車載用マイクロコントローラの機能安全と故障注入テストシステム

Functional Safety in Automotive Microcontrollers and Fault Injection Test System for Compliance with High Functional Safety Requirements

大溝　孝　　畦崎　勉　　高野　裕之
■OMIZO Takashi　■UNESAKI Tsutomu　■TAKANO Hiroyuki

現在，自動車をはじめ人命に関わる制御システムの安全が電子・電気的な機能により支えられている。それに伴い機能安全標準 IEC 61508（国際電気標準会議規格61508），ISO 26262（国際標準化機構規格26262）などの制定が進んでいる。

東芝は，これら規格に準拠した車載用マイクロコントローラを開発するとともに，顧客へ機能安全サポートパッケージTM-SIL™を提供している。その中のシステムサポートでは，中核となるFPGA（Field Programmable Gate Array）によるフルICE（In Circuit Emulator）型故障注入テストシステムを開発した。これにより，機能安全への要求が高まるにつれて質的かつ量的に増大する顧客での検証コストを低減できる。

With the recent expansion of safety-critical control systems utilizing electrical and electronic functions in areas affecting human life, such as automobiles, functional safety standards including the IEC (International Electrotechnical Commission) 61508 and ISO (International Organization for Standardization) 26262 standards have been specified.

Toshiba has developed an automotive microcontroller complying with these functional safety standards, and offers users the TM-SIL™ functional safety support package consisting of device support, software support, and system support subpackages. To meet users' requirements for reduction of the costs incurred in the implementation of the increasing number of functional safety verification and validation tests, we have also developed a field-programmable gate array (FPGA)-based full in-circuit emulator (ICE) type fault injection test system as a core of the system support subpackage of the TM-SIL™ package.

1　まえがき

現在，発電所や，鉄道，プラント，自動車など，人命に関わる制御システムの“安全”が，電子・電気的な“機能”により支えられている。この機能の故障による安全への影響が許容範囲内にあるかどうかを客観的に判断できる“機能安全”の標準として，IEC 61508（1st edition）が2000年に発行され，更にこの標準を車載システムに特化したISO 26262が2011年に発行されている[(1)(注1)]。

2011年の規格発行直後は，各社の対応は，ブレーキやステアリングなど明らかに厳しい安全性が求められるシステムに絞られていたが，最近は，エンジンやADAS（Advanced Driver Assistance System），ボディ系など，対応システムの範囲は急速に広がってきている。

こうしたなか，機能安全への対応は，多くのベンダーにとって，数多くのあたりまえ品質の一つになりつつあり，特に部品サプライヤーにとっては，顧客に提供するソリューションをいかにわかりやすく簡潔に説明できるかが重要になってきている。そのため，豊富でわかりやすいドキュメント群やサポート体制が求められている。

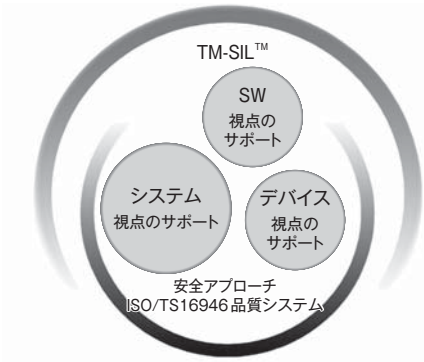
そこで東芝は，顧客の機能安全システムでの故障注入テストを容易化する目的で，FPGA（Field Programmable Gate Array）によるフルICE（In Circuit Emulator）型故障注入テストシステムFFFIT（FPGA Based Full ICE Fault Injection Test System）を開発した。ここでは，車載IC群の中でFFFITの最初のモチーフになっている車載用マイクロコントローラ（MCU）を中心に，機能安全に対する当社の取組み全般について述べ，次いで故障注入テスト技術及びFFFITの概要と特長について述べる。

（注1）　IEC 61508は2010年に2nd editionが発行された。ISO 26262も今後，改定が予定されている。

2　車載用MCUにおける取組み

当社は，2007年から車載用MCUを中心にIEC 61508準拠の検討を始め，2009年には車載用MCUのプラットフォームに対し第三者認証機関のTÜV SÜD Automotive社からSIL3（Safety Integrity Level 3）Technical Report Iを取得した。獲得した機能安全対応のスキルをもとに，2010年から，パワーステアリングや，ハイブリッドエンジン，電池監視，ADASなどISO 26262対応システムに適用可能な車載用MCU，アナログIC，及びSoC（System on a Chip）を順次開発した。2012年にISO 26262ソフトウェア（SW）開発プロセスの認証を得るとともに，2013年には最初の製品を量産し始めた[(2)]。

他社も同様の状況にあるなか，機能安全への対応は，製品自体の対応だけでなく，豊富でわかりやすいドキュメント群や



TS16946：技術仕様16946

図1. TM-SIL™の概念 — TM-SIL™はデバイス，SW，及びシステムの三つの視点からサポートしている。

Concept of TM-SIL™ functional safety support package

サポート体制が重要になってきている。

このような要求に対応するため，当社は機能安全サポートパッケージTM-SIL™を策定した（**図1**）。TM-SIL™は，次の三つのサブパッケージから構成される。

(1) デバイスサポート

(2) SWサポート

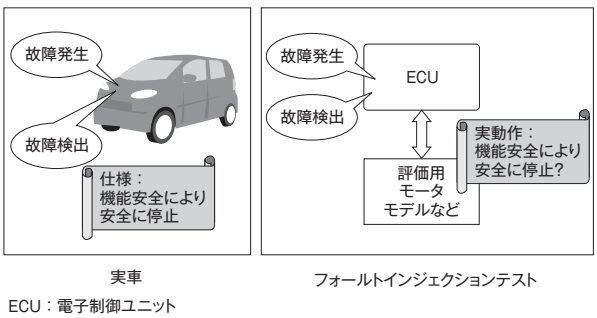
(3) システムサポート

車載用MCUにおけるデバイスサポートでは，製品自身のサポートに加え，セーフティマニュアル及びエビデンス群を提供する。SWサポートでは，機能安全SWライブラリ群を提供する。システムサポートでは，アナログICとのチップセット提案に加え，故障注入テストシステムFFFITのサポートが可能である。

3 様々な故障注入テスト技術とFFFIT

3.1 故障注入テスト

故障注入テストの概念を**図2**に示す。



ECU：電子制御ユニット

図2. 故障注入テストの概念 — 故障注入テストは，実車を使用するのではなく，テスト対象箇所と評価用装置やモデルなどを組み合わせて行う。

Concept of fault injection test

車載安全関連システムでは，故障が発生した場合に事故につながるリスクが許容範囲内になるように設計している。実際に故障が発生した場合にシステムが設計どおりにほんとうに安全状態に移行するか，それを検証するための方法の一つが故障注入テストである。この場合，実車ではなく，テスト対象箇所と評価用装置やモデルなどを組み合わせて実施する。

3.2 故障注入テストの各種方式

故障注入テストは従来から様々な方式が提案されている[3]。従来の代表的な故障注入テストの方式を分類して**表1**に示す。

ハードウェア（HW）ベースでは，実機を用いるためリアルタイムで動作するが，制御性及び再現性は良くない。

SWベースでコード変更する場合は，テスト対象のSW自体を改変するため，実際のシステム動作と異なるという問題がある。

SWベースでデバッガなどを使用する場合を**図3**に示す。この場合はテスト対象のSWを変更する必要はなく，システムに接続したデバッガからメモリの値やレジスタの値を変更することで，故障状態を擬似的に起こすことができる。車載用MCUでは，一般にプロセッサ動作のブレークなしに値を変更できるNBD（Non Breakable Debug）インタフェース（IF）を持つので，これにデバッガやHILS（Hardware in the Loop Simulation）を接続してリアルタイム動作が可能である。ただし，変更可能な箇所はメモリやレジスタに限られるため制御性があまり良くない。

モデルベースの仮想プラットフォームを用いる場合を**図4**に示す。この場合は，SWを実行する命令ベースシミュレータと，

表1. 代表的な従来の故障注入テスト

Conventional fault injection test methods

カテゴリー	方　式	特　性				
		速度	制御性	観測性	再現性	非改変度
HWベース	外部信号注入あり	○	△	×	×	○
	外部信号注入なし	○	×	×	×	○
SWベース	SWコード変更	○	△	○	△	×
	デバッガなどを使用	○	△	○	×	○
モデルベース	仮想プラットフォーム	△	○	○	○	△

○良い　△普通　×悪い

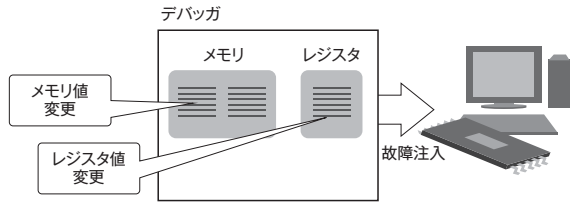


図3. SWベースでデバッガを使用した場合 — テスト対象のSWを変更することなく，デバッガで故障状態を擬似的に起こすことで故障注入テストができる。

Fault injection test using software debugger

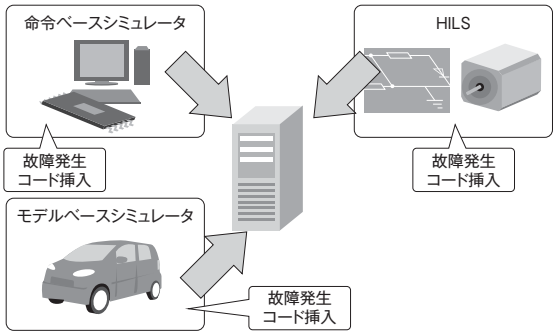


図4．モデルベースで仮想プラットフォームを用いる場合 ― 命令ベースシミュレータとモデルやHILSを組み合わせて故障状態を擬似的に起こすことで，故障注入テストができる。

Fault injection test using model-based virtual platform

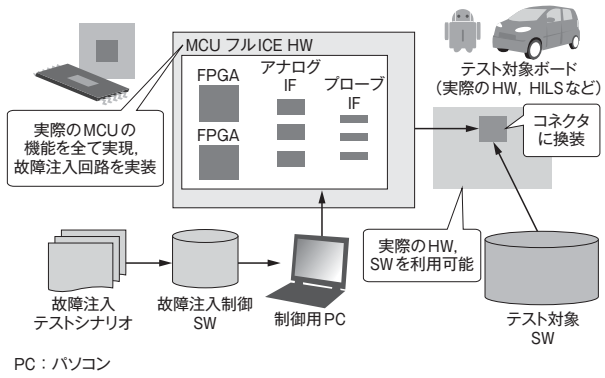


図5．FFFITの概要 ― 対象となるMCUの機能全てをエミュレートするMCU フルICE HW，故障注入制御SW，及び故障注入テストシナリオから構成される。

Overview of FPGA-based full ICE type fault injection test (FFFIT) system

モデルベースシミュレータ上のモデルやHILSによるモデルを接続することで，システム全体の故障注入テスト環境を構築できる。命令ベースシミュレータによりSWは高速に動作するが実際のシステムとは動作タイミングは異なる，モデルの精度や規模を上げると動作速度は落ちるといったことから，テスト対象やテストレベルに応じて適切なモデルを用いることが必要である。

これまで述べたように様々な故障注入テスト方式が存在するが，いずれも一長一短があり，テスト対象やテストレベルに応じて適切に使い分ける必要がある。しかし機能安全システムに要求される故障注入テストは質的かつ量的に増加する傾向にあり，これに対応するための新たな故障注入テスト技術が必要とされている。

今回開発した，従来と異なるFPGAによるフルICE型故障注入テストシステムFFFITを使用することで，故障注入テストがより容易に導入でき実施できる。

4　FFFITの概要と特長

4.1　FFFITの概要

FFFITの概要を**図5**に示す。

FFFITは，MCU フルICE HWとそれを制御するための故障注入SWから構成される。一つ又は複数のFPGAを持ち，テスト対象（主にMCU）の機能が実装される。ADC（Analog Digital Converter）などのFPGAに実装できないアナログ回路が必要な場合は外付けの回路で実装される。また対象となる回路の信号電圧レベルが異なる場合はプローブIFとして信号レベルを変換する回路が設けられる。これらにより，対象となるMCUの機能全てをこのMCU フルICE HWでエミュレートすることが可能になる。

故障注入テストを行うテスト対象ボード上の本来MCUが取り付けられている部分へ実LSIの代わりにコネクタを実装し，それを介してMCU フルICE HWへ接続される。テスト対象ボードでは実際のMCUが実装されている場合とまったく同じテスト対象のSWを実行しながら，故障注入テストを行うことができる。

故障注入は，対象となるMCUのうちFPGA内に実装された部分に対して行うことができる。例えばレジスタや，メモリ，演算器，バス，デジタル入出力信号などである。どこに，どのような故障を，いつ発生させるかは，故障注入テストシナリオで記述される。故障注入テストシナリオはスクリプト言語で記述され，柔軟な故障注入テストを行うことができる。故障注入テストシナリオは，故障注入制御SWによりFPGA内に実装された故障注入回路に送られ，指定された条件が満たされるとFPGAの回路上に故障状態を作り出すことで故障注入テストを行うことができる。

4.2　故障注入方式と故障種別

FFFITの故障注入方式を**図6**に示す。

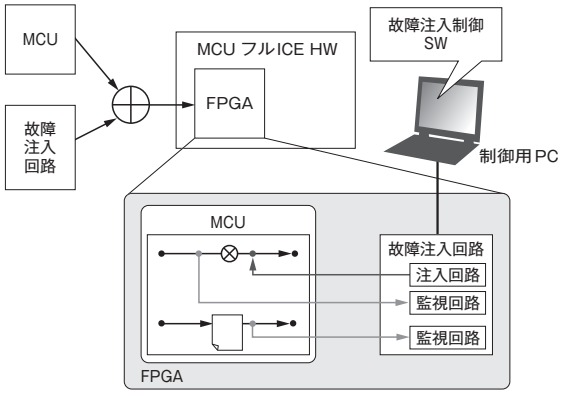


図6．FFFITの故障注入方式 ― FPGAに実装されたMCUの回路の任意部分に故障注入回路を挿入することで故障を注入できる。

Mechanism of fault injection method in FFFIT

表2. FFFITで標準的にサポートする故障種別
Fault categories supported by FFFIT

故障注入対象	設定項目	設定値
メモリ	故障種別	一時故障，永久故障
	条件	アドレス，マスク
	値	即値，反転
ロジック信号	故障種別	一時故障，永久故障
	値	即値，反転

FPGA内に実装されたMCUの回路の任意部分に対し，FPGA内に故障注入が必要なポイントへ故障注入回路を挿入する。また故障注入のタイミング条件に必要な信号を監視回路によりモニタすることができる。これを故障注入制御SWから制御することで，制御性及び再現性の高い故障注入テストを行うことが可能である。

FFFITで標準的にサポートする故障種別を**表2**に示す。これは一例であり，必要に応じて故障注入回路を構成することにより様々な故障種別に対応することが可能である。

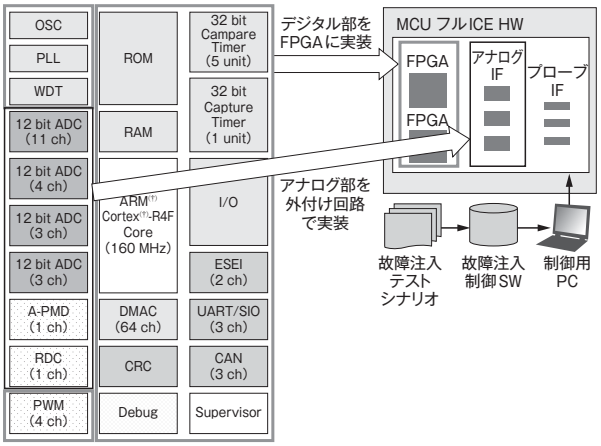
これまで述べたようにFFFITはテスト対象のボード及びSWを原則変更することなく，リアルタイムで又はリアルタイムに近い速度で故障注入テストを行うことができる。顧客にとっては特別なHWや，SW，モデルを開発することなく，よりリアリティの高い故障注入テストを容易に行うことができることが，FFFITの特長である。

5 FFFITの適用事例

5.1 TMPR454F用プロトタイプシステム

FFFITをHEV（ハイブリッド電気自動車）及びEV（電気自動車）の車載用機能安全対応モータ制御MCUであるTMPR454Fに適用した例を**図7**に示す。

TMPR454Fにはモータを制御するためのCPUコアのほか周辺機能があり，デジタル部とアナログ部を併せ持つ構成となっている。これをFFFITに実装するためには，デジタル部のLSIデザイン（RTL（Register Transfer Level）記述）をFPGA上に実装し，またFPGAに実装できないアナログ部分（ADCなど）は別基板上に外付け回路として実装する。またTMPR454Fは5 Vの信号IFであるが，FPGAの信号レベルと異なるため，プローブIFで5 V信号への変換を行っている。この結果，TMPR454FはXilinx社のVirtex7 690T 2個と外付けADC及び5 V-1.8 V信号レベル変換回路により実現することができた。FPGAの使用率は約70 %，また動作周波数はTMPR454Fと同じ160 MHzでの動作が可能となる見込みである。TMPR454Fを実装したFFFITプロトタイプシステムを**図8**に示す。プロトタイプシステム上でTMPR454Fのモータ制御SWを動作させることで車載用と同じ三相交流モータを駆動することが可能である。更に，パソコン（PC）上の故障注入制御SWにより故障注入テストシナリオを実行することで，モータを動作させながら様々な故障注入テストを実行することができる。



OSC ：オシレータ　ESEI ：多機能シリアル拡張インタフェース
PLL ：Phase Locked Loop
UART：Universal Asynchronous Receiver Transmitter
WDT ：ウォッチドッグタイマ　SIO ：シリアル入出力
ch ：チャネル　A-PMD：Advanced Programmable Motor Driver
CAN ：Controller Area Network　RDC ：レゾルバデジタルコンバータ
PWM ：パルス幅変調　DMAC ：Direct Memory Access Controller
CRC ：巡回冗長検査　I/O ：入出力

図7. TMPR454Fへの適用事例 — FFFITを車載用MCU TMPR454Fに適用した場合，デジタル部分をFPGAに，アナログ部分を外付けアナログ回路で，信号電圧変換をプローブIFで実現できる。
Example of application of FFFIT to TMPR454F onboard microcontroller unit

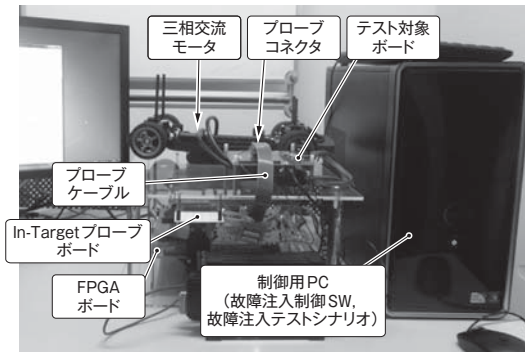


図8. FFFITプロトタイプシステム — FFFITをTMPR454Fのプロトタイプシステムに適用した。
FFFIT prototype system

5.2 故障注入テストの適用事例

ここではプロトタイプシステム上で行った故障注入テストの適用事例について述べる。

クリティカルなタイミングの故障注入を行う事例を**図9**に示す。この例では，割込みベースで行われる制御において，クリティカルセクションである割込み処理内で故障を発生させるものである。故障注入テストシナリオでは割込み信号が1となる

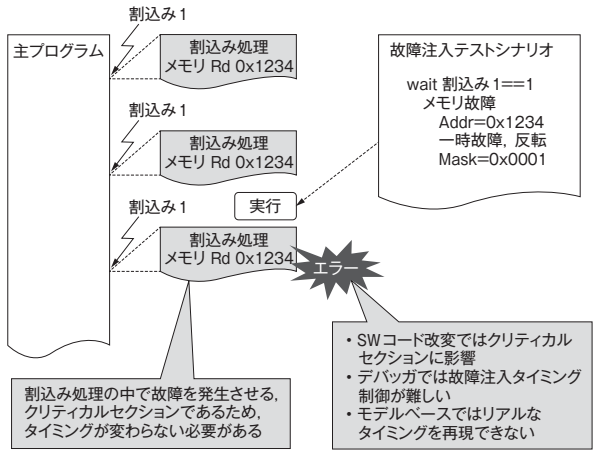


図9．クリティカルなタイミングの故障注入テストの事例 — クリティカルなタイミングの制御が必要な場合でも，FFFITでは制御性及び再現性の良いテストを行うことができる。

Example of fault injection test in case of timing-critical application

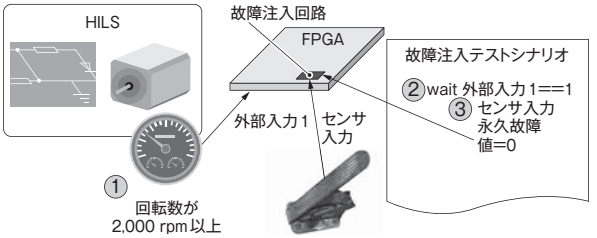


図10．システムと同期した故障注入テストの事例 — FFFITではMCU内部だけでなく，システムと同期した故障注入テストを行うことができる。

Example of fault injection test synchronized with system

ことを待って割込み処理内でアクセスされるメモリへの故障を注入することで，クリティカルなタイミングの故障注入テストを確実に行うことができる。またコードを改変する必要がなく，処理タイミングが変わることがない。

もう一つの事例として，システムと同期して故障注入テストを行う場合を**図10**に示す。この例ではFFFITに接続されるシステム上の状態により故障注入のトリガを掛けることができる。例えば，モータの回転数が2,000 rpm以上で1になる信号があった場合，これをFFFITの外部入力に接続する。故障注入テストシナリオではこの状態を監視し，モータの回転数が2,000 rpm以上になり信号が1になると，センサ入力に永久故障として値0を入れることで故障を発生させる。この例のようにMCUの内部故障だけでなく，アクセルペダルなどの外部センサの故障を模擬することができ，システムと同期した故障注入テストを行うことが可能である。

6　あとがき

TM-SIL™におけるサポート技術の柱の一つである故障注入テストシステムFFFITをより広い範囲に適用できるよう，対象となるMCUを増やし，より多くの顧客が利用できるようにしていく。

車載用MCUなど車載用ICの機能安全に向けて今後もTM-SIL™の適用を推進することにより，高度な機能安全の実現と，顧客での導入コストの低減に貢献していく。

文　献

(1) ISO 26262 : 2011. Road vehicles-Functional safety. First edition.
(2) 東芝．“車載用マイクロコントローラ”．半導体＆ストレージ製品ホームページ．<http://www.semicon.toshiba.co.jp/product/assp/automotive/micro/>，(参照2014-07-11).
(3) Hsueh, M-C. et al. Fault Injection Techniques and Tools. Computer. **30**, 4, 1997, p.75－82.

大溝　　孝　OMIZO Takashi
セミコンダクター＆ストレージ社 システム・ソフトウェア推進センター ソフトウェア・プラットフォーム担当参事。車載用開発支援ツール及びLSI利用技術の企画・開発に従事。
System & Software Solution Center

畦崎　　勉　UNESAKI Tsutomu
セミコンダクター＆ストレージ社 システム・ソフトウェア推進センター ソフトウェア・プラットフォーム担当主務。フルICE型故障注入システムの企画・開発に従事。
System & Software Solution Center

高野　裕之　TAKANO Hiroyuki
セミコンダクター＆ストレージ社 ミックスドシグナルIC事業部 車載IC応用技術部主査。車載用マイクロコントローラ・SoCの企画・開発に従事。情報処理学会会員。
Mixed Signal IC Div.