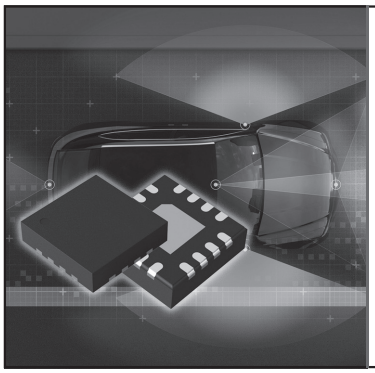
短期連載



安全の基本から規格書の構成と読み方，
設計フロー，最新動向まで

世界に負けない製品づくりに取り組む

車載向け電気/電子システムの機能安全規格「ISO 26262」入門

第7回　故障注入シミュレーション

中嶋　崇順　Takayuki Nakashima

本連載では，自動車の電気/電子システム向けに策定された最新の機能安全規格ISO 26262を例に，製品づくりで安全性を担保する方法を解説していきます．

今回は，機能安全規格を適用した設計をする際に必要な故障注入シミュレーションについて解説していきます．

1 故障注入シミュレーション

機能安全設計では，IF(Intended Function；意図した機能)に故障が発生した際，SM(Safety Mechanism；安全機構)が機能するかを検証するために，故障注入シミュレーションを実施します．これは，機能確認のための通常の回路シミュレーションとは異なり，回路の素子ひとつひとつに故障を注入してシミュレーション・パターンを流します．ロジックの場合，NANDやNORなどのゲートの入出力端子を0や1に固定(Stack at 0/1)してパターンを流し，IFとSMの動作を確認します．ゲート数の約2倍のパターンを流す必要があるため，膨大な時間がかかります．

● シミュレーション時間の見積もり

実際にシミュレーションを実施すると，どのくらいの時間がかかるか考えてみましょう．例えば，50万ゲートの回路で1回5分のシミュレーションを，100万ポイントに故障注入するとどのくらいかかるでしょうか．

5分×100万ポイント＝8.3万時間＝9.5年

なんと，10年近くかかることがわかります．これは現実的ではありませんね．

それでは，どのようにしたら現実的な時間で故障注入シミュレーションを行うことができるでしょうか．複数のCPUやPCに割り当ててシミュレーションを実行することも可能ですが，それでも限界があります．そこで，統計的手法を用いてシミュレーション時間を短縮することを検討してみましょう．

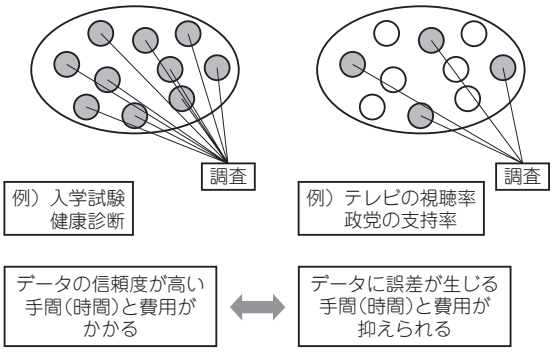
● 統計的手法(標本調査)

統計的手法に，「標本調査」というものがあります．**図1**に「全数調査」と「標本調査」の関係を示しています．全数調査とは，文字のとおり，集団全部について調査する方法です．一方，標本調査とは，集団の一部分を調査して全体を推定する方法です．全数調査の例としては，高校や大学などの「入学試験」や会社で受ける「健康診断」などがあります．標本調査の例としては，「テレビの視聴率」や「政党の支持率」などがあります．全数調査は「データの信頼度が高い」ですが「手間と費用」がかかります．標本調査は「手間と費用」は抑えられますが，「データに誤差」が生じます．

それでは，標本調査には，いったいどのくらいの誤差が含まれるのでしょう．標本調査で生じる誤差のことを「標本誤差」といい，次のような式で表されます．

$$e = t \times \sqrt{\frac{p \times (1-p)}{n} \times \frac{N-n}{N-1}} \quad \cdots\cdots\cdots\cdots (1)$$

ただし，e：標本誤差，t：信頼水準から決まる値(正規分布の表より信頼水準95％のときはt＝1.960，信頼水準98％のときはt＝2.330，信頼水



(a) 全数調査
調査の対象となっている集団全部について調査すること

(b) 標本調査
調査の対象となっている集団の一分部を調査して全体を推定する調査

図1　全数調査と標本調査