機能安全規格対応のための診断率算出ツール

稲田 遼一†, 広津 鉄平†, 森田 康史††, 秦 尚廣††

アブストラクト

ISO 26262 の発行に伴い, 規格に準拠した製品の開発が必要となっている. 規格準拠には, 安全機構で保護される故障の割合を診断率として算出する必要があるが, 算出には多くの工数がかかる. そこで, 対象回路に故障を注入し, その影響から故障を安全側故障, 保護がある危険側故障, 保護が無い危険側故障に分類し, 各故障の割合から診断率を算出するツールを開発した. 本ツールにより, 診断率算出時の工数削減が可能となる.

Diagnostic Coverage Evaluation Toolkit for Functional Safety

Ryoichi Inada†, Teppei Hirotsu†, Yasushi Morita†† and Takahiro Hata††

Abstract

Automotive manufacturers are developing products that comply with ISO 26262. In order to comply with this standard, manufacturers evaluate to the diagnostic coverage that is defined as failure rate that is covered by safety mechanisms. However, it takes many workloads to evaluate the diagnostic coverage. Therefore, we develop a diagnostic coverage evaluation toolkit. This toolkit injects some faults in a target circuit and observes propagation of effects from injecting faults. Then it classifies each one of the injected faults into either safe faults, hazardous protected faults, or hazardous unprotected faults. After that it evaluates the diagnostic coverage by failure rare of safe faults, that of hazardous protected faults and that of hazardous unprotected faults. This toolkit decreases the amount of work for evaluation of the diagnostic coverage.

1. はじめに

自動車向け機能安全規格である ISO 26262[1]が 2011 年に発行されたことにより, カーメーカやサプライヤ各社は規格に準拠した製品の開発に注力している. 規格に準拠した製品を開発するためには, まず対象製品の危険事象を分析し, 危険事象ごとに安全度水準の割り当てを行う. そして, 製品内で危険事象に関連するハードウェア故障を抽出し, その故障のうち安全機構によって保護可能な故障の割合を診断率として算出する. 最後に, 算出した診断率が安全度水準ごとに定められた基準値を満たしていることを示す必要がある.

この診断率を算出する方法は 2 種類ある. 1 つは, 規格の Part 5 Annex D を参照する方法である. Annex D には代表的な安全機構とその診断率が記載されているため, そこから診断率を引用することができる. しかし, Annex D に記載されていない安全機構を用いる場合には診断率の引用ができない. また, 単純に Annex Dから診断率を引用するだけでは, 診断率の算出根拠が乏しいという問題がある. もう 1 つは, 診断率の定義の通り, 対象回路に故障が発生した場合の動作を計算し, 安全機構で保護可能な割合から診断率を算出する方法である. しかし, この方法は, 対象回路が大きくなるほど診断率算出に多くの工数を必要とする. この問題を解決するため, 対象回路情報や故障情報を入力することで, 自動で診断率を算出する診断率算出ツールを開発した.

†株式会社日立製作所 日立研究所
Hitachi, Ltd., Hitachi Research Laboratory
††日立オートモティブシステムズ株式会社
Hitachi Automotive Systems, Ltd.

2. 診断率算出ツール

開発した診断率算出ツールの全体図を図 1 に示す. まず本ツールは, 入力された対象回路情報と素子故障情報をもとに故障を注入した回路を作成する. 図 1 のような回路情報および素子故障情報を入力した場合, 抵抗 R1 が開放(抵抗値極大)状態となった回路, 抵抗 R1 が短絡(抵抗値極小)状態となった回路, 抵抗 R2 が

開放状態となった回路，抵抗 R2 が短絡状態となった回路の 4 種類を作成する．素子故障情報にて故障注入設定可能な素子は，抵抗，インダクタ，キャパシタ，ダイオード，MOSFET，バイポーラトランジスタの 6 種類である．また，IEC 62380[2]を参考として，注入できる故障は開放，短絡，ドリフトの 3 種類に設定した．ドリフト故障では，素子値の変動量も設定可能としている．

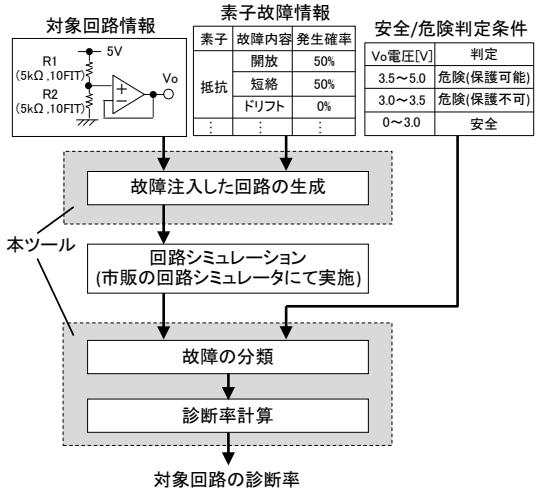

図 1 ツール全体図と入力情報の例

ツールは，故障を注入した回路を作成した後，この回路情報を市販の回路シミュレータに入力し，回路シミュレーションを行う．

シミュレーション終了後，ツールはシミュレーション結果を安全/危険判定条件と照合して，表 1 のように各故障を安全側故障，安全機構の保護がある危険側故障，安全機構の保護がない危険側故障のいずれかに分類する．例えば，抵抗 R1 が開放状態となった場合は Vo 電圧=0[V]となり，安全/危険判定条件の Vo 電圧が 0～3.0[V]の状態に該当するため，安全側故障となる．

表 1 故障の分類結果

素子	故障内容	シミュレーション結果	故障の分類
R1	開放	Vo=0[V]	安全側故障
	短絡	Vo=5[V]	保護がある危険側故障
R2	開放	Vo=5[V]	保護がある危険側故障
	短絡	Vo=0[V]	安全側故障

表 2 保護が無い危険側故障の故障率算出結果

素子	素子の故障率[FIT]	故障内容	発生確率	故障の分類			保護が無い危険側故障の故障率[FIT]
				安全側故障	保護がある危険側故障	保護が無い危険側故障	
R1	10.0	開放	50%	100%	0%	0%	0.0
		短絡	50%	0%	100%	0%	0.0
R2	10.0	開放	50%	0%	100%	0%	0.0
		短絡	50%	100%	0%	0%	0.0
合計	20.0						0.0

最後に，ツールは各素子の故障率，故障の発生確率，保護が無い危険側故障の発生割合を掛け合わせて，表 2 のように保護が無い危険側故障の故障率を計算する．そして，式 1 に基づいて診断率を算出し，出力する．今回の例の場合，保護が無い危険側故障の故障率が 0[FIT]であるため，診断率は 1.0=100%となる．

$$診断率 = 1 - \frac{\sum 保護が無い危険側故障の故障率}{\sum 素子の故障率} \quad (1)$$

3. 工数削減の評価

本ツールの工数削減効果を確認するため，ツールを利用した場合と手動でシミュレーションおよび診断率計算を行った場合の処理時間の比較結果を表 3 に示す．この比較は，図 2 に示した回路および条件で測定した結果である．本ツールの利用によって，回路シミュレーション以外にかかる時間を手動計算時と比べて大幅に削減することができる．

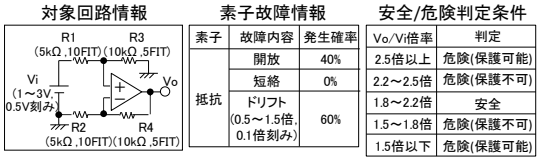

図 2 工数比較用回路および各種条件

表 3 各工程にかかる時間の比較

処理工程	処理時間[s]	
	ツール	手動
故障注入，シミュレーション結果確認，故障分類，診断率計算の総和	4.8	617.5
回路シミュレーション	6.1	6.1
合計	10.9	623.6

4. まとめ

本研究では，診断率算出時の工数削減を目的として，自動で診断率を算出する診断率算出ツールを開発した．本ツールを利用した場合の診断率算出時間を手動計算の場合と比較したところ，測定に用いた条件では，ツールの利用により手動計算時と比べて 98%の時間を削減可能であることを確認した．このように，本ツールの利用によって診断率算出にかかる工数を削減することが可能である．

参考文献

[1] ISO 26262:2011. Road vehicles - Functional safety -.

[2] IEC TR 62380:2004. Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment.