Property Coverage for Quality Assessment of Fault Tolerant or Fail Safe Systems

F.M. Gonçalves, M.B. Santos, I.C. Teixeira, and J.P. Teixeira
IST/INESC-ID, Rua Alves Redol, 9, 1000-029 Lisboa, Portugal
jct@inesc-id.pt

Abstract

In the design environment, system properties, such as fault tolerance and safe operation, need to be demonstrated in new product development of safety-critical systems. The onus of the proof is by no means trivial, and the associated computational costs can be overwhelming. In this paper, a novel quality metrics is introduced, Property Coverage (PC), which allows, with affordable computational effort, to have a measure of the degree of confidence within which the Property under evaluation holds. The proposed method uses fault sampling, and enables PC evaluation with limited fault list sizes. The methodology and associated metrics are ascertained through a case study, an ASIC for a safety-critical gas burner control system, recently certified to be compliant to EN 298 safety standard.

1. Introduction

New product development of safety-critical systems require *safe operation*. Hence, for harm prevention, system incorrect behavior (in the presence of disturbances) must not propagate beyond a pre-defined boundary; instead, the system must be driven to a safe state of operation within a specified period of time. Usually, some degree of *fault tolerance* is required, i.e., the system must continue to operate according to specifications, in the presence of assumed disturbances. The demonstration, in the design environment, that such properties hold is not trivial, and can lead to unacceptable Non-Recurring Engineering (NRE) costs. Property Coverage (PC), allows, with affordable computational effort, to have a measure of the degree of confidence within which the Property under evaluation holds.

2. Problem Statement

Assume that the system functionality, $G(X,t)$, has been validated (by simulation) according to specifications ($X = \{x_1 x_2 \ldots x_n\}$ is the input vector space and t the time variable). The system output vector space $Y = \{y_1 y_2 \ldots y_m\}$ is such that $Y(t) = G \cdot X(t)$. Within the set of output variables, $Y=\{y_1 y_2 \ldots y_m\}$, two sub-sets can be identified: Y_F, associated with the key functionality, and Y_C, the set of *critical variables* ($Y = (Y_F \cup Y_C)$). Critical variables need to get assigned *safe values*, Y_{SC}, within a specified time frame, $\Delta\tau$, to avoid harm. In the above, the formulation describes a combinational circuit; however, extension for a sequential one is trivial.

The safety-critical system designer, while trying to introduce some fault tolerance, must always guarantee the safe operation property, allowing the occurrence of some (defective) G^* behavior, leading to $Y_C = Y_{SC}$. In the design environment, proving that G^* never leads to unsafe states requires a computational effort dependent on test length, fault list size, fault model type, fault multiplicity (single or double fault occurrence) and time frame length, $\Delta\tau$.

The **Safe Operation Property Coverage problem** can, thus, be stated as follows:

Given a system, C, described in the absence of disturbances (defects) as $G(X,t)$, a set of *single* faults $f \in F$ (F being the set of listed faults), and a test pattern, $T = \{T_1, T_2, \ldots T_{Nv}\}$, able to uncover *all* single and double listed faults $f_i \in F$, demonstrate (within a *confidence interval*) that *all* error situations ($G^* \neq G$) lead to safe values of the critical output variables, within a specified time period, $\Delta\tau$.

3. Methodology

In order to solve the problem, three issues need to be tackled: (1) an adequate design technique (namely, using *self-checking*), (2) an extended fault simulation (FS) process*,* and (3) a new metrics. Details of the first issue are beyond the scope of this paper. Extended FS includes single and double faults, adequate faults models to ensure high Defects Coverage, and timing analysis within $\Delta\tau$ for a subset of the faults. We assume that a fault is *covered* if, activating G*≠G, the Property holds within $\Delta\tau$. Using such extended FS process for all *N* listed faults in *F,* if *n* out of *N* are covered, the **Property Coverage metrics**, PC, is defined as PC $= n / N$.

Exhaustive fault simulation is prohibitive: for a digital circuit with *n* cells, FS complexity is proportional to *n*, n^2 or n^4. for single Line Stuck-at (LSA) and Bridging (BRI) faults, respectively. Hence, *fault sampling* is mandatory. Assuming a random fault sample $R<<N$ is selected, and $r = R$ are covered, it is possible to demonstrate [1,2] that the confidence level for which the exact Property Coverage, *PC*, is within the interval [PC_{min}, 100%], P_{PC}, is

$$P_{PC} = 1 - PC_{min}^{R+1} \qquad (1.)$$

In practice, P_{PC} and PC_{min} should be as high as possible (close to 100%). Equation (1.) can also be re-written to determine the sample size, *R,* that guarantees, for a given confidence level P_{PC}, that PC is within the interval [PC_{min}, 100%] (fig. 1):

$$R = \frac{\ln(1 - P_{PC})}{\ln PC_{min}} - 1 \qquad (2.)$$

As it can be seen, a sample of few thousand faults is enough to ensure a high confidence level, even for narrow PC_{min} intervals. This enables significant fault list compression for PC computation, especially for high *N* values, making the extended FS process affordable.

4. Results

The methodology was used in the validation of a safety-critical industrial ASIC for a gas burner control system, compliant to the EN298 safety standard [3]. Safe operation has to be guaranteed in the presence of double faults, and for $\Delta\tau=3$ s. For the chosen samples, extended FS with the `tfs` tool [2] leads to PC(R)=100%. For PC_{min}=99.90%, the smaller sample (R=2,192) leads to P_{PC} = 88.5%. However, double LSAs (18,039 faults), or the total fault list (double LSA, single and double BRI) (24,971 faults), leads to the extremely high P_{PC} = 99.99% value. Detailed data can be found in [2]. The theoretical model uses random sampling. Confidence level may be more accurately estimated, if stratified fault sampling techniques are considered, to take into account e.g. the non-equally likelihood of the faults.
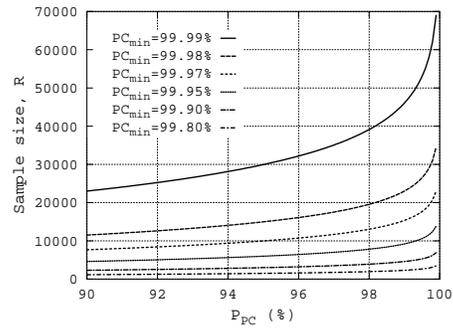

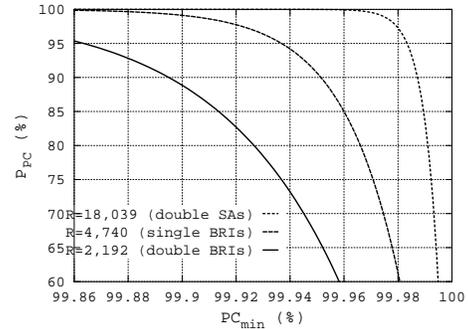Figure 1: R, as a function of the confidence level, P_{PC}.

Figure 2: P_{PC} for different sample sizes, R.

References

[1] W. Daehn, "Fault Simulation Using Small Fault Samples", JETTA, (2), pp. 191-203, Kluwer , 1991.
[2] F.M. Gonçalves et al., "Self-Checking and Fault Tolerance Quality Assessment using Fault Sampling", Proc. DFT, pp. 216-224, 2002.
[3] F.M. Gonçalves et. al., "Design and Test of a Certifiable ASIC for Safety-critical Gas Burners Control System", JETTA, (18), Nº. 3, pp. 285-294, Kluwer, 2002.