less representative of the conditions that the design will be subjected to in the field. For example, in accelerated testing having stress levels higher in a test than those experienced in the field might cause failure modes to occur in the test which will not occur in the field.

This focus on the underlying statistical foundations of design verification at the expense of the engineering of the design being tested is reinforced by the recommendation common in the literature (6) that design verification should be the responsibility of an organisation other than engineering. While it is important that any design verification needs to be conducted in an impartial and objective manner if it is divorced from engineering there is a danger that best use will not be made of valuable information gained during the design of a system.

The approach to design verification based on FMA discussed in this paper allows verification testing to be conducted in an objective manner from the engineering perspective. As has been noted an FMA approach to design verification also leads to testing efficiencies one of which is discussed next.

DESIGN VERIFICATION AND THE SYSTEMS HIERARCHY

In the automotive sector design verification often focuses on the testing of vehicles since it is thought that such tests are representative of the use of the product in the field. Unfortunately vehicle level testing is both expensive and, because it is dependent on the availability of prototype vehicles which are representative of the final production vehicle, necessarily conducted late in the product design

**Table 1. Relative advantages/disadvantages of conducting design verification at different levels of systems hierarchy
(Disadvantages in italics)**

Vehicle	Subsystem	Component
• Representative of usage in field • <i>Expensive</i> • <i>Late in program</i> • <i>Little latitude for change</i> • <i>Not always clear what is being tested</i> • <i>Design change has knock-on effect</i>	• <i>Not as representative of usage in field as vehicle</i> • Not expensive • Not too late in program • Some latitude for change • Clear what is being tested • <i>Design change has knock on effect</i>	• <i>Not representative of usage in field</i> • Cheap • Early in program • Good latitude for change • Clear what is being test • Design change has smaller knock on effect

process. Also it is not always clear what is being tested in a vehicle test. For example, when a vehicle is driven on a proving ground while it might be argued that all of the many thousands of components that make up the vehicle are under test it is extremely unlikely that all components will be subject to all combinations of stresses they will potentially be subjected to in customer use.

Despite the belief that the testing of subsystems and components in isolation of the vehicle is less representative of customer usage than vehicle level testing conducting design verification testing at sub-system and component levels has a number of advantages as [table 1](#) illustrates.

<[table 1](#) here>

FMA can overcome the disadvantage of component level testing not being representative of usage in the field thus making testing at this level an attractive focus for design verification. The way in which FMA overcomes this disadvantage is demonstrated in the case study that follows. The case study illustrates how an FMA approach to engineering facilitates efficient and effective design verification.

CASE STUDY

The use of the Failure Mode Avoidance process to establish effective and efficient design verification is illustrated using a case study based on a vehicle engine cooling system (8, 9). A new front engine cover assembly ([figure 1](#)) has been designed which integrates the engine coolant transfer path within it so achieving packaging space and cost efficiencies.

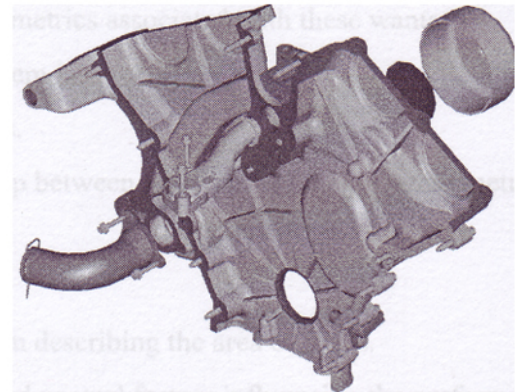


Figure 1. Front Engine Cover

In focusing on design verification of the front engine cover assembly it is assumed that the FMA process has been used as an integral part of the design of this sub-system. Design verification is part of Step 4 in the FMA process described by the authors (10) and summarised in [table 2](#) which lists the primary FMA engineering tools used in each step.

<[table 2](#) here>

The case study is used to demonstrate how the information flow between the FMA tools helps to establish effective and efficient design verification. The case study focuses on one function failure mode of the sub-system and by way of example takes a narrow sequential slice of information through the tools noting that in reality the tools are used in an iterative manner (10).

The case study focuses on coolant transfer within the engine cover assembly with the function of interest being:

Transfer coolant at specified rate

This function supports the higher level vehicle function of maintaining engine temperature within its operating range.