

シミュレーションを用いた回路故障発生時の車載制御ソフトウェア検証環境 Virtual Circuit Fault Injection Testing Environment for Automotive Software Verification

中尾 将吾[†] 兵頭 章彦[†] 勝 康夫[†]
Shogo Nakao Akihiko Hyodo Yasuo Sugure

1. 諸言

昨今、自動車業界では、利便性、快適性、安全性、環境性能の向上を目的とした電動化や車両走行制御の高機能化により、車載制御ソフトウェアの複雑化と大規模化が進んでいる。このような中で、自動車向けの機能安全規格 ISO26262 が制定され、車載電子部品の故障を想定したセーフティメカニズム導入による安全性向上が重要視されている。その結果、車載制御ソフトウェアの一部として実装されるセーフティメカニズムの割合は大幅に増加し、テストケースの増加と複雑化によるテスト不足が問題となっている。

この問題に対して、論理故障をターゲットとしたシミュレーションを利用したテスト手法が提案されてきた[1]–[4]。しかしながら、従来手法や実機環境を利用する場合、抵抗やキャパシタの素子値が中間値に変化するようなドリフト故障を想定したテストが実施できないという課題がある。

本課題解決のために、筆者らは、計算機上に構築した車両モデルを用いて、回路素子故障を模擬可能な故障時シミュレーション環境(Virtual FMEA)を提案する。本稿では、電動パワーステアリングの制御ソフトウェアテストを対象として、故障発生時のメカ挙動とソフトウェア挙動の両方を評価可能なマイコンと回路及びメカの 3 種連成故障シミュレーション技術と回路の素子値が中間値に変化するようなアナログ的挙動を示す故障を模擬するための動的故障注入技術の 2 つについて述べる。さらに、本技術を電動パワーステアリングのモータ電流モニタ機能のテストに適用した結果を報告する。本稿では、従来手法を用いて実現できなかったドリフト故障のテスト完了を目標とする。

2. 電動パワーステアリングのセーフティメカニズムテストについて

2.1 電動パワーステアリングの概要

本節では、本稿で対象とする電動パワーステアリングシステム(EPS)の概要について述べる。EPS は、ドライバの操舵量に基づき、電子制御ユニット(ECU)がモータ等のアシスト機構を制御することで、操舵をアシストするシステムであり、電流モニタ機能を有する ECU、セーフティメカニズム(SM)を含む制御ソフトウェア、ブラシレスモータ、操舵トルクセンサ、操舵角センサ、ラックやピニオンギア等のメカ部品から構成される。操舵トルクセンサが検出した操舵情報に基づき、ECU はモータ制御電流を出力し、アシスト用のモータを制御する。ここでモータ制御電流は、

ECU 上の電流モニタで測定され、モータのフィードバック制御や SM でも利用される。

2.2 セーフティメカニズムテストの概要と問題

本節では、EPS 等の車載制御システムに実装される SM テストの概要を述べる。図 1 に ISO26262 に沿った車載制御システムの V 字開発プロセスを示す。本プロセスのパート 4-8 「システム開発フェーズにおけるアイテム統合とテスト」では、EPS のようなセーフティクリティカルシステムは、ハードウェア-ソフトウェア統合環境における故障注入テストが強く推奨され、システムレベルで故障時の影響を評価する必要がある。さらに、定量的なエビデンスを残すことも重要視されており、机上検討が困難な回路素子レベルの故障に対しては、網羅的に実施することが要求されている。

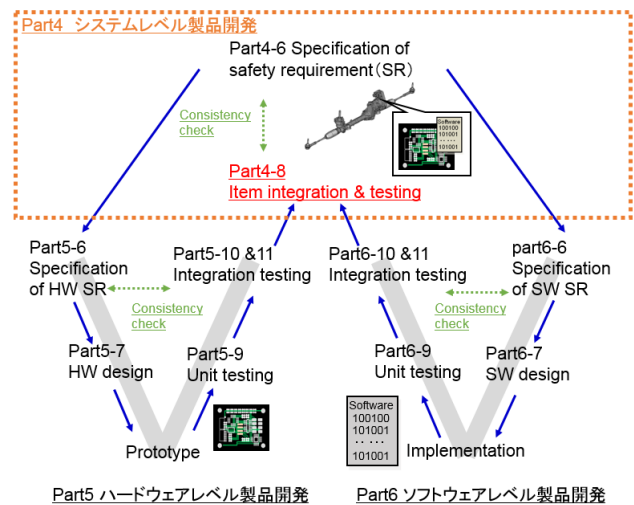


図 1. 車載制御システムの V 字開発プロセス

2.3 セーフティメカニズムテストの課題

SM テストで要求される回路素子レベルの故障モードを表 1 に示す。本稿では、故障の発生確率を纏めた IEC TR 62380 に基づき故障モードを定めた[5]。抵抗やキャパシタ等では、オープン故障とショート故障だけでなく、ドリフト故障についても定められている。ドリフト故障は、回路素子の素子値が正常値から 0.5 倍、2 倍といった中間値に任意の傾きで変化するような故障を指す。従来の実機環境を利用する手法では、ドリフト故障が模擬できない、またはアナログ素子で構成される電流モニタのような機能については、測定環境の影響を受け、システムの振る舞いの再現

[†]株式会社日立製作所 Hitachi, Ltd

性が低下し、ドリフト故障を想定したテストを正しく実施することができないという課題があった。

表1 素子と故障モード

素子	故障モード	素子	故障モード
抵抗	オープン故障、ドリフト故障	FET	ピンオープン故障、ピンショート故障
キャパシタ	オープン故障、ショート故障、ドリフト故障	ダイオード	オープン故障、ショート故障
コイル	オープン故障、ショート故障	IC	ピンオープン故障、ピンショート故障

3. 電動パワーステアリング向け Virtual FMEA 環境

3.1 Virtual FMEA

前章で述べた課題解決のために、図2に示すような、計算機上に構築した ECU モデル、メカモデルと故障注入機構を接続することで、ハードウェア-ソフトウェア統合環境における回路素子レベルの故障注入テストが可能なシミュレーション環境 (Virtual FMEA) を開発した。本稿では、ECU モデルに含まれるマイコン及びデジタル機能は Virtualizer™¹ 上で実装し（以降、コントローラモデルと称する）、ECU モデルに含まれるアナログ回路部分は Saber®² 上で実装し（以降、周辺回路モデルと称する）、メカモデル及び故障注入機構は MATLAB®/Simulink®³ 上で実装した。

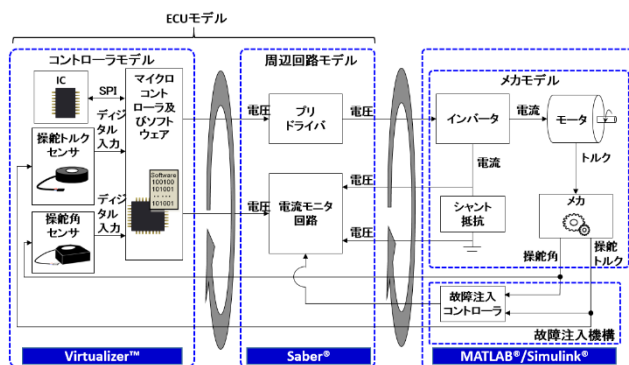


図2. EPS 向け vFMEA

以降では、各モデルの詳細とそれらの連成シミュレーション技術及び素子のドリフト故障を模擬するための動的故障注入技術について説明する。ただし、メカモデルについては、従来手法と同様のモデルが利用できるため、本稿では ECU モデルに焦点をあてる。

3.2 モデルと連成シミュレーション技術

3.2.1 コントローラモデル

コントローラモデルは、サイクル精度のマイコンモデル、バイナリコード化された制御ソフトウェア、センサ処理モデル、IC モデルで構成される。センサモデルは、メカモデルから物理量を受け取りマイコンへの入力フォーマットに変換する。ここで、センサモデルは、操舵角と操舵トル

1. Virtualizer™ is a trademark of Synopsys, Inc.
2. Saber® is a registered trademark of Synopsys, Inc.
3. MATLAB®/Simulink® is a registered trademark of The MathWorks, Inc.

クを Serial Peripheral Interface フォーマットと Single-Edge Nibble Transmission フォーマットに変換する。

3.2.2 周辺回路モデル

本稿では、EPS の SM テストとして、モータ電流モニタを構成する回路素子に故障が発生した際のメカ挙動及びソフトウェア挙動を評価することを目指している。そのため、故障注入部分である電流モニタとその伝播経路上にあるブリドライバを Saber®上でアナログ HDL を用いてモデル化した。周辺回路モデルを図3に示す。電流モニタモデルは、増幅器、抵抗、キャパシタ、参照電圧源、5V クランプ回路の各モデルで構成される。

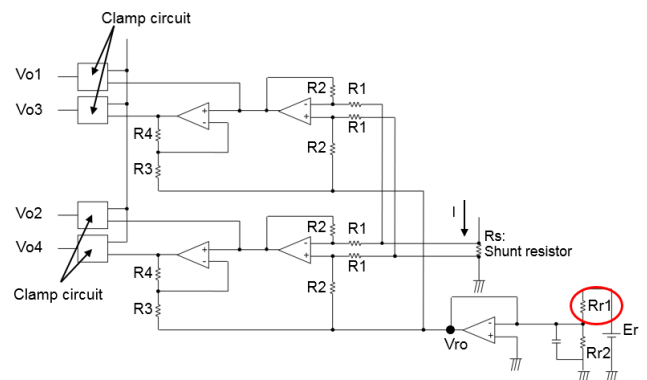


図3. 周辺回路モデル

3.2.3 連成シミュレーション技術

本項では、マイコンモデルが動作する Virtualizer™と周辺回路モデルが動作する Saber®とのインターフェイスブロックについて述べる。Virtualizer™は、System C で実装された論理演算をシミュレーションする論理シミュレータであり、電気特性等の物理特性を有さない信号が入出力される。一方で、Saber®はハードウェア記述言語で記述された物理システムをシミュレーションするアナログ-デジタル混在シミュレータであり、電気特性等の物理特性を有する物理値が入出力される。そのため、両シミュレータ上で実装する co-sim 用インターフェイスブロックは、シミュレータ間でデータ交換する機能と共に、信号値と物理値を変換する機能を設ける必要がある。従って、開発したインターフェイスブロックは、プロセス間でデータを交換する機能と信号値と物理値の間の変換機能を有する。

まず、シミュレータ間でデータ交換する機能について説明する。Virtualizer™とSaber®上の各インターフェイスブロックは、シミュレータ間で共通のインターフェイス名をパラメータとして所持する。各シミュレータは、このパラメータを参考に、共通のメモリ領域に書き込み/読み込みを行うことで、お互いのデータを交換する。文献[1]では、ソケット間通信を利用したデータ交換手法を採用した連成シミュレーション技術が述べられているが、本稿では、ソケット間通信よりも高速にデータ交換可能な共有メモリによるプロセス間通信手法を採用した。さらに、データ交換機能は、Virtualizer™とSaber®のシミュレーション実行を制御しており、シミュレータが共有メモリにアクセスするタイミングで、それぞれのシミュレーションの実行時間を同期させる。本稿では、シノプシス社が提供する共有メモリを利用したデータ交換機能をベースとして使用した[6]。

次に、信号値と物理値の変換機能について説明する。前述の通り、Virtualizer™上のインターフェイスブロックは単位を有さない信号値を扱うが、Saber®上のインターフェイスブロックは、2つの変数を持ち、それぞれの変数は、電圧[V]と電流[A]、角度[deg]とトルク[Nm]等の特性を持つ。この特性に従い、それぞれのシミュレータ上で、データタイプの変換及び特性の付与又は、削除を行う。例えば、AD変換器は、Saber®上では、電圧[V]と電流[A]の値を持つ変数として扱われるが、Virtualizer™上では、ビットレート0.0012[V/bit]の整数型“uint16”で扱われる。そのため、Saber®からVirtualizer™にデータ送信する際に、変換機能は、電圧値のみを抽出（電流値を削除）し、整数型にビットレート変換し、共有メモリに書き込む値を生成する。その一方で、Virtualizer™からSaber®にデータ送信する際には、変換機能は、ビットレートの逆変換により電圧値を算出するとともに、電流値を付与する。ここで、電流値は、マイコンベンダーより提供されるマイコンのデータシートに記載の、電圧電流特性を参考に、出力端のインピーダンス特性を模擬することで、算出する。

3.3 動的故障注入技術

この節では、操舵角や操舵トルクのようなメカ挙動が事前に設定した特定の条件を満足した場合に、Saber®上の回路素子モデルに動的に故障注入が可能な技術について説明する。本技術は、図4に示すMATLAB®/Simulink®上で実装した故障注入コントローラ、Saber®上の故障注入用のインターフェイスを有する回路素子モデルとシミュレータ間の接続インターフェイスで構成される。ここで、故障注入コントローラは、メカ挙動をモニタリングし、特定の条件を満足した場合に、故障時の素子値を出力する。回路素子モデルは、素子値を動的に変更するための故障注入用のポートを持ち、コントローラから送信された値に従い回路素子モデルの素子値を更新する。ここで、回路素子モデル上では、故障注入用のポートから与えられる素子値を時変な係数として扱っている。

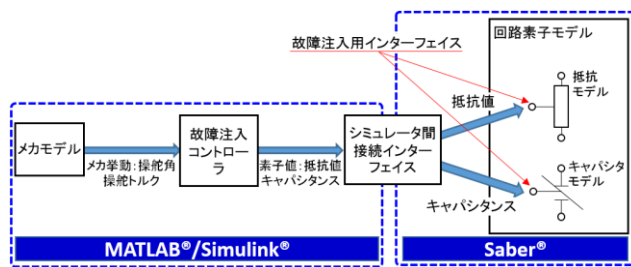


図4. 動的故障注入技術実現のための機構

4. 結果

4.1 実証例

本節では、SMテストへのvFMEA適用例として、図3に示す降圧用抵抗Rr1の抵抗値が3倍になるドリフト故障を想定したテストを実施する。本稿で検証するSMの状態遷移を図5に示す。SMは、電流センサの故障に対して、センサの出力電圧をマイコンが監視し、その電圧が許容回数以上閾値外の値（約2V未満）となった際に、電流センサの故障を検出する。さらに、故障検出後、システムをシャットダウンし、モータからのアシストトルクを0[Nm]にする。ここで、

SMが故障を検出しない許容回数は59回であり、ソフトウェアで実装されたカウンタ（以降、フェイルカウンタと称する）を用いて、出力電圧が閾値外となった回数を計測する。従って、SMが出力電圧の異常を60回カウントした場合、故障と判断して、システムをシャットダウンし、モータからのアシストトルクを停止する。

また、本テストは、操舵中の故障発生時のシステムへの影響を評価するとし、操舵中にアシストトルクが一定以上発生している状態として、40°以上の操舵中にドリフト故障が発生したことを想定する。

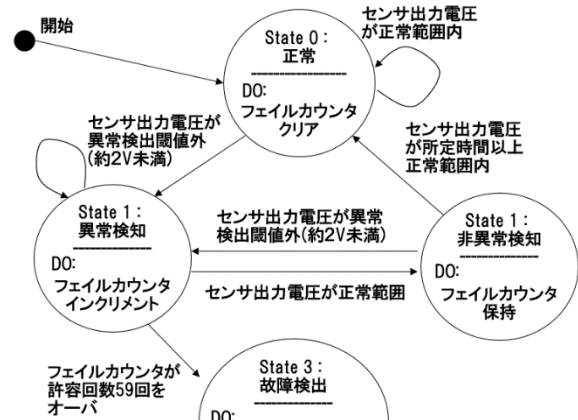


図5. セーフティメカニズム状態遷移

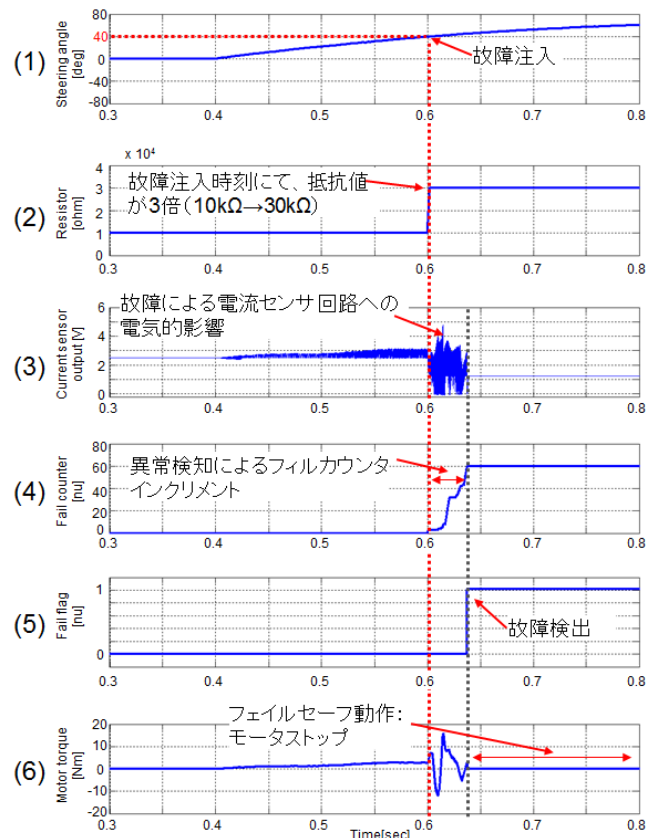


図6. vFMEA実証例

図6に、(1)操舵角入力、(2)故障注入対象Rr1の抵抗値、(3)電流センサ出力電圧、(4)フェイルカウンタ、(5)電流センサの故障検出フラグ、(6)モータからのアシストトルクのシミュレーション結果をそれぞれ示す。図6(1)、(2)より、3.3節で述べた動的故障注入技術を用いた結果、メカモデル挙動をきっかけとして、動的にドリフト故障が注入されていることがわかる。さらに、図6(3)-(5)より、SMが電流モニタ機能の異常を検知し、故障を検出しているのがわかる。図6(5)、(6)より、故障検出後、システムがシャットダウンされたことで、モータからのアシストトルクが停止している。以上より、vFMEAを適用することで、設計通りのSMが実装できていることを確認できた。

4.2 実適用結果

本節では、IEC TR 62380に基づき、電流モニタ機能故障時のSMテストとして想定した82件に対して、実機を利用したテストとvFMEAを併用した結果を述べる。表2に適用結果を示す。(1)は、各素子のIEC TR 62380で定義される故障モードであり、従来故障はオープン故障とショート故障といったドリフト故障以外を指す。(2)は、電流モニタに含まれる抵抗とキャパシタの各故障モードで想定したテスト件数を指す。(3)は、vFMEAを適用したテスト件数とそれらのテスト結果を指す。OK列は設計通りにセーフティメカニズムが動作した件数を、NG列は設計通りにセーフティメカニズムが動作しなかった件数を、それぞれ示す。

表2. 実適用結果

素子	(1)故障モード	(2)想定 テスト件数	(3)実機テスト 件数	Virtual FMEA(提案手 法)テスト件数 とテスト結果	
				OK	NG
抵抗	従来故障	14	8	6	0
	ドリフト故障	32	0	32	0
キャパシタ	従来故障	18	6	12	0
	ドリフト故障	18	0	18	0
トータル		82	14	68	0

表2からも明らかなように、vFMEAを利用することで、抵抗及びキャパシタのドリフト故障を対象としたテスト50件をすべて実施することができた。さらに、ECU基板上の素子の配置が原因で人為的な故障注入が困難な従来故障についても想定されるテストを完了することができた。その結果、実機テストとvFMEAを併用することで、電流モニタ機能のSMテストとして想定されるテスト82件すべてを完了することができ、これらの併用により、EPSのSMテストをすべて完了できる見通しを得た。

5. 結言

電動パワーステアリング(EPS)のセーフティメカニズム(SM)のテスト実施件数増加を目的に、回路素子故障時のシステムへの影響を評価可能な故障シミュレーション環境(vFMEA)を構築し、EPSのSMテストに実適用した。vFMEA環境を実検証に適用するにあたっては、回路素子故障時のシステム全体の振る舞いを評価することと、素子値が中間値に変化するようなアナログ的挙動を示す故障を模擬することが必要であり、以下2点の開発を行った。

1. 異種シミュレータ上で動作するマイコン、ECU回路、メカモデルの連成シミュレーション技術
2. ドリフト故障を模擬可能な動的故障注入技術

上記開発した技術を適用したvFMEA環境を併用することで、従来手法により実施されたテスト14件に追加して、ドリフト故障を含めたテスト68件すべてを完了することができた。以上より、SMテストへのvFMEA適用の有効性を示せた。

参考文献

- [1] 伊藤康宏, 勝康夫, 於保茂. "Virtual HILS: システム全体仮想化による、組込みソフト検証の高効率化(ソフトウェアテスト、組込み技術とネットワークに関するワークショップ ETNET2011)." 電子情報通信学会技術研究報告. CPSY, コンピュータシステム 110.473 (2011): 243-247.
- [2] Niimi, Yukihide, Takayuki Ono, and Naoya Tsuchiya. "Virtual Development of Engine ECU by Modeling Technology," No. 2012-01-0007. SAE Technical Paper, 2012.
- [3] Nakao, Shogo, Masafumi Shimozawa, and Yasuo Sugure. "Virtual FMEA: Simulation-Based ECU Electrical Failure Mode and Effects Analysis," No. 2014-01-0205. SAE Technical Paper, 2014.
- [4] Rafaila, Monica, et al. "New Methods for System-level Verification using SystemC-AMS Extensions: Application to an Automotive ECU," MBMV. 2009.
- [5] IEC, "TR. 62380," Reliability and handbook-universal-Universal model for reliability prediction of electronics components, PCBs and equipment, 2004.
- [6] Synopsys, Inc., "Virtualizer simulink integration manual," 2013.