MATLAB EXPO 2020 Japan

HITACHI
Inspire the Next

車載ECU周辺回路の故障注入の シミュレーション検証技術

2020年10月1日

日立オートモティブシステムズ(株)
技術開発統括本部 技術プラットフォーム本部 ソフト開発技術部
主任技師　深野 善信

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

HITACHI
Inspire the Next

Contents

1. 車載ECU開発を取り巻く状況について
2. MBD拡張：仮想ECUテスト環境
3. 活用事例：仮想FMEA(vFMEA)検証
4. まとめ

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

HITACHI
Inspire the Next

1. 車載ECU開発を取り巻く状況について

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

走る・曲がる・止まるの電子制御化の進展

HITACHI
Inspire the Next

自動運転

予防安全制御
エネルギーマネジメント制御

ブレーキ

電動油圧式ﾌﾞﾚｰｷ

電動ﾌﾞﾚｰｷ(BBW)

サスペンション

電磁ｱｸﾃｨﾌﾞｻｽ

電動ｽﾃｱﾘﾝｸﾞ(SBW)

ステアリング

電動ﾊﾟﾜｰｽﾃｱﾘﾝｸﾞ

HEV・EVシステム

- 環境対応
- 安全・快適

電制スロットル

変速機制御

筒内噴射（DI）

エンジン制御

ディジタル制御

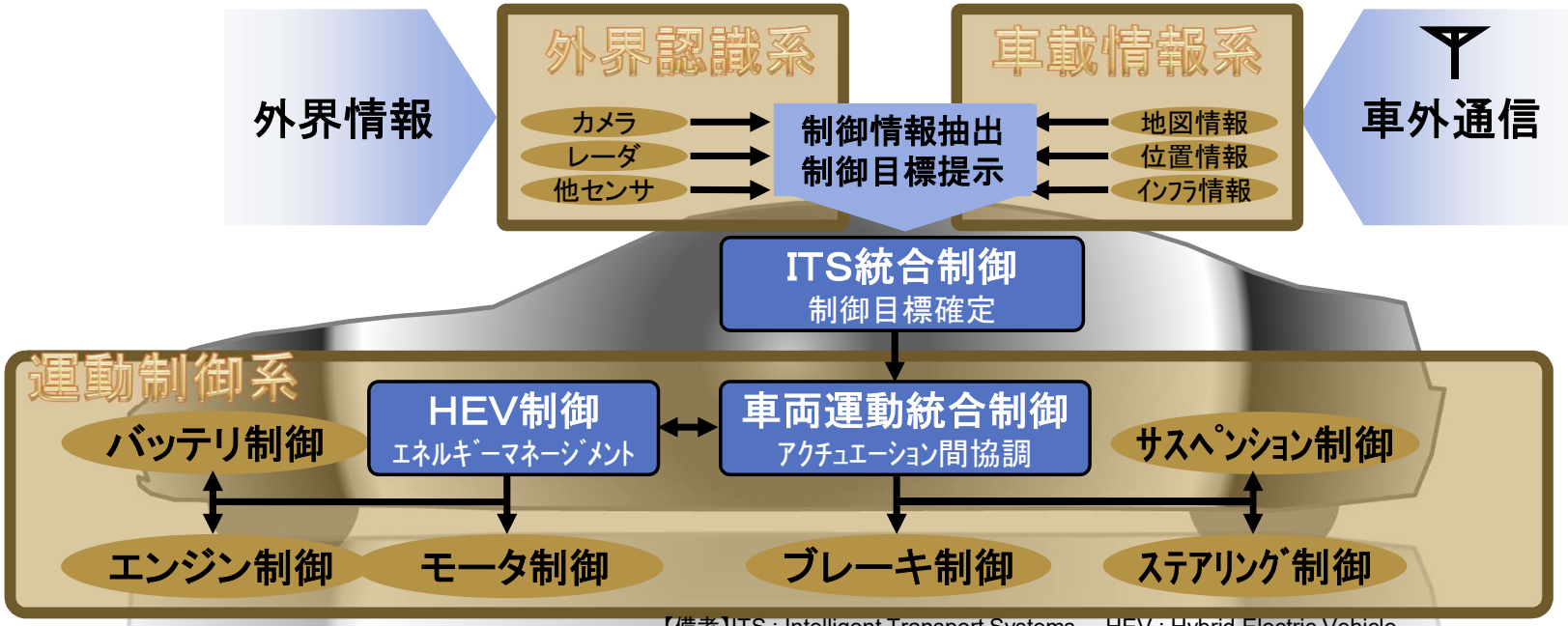
アナログ制御

車載ソフトウェアの大規模化・複雑化
・コード行数：数百倍／20年間
・すでに1億行を超える
・自動運転対応でさらに急増

1980　2000　2020　2025　年

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

車載電子制御システムの高度化・複雑化と安全・高品質への要求



【備考】ITS : Intelligent Transport Systems、 HEV : Hybrid Electric Vehicle

- 単体制御の集合体から統合制御への進化

→ 検証の難易度アップ

- 電子制御システムの安全性への市場注目度の高まり
- 電子制御機能の更なる高度化・複雑化
- 自動車用機能安全規格ISO26262への対応（2011年11月制定）

→ 従来以上に安全、高品質、高効率な設計・検証要

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

機能安全とは

HITACHI
Inspire the Next

■本質安全 (Inherent Safety)

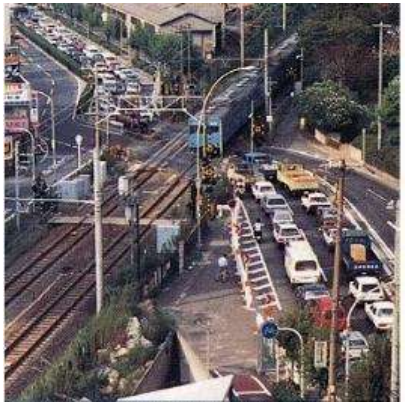
リスク発生要因を根源から排除する。

例：立体交差

■機能安全 (Functional Safety)

機能や仕組みによって、リスクが発生する確率を許容できるレベルまで下げる。

例：踏切



対策方法は大きく2種

（1）ハードウェア故障やシステマティックフォールトが発生しても冗長化や診断などの安全機構により安全目標侵害を防止する。

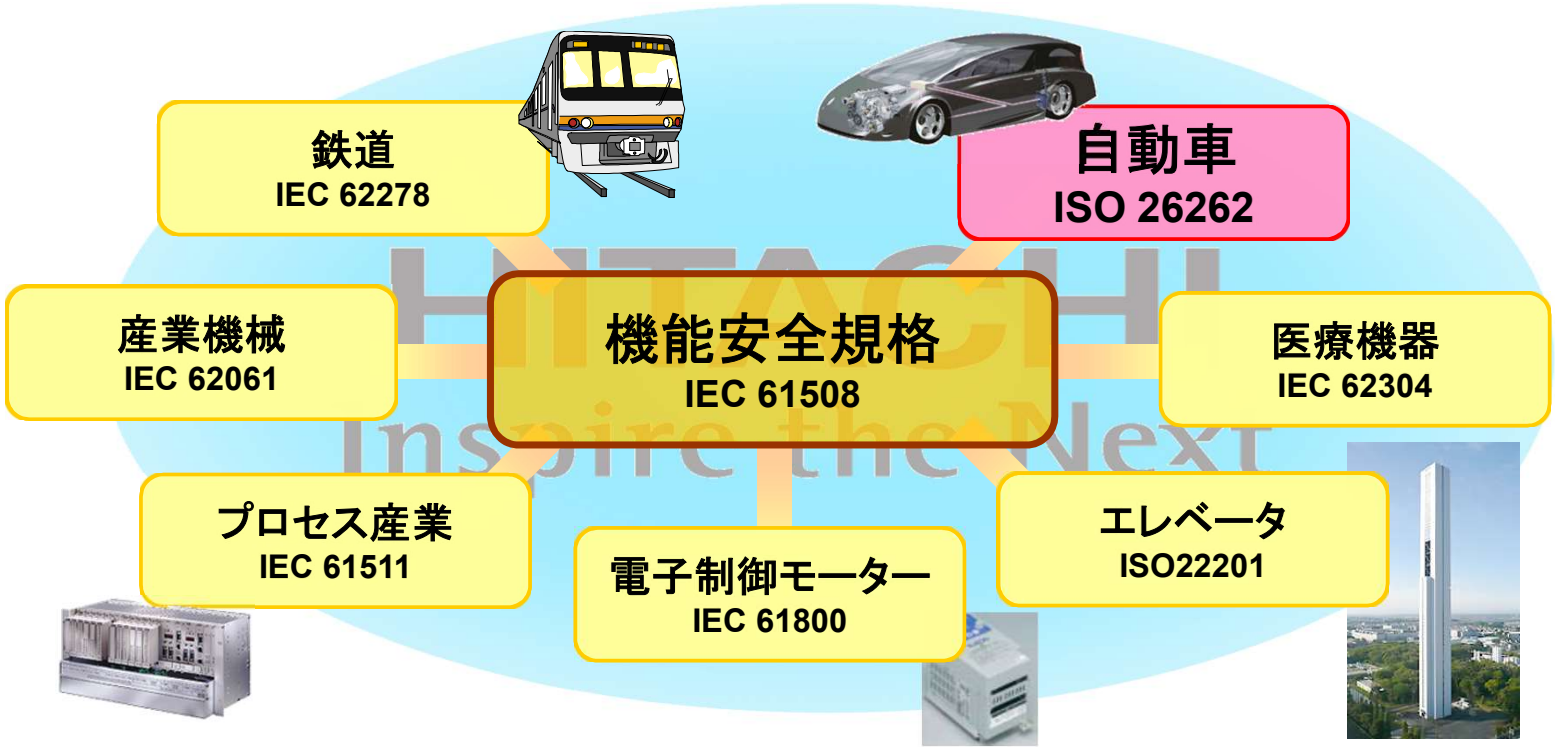
（2）システマティックフォールト（設計不良）の発生を予防する開発手法

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

自動車用機能安全規格ISO26262

マスター規格であるIEC61508をベースに
自動車用機能安全規格ISO26262が2011年11月に国際規格として発効

日立グループは、自動車産業(ISO26262)分野以外にも、
鉄道、エレベータ、プラント制御など幅広い産業分野で機能安全に取り組み



Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

自動車用機能安全規格ISO26262の要求

HITACHI
Inspire the Next

機能安全の視点で設計・検証したことを示すように求められている

A. ハザード解析・リスク評価を実施して目標安全度水準(ASIL)を設定する

ASIL: Automotive Safety Integrity Level

B. 目標安全度水準(ASIL)を達成するような安全機能のモノづくり

C. 目標が達成されていることを証明する

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

開発手法＆ツールの強化

HITACHI
Inspire the Next

最新の開発手法・ツール活用により、機能安全対応による工数増大を抑制
→さらに高効率・高品質な開発をめざす

ISO26262規格本文中でも、各種の開発手法・開発ツールの活用を推奨

MUST要件

- 安全に関する要件管理およびトレーサビリティ管理ツール
- テストカバレッジ支援ツール
- ハードウェアアーキテクチャ定量評価支援ツール
- ⋮

WANT要件 ➔ 必須ではないが、ISO26262で推奨されている新たな手法

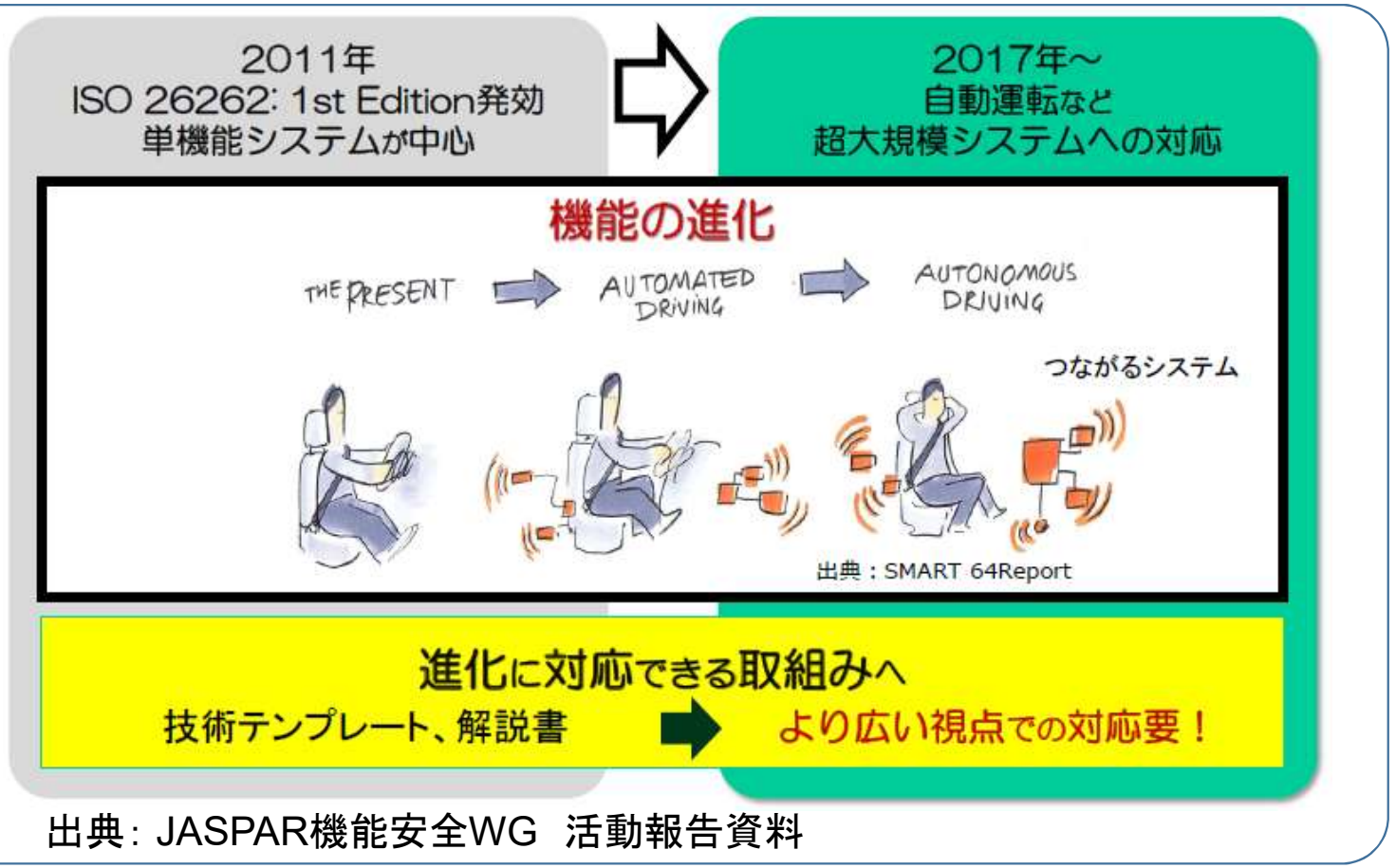
- 形式検証活用支援ツール
- 仮想ECUテスト環境　(vHILSとvFMEA)　今回の紹介事例
- ⋮

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

機能安全にかかわる環境変化と取り組み

HITACHI
Inspire the Next

単機能システム開発から超大規模システム開発へ
⇒　機能安全に関わる開発手法/環境も進化が必要



出典：JASPAR機能安全WG　活動報告資料

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

HITACHI
Inspire the Next

2. MBDの拡張：仮想ECUテスト環境

MBD: Model Based Development
ECU: Electronic Control Unit

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

仮想環境構築の目的

HITACHI
Inspire the Next

機能安全規格ISO26262において、ASIL-CまたはASIL-Dの製品に対しては故障注入テスト(Fault Injection Testing)の実施を強く推奨

実機テストの限界

◆ECUハードウェアの高密度実装化（例：BGA、SoC）
→実機での故障注入が困難に

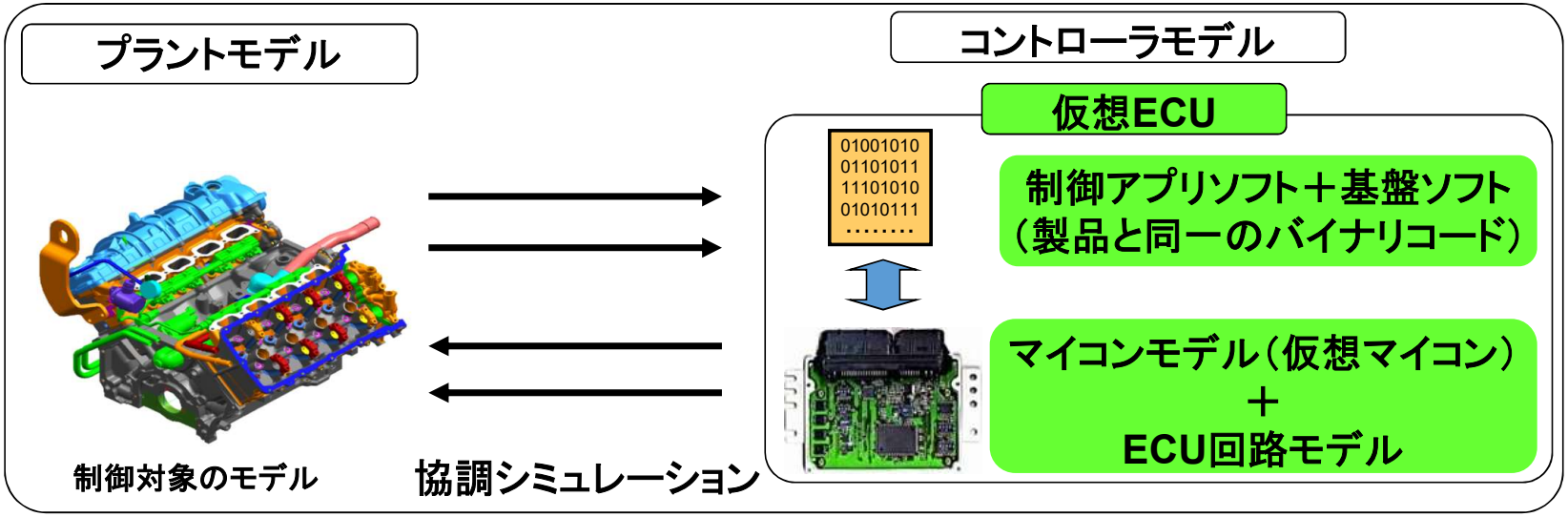
◆フェールセーフからフェールオペレーショナル
→2nd故障まで考慮→膨大なテストケース数
例： 1st故障数(500ケース)＋縮退モード数(5モード) x 2nd故障数(500ケース) = 3,000ケース

シミュレーションを用いた仮想検証技術によりテスト工数を削減

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

MBDの拡張：実ECUから仮想ECUへ

HITACHI
Inspire the Next



仮想ECUの応用

システム・制御：　電子制御システムの実装性評価（演算負荷、実装コスト）、FMEA検証
ソフトウェア：　機能検証、回帰テスト、CPU負荷率評価、OS・ミドルソフト性能評価、網羅的タイミング検証（割込など）、HILS代用
ハードウェア：　マイコン設計（含選定）、ECU設計、ASIC開発
ネットワーク：　通信障害、ネットワーク遅延、分散制御

自動車用機能安全規格ISO26262でも仮想ECUの適宜活用を推奨
・ソフトウェアのテスト環境にプロセッサエミュレータを用いてもよい
・ハードウェアへのフォールト注入テストはモデルベースでもよい

→ 活用拡大が期待される技術

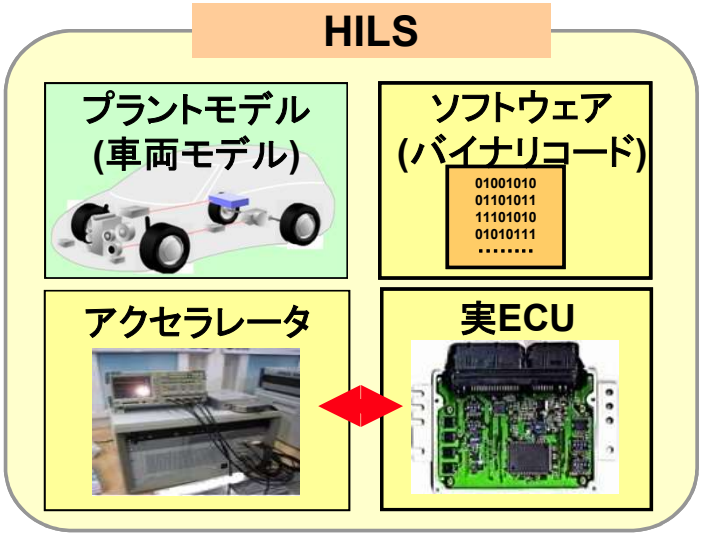
Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

応用例：仮想HILS (バーチャルHILS/vHILS)

HITACHI
Inspire the Next

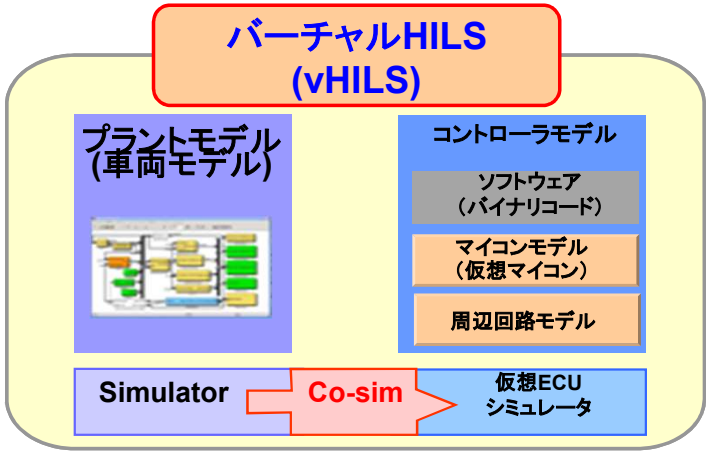
既存手法

HILS (Hardware-in-the-loop Simulator)
■構成： 実ECU＋プラントモデル
■特長
- 製品と同一のバイナリコードを動作検証
- 実機ベースのソフトウェア検証
■用途： ターゲット環境に近いソフトウェア
■短所： コスト、場所、ターゲット環境切替、再現性、観測性など



新手法

バーチャルHILS (vHILS)
■構成： 仮想ECU＋プラントモデル
■特長
- 製品コードでの動作検証
- 実機レスのためクラウド上での並列実行可
- 場所、ターゲット環境切替、再現性、観測性等の実機(HILS)の短所をカバー
- 精度の高いプラントモデル（リアルタイム実行不可）との協調利用可能
■用途： ターゲット環境に近いソフトウェア
HILSの補完利用



Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

HITACHI
Inspire the Next

3. 活用事例：仮想FMEA(vFMEA)検証

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

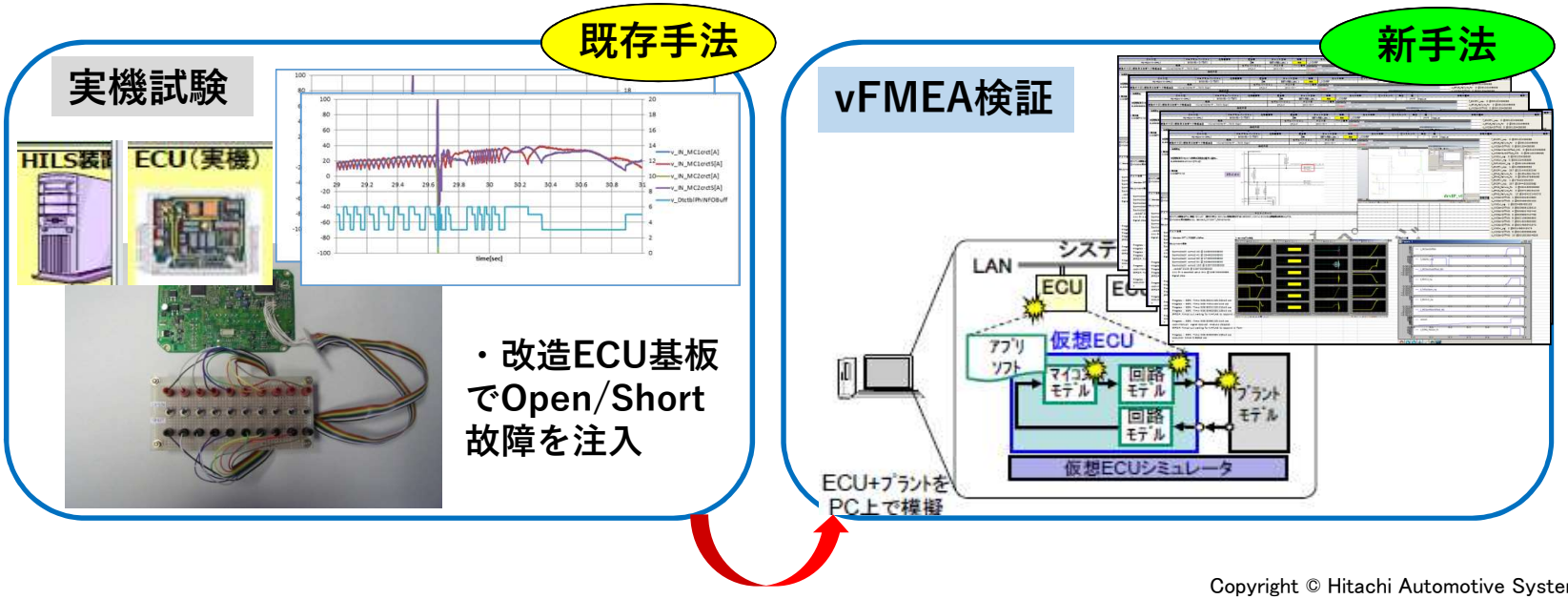
仮想FMEA(vFMEA)検証とは

HITACHI
Inspire the Next

FMEA検証(故障注入テスト)：
フォールト（故障）を発生させたときに、フェールセーフ機能やフェールオペレーショナル機能が有効に動作してシステムの挙動が安全目標を侵害しないことを検証する。

故障注入テストは、従来は実機ベースが主であったが、ISO26262ではモデルベース（シミュレーションベース）を適宜活用してもよいと推奨している。

シミュレーションベースのFMEA検証(故障注入テスト)を、
「仮想FMEA（vFMEA）検証」 あるいは「仮想故障注入テスト」　と呼ぶ。



Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

活用例：量産開発品の仮想FMEA(vFMEA)検証

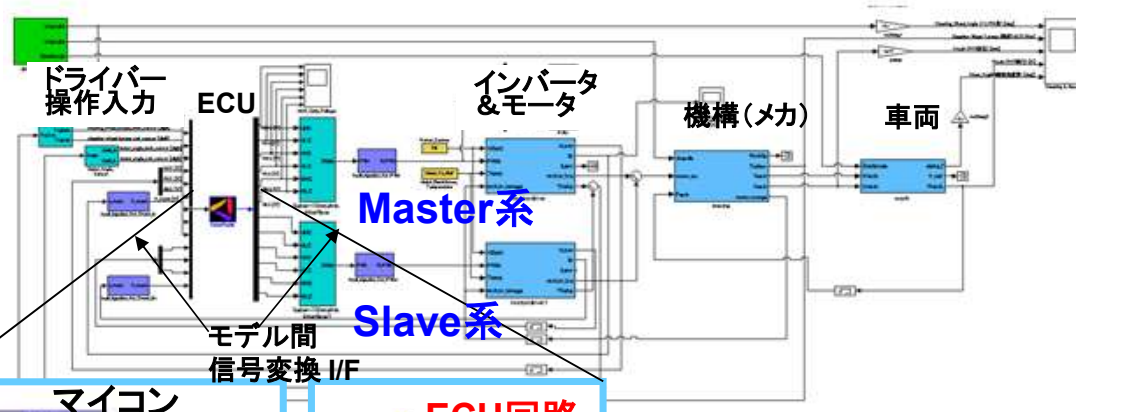
HITACHI
Inspire the Next

■仮想FMEA(vFMEA)検証を量産開発品において活用開始

対象製品： 電動式パワーステアリングシステム （安全度水準：ASIL-D＋フェールオペレーショナル)

特徴： 協調シミュレーションによる制御システムの仮想FMEA検証

テスト対象
制御システムの
モデル構成



ECU搭載
ソフトウェア
（バイナリコード）

011110
100100
101001
・・・

マイコン、入出力回路や
インバータなどを2重化

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

Simscape Electrical導入の動機

以前のプロジェクト
- ECU回路モデルの作成・実行には、他社ツールを利用
- マイコン・ECU回路・プラントの各モデルが異なるツールでの協調シミュレーション実行が煩雑
- ツール間での信号の受け渡しによるオーバーヘッドも課題

MathWorks社様主催の各種イベントにおいて、Simscapeご担当のアプリケーションエンジニアの方々と会話する中で、Simscape Electrical™の回路素子への故障注入機能をご紹介いただいた

ECU回路モデルの作成・実行にSimscape Electrical™を採用

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

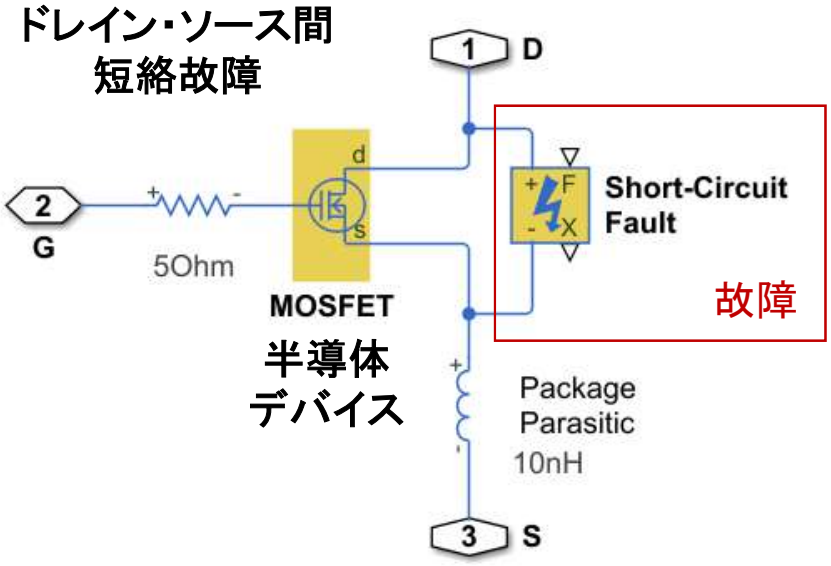
Simscape Electricalを用いた回路素子への故障注入(その1)

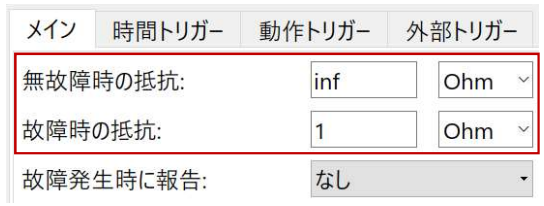
HITACHI
Inspire the Next

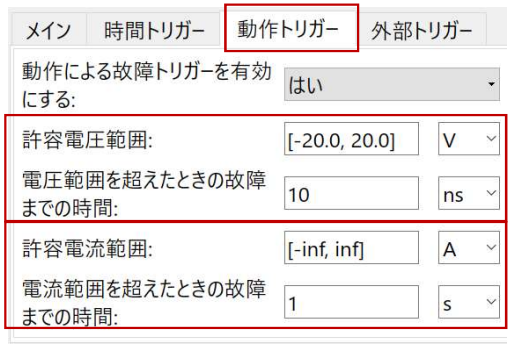
回路故障 (断線・短絡)

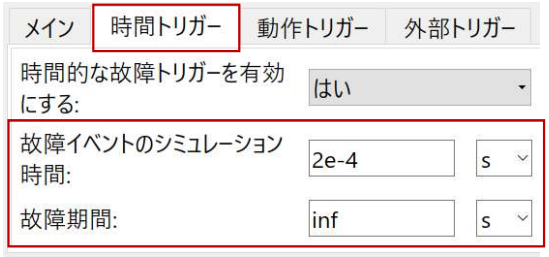
MathWorks Japan様ご提供資料

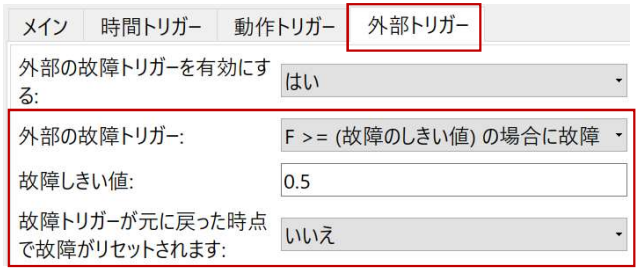
回路接続・コンポーネントの故障を、指定した時間、許容範囲の超過、外部トリガーで発生させる









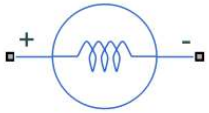


コンポーネント故障

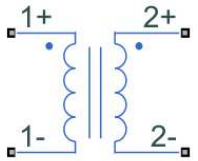
Resistor

Inductor

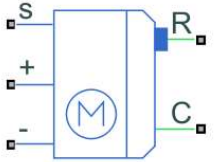
Capacitor



Incandescent Lamp



Mutual Inductor



RC Servo

https://www.mathworks.com/help/physmod/sps/examples/mosfet-fault-in-buck-converter.html

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

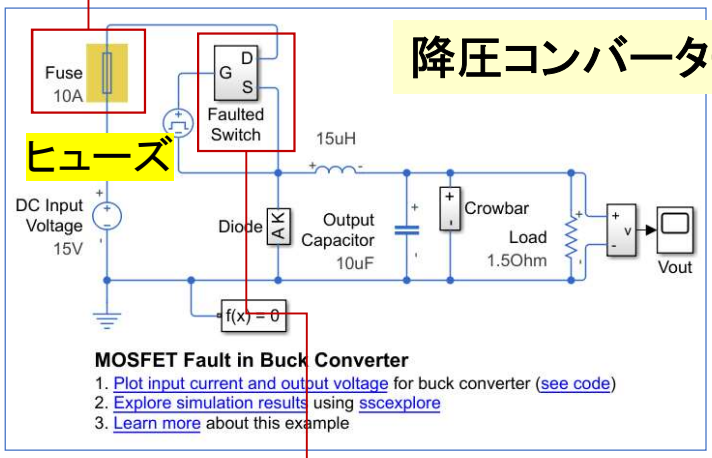
Simscape Electricalを用いた回路素子への故障注入(その2)

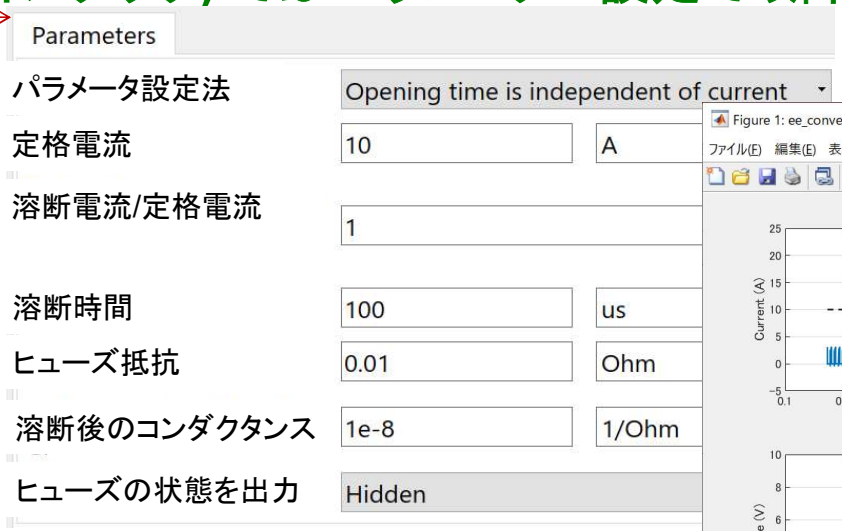
HITACHI
Inspire the Next

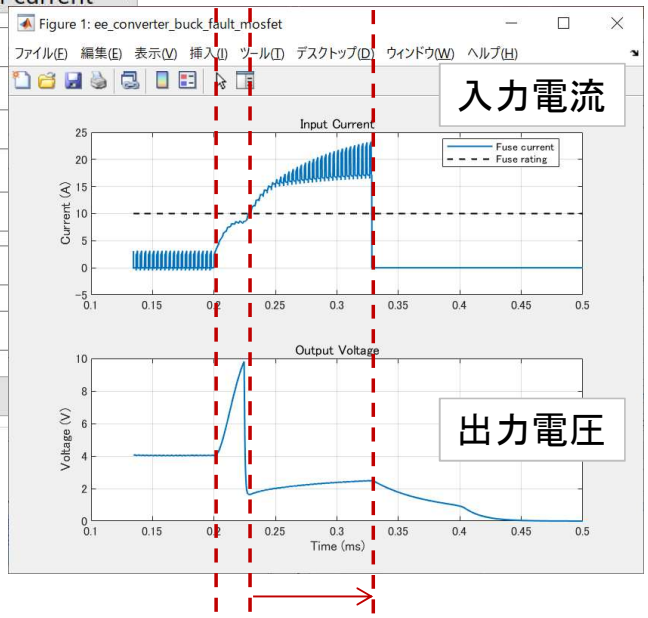
回路故障 (断線、短絡)

MathWorks Japan様ご提供資料

→ 他にも、受動素子 (RLC、相互インダクタ) ではパラメーター設定で故障の入れ込みが可能

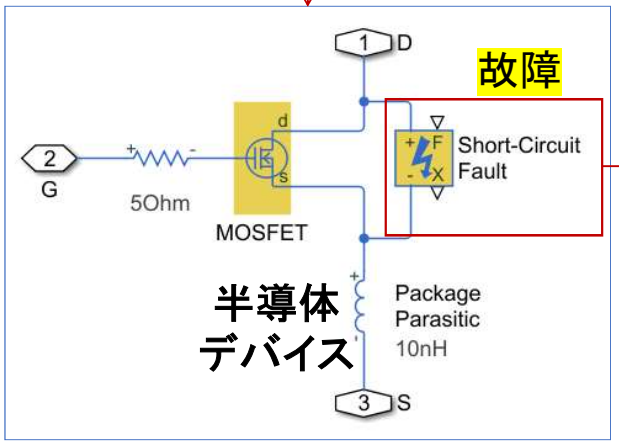


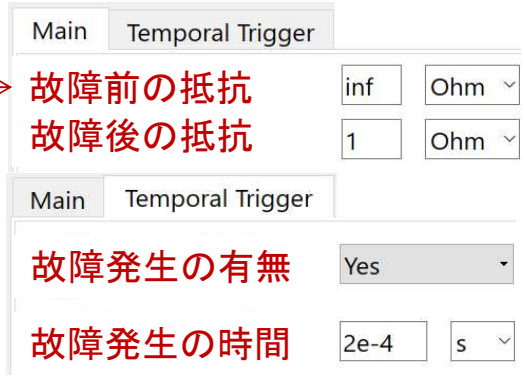




MOSFETが故障

ヒューズが飛ぶ





他に、以下の故障の発生が可能。

- ✓ 許容値以上の電流・電圧が何秒間以上続くと故障させる。
- ✓ 外部トリガーを使って故障させる。

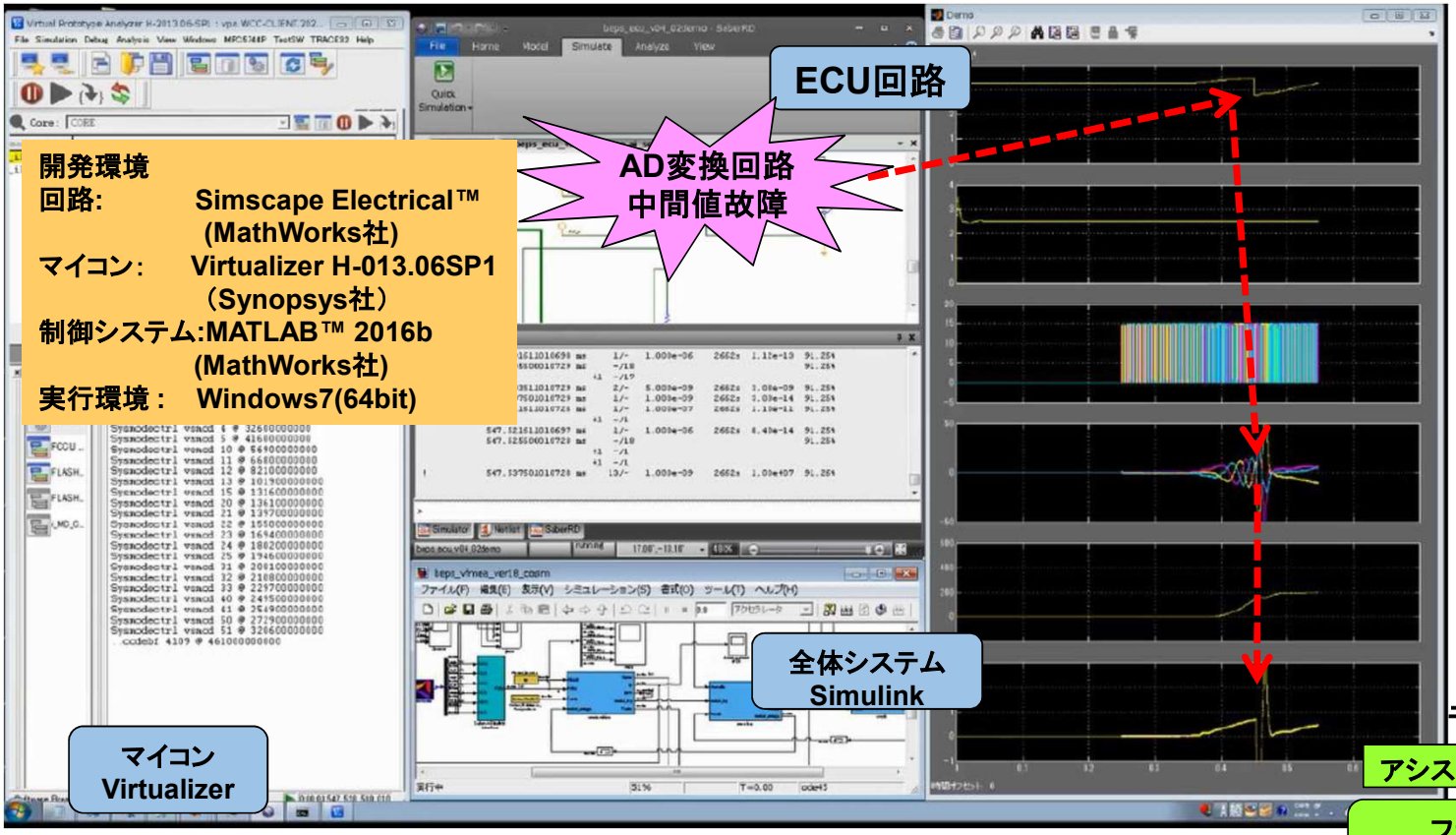
https://www.mathworks.com/help/physmod/sps/examples/mosfet-fault-in-buck-converter.html

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

仮想FMEA(vFMEA)検証のシミュレーション実行の様子

HITACHI
Inspire the Next

1st故障発生　→ 異常検出し縮退運転に遷移　【 1st故障時フェールオペレーショナル】



Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

仮想FMEA(vFMEA)検証のメリット

HITACHI
Inspire the Next

仮想FMEA(vFMEA)検証のメリット

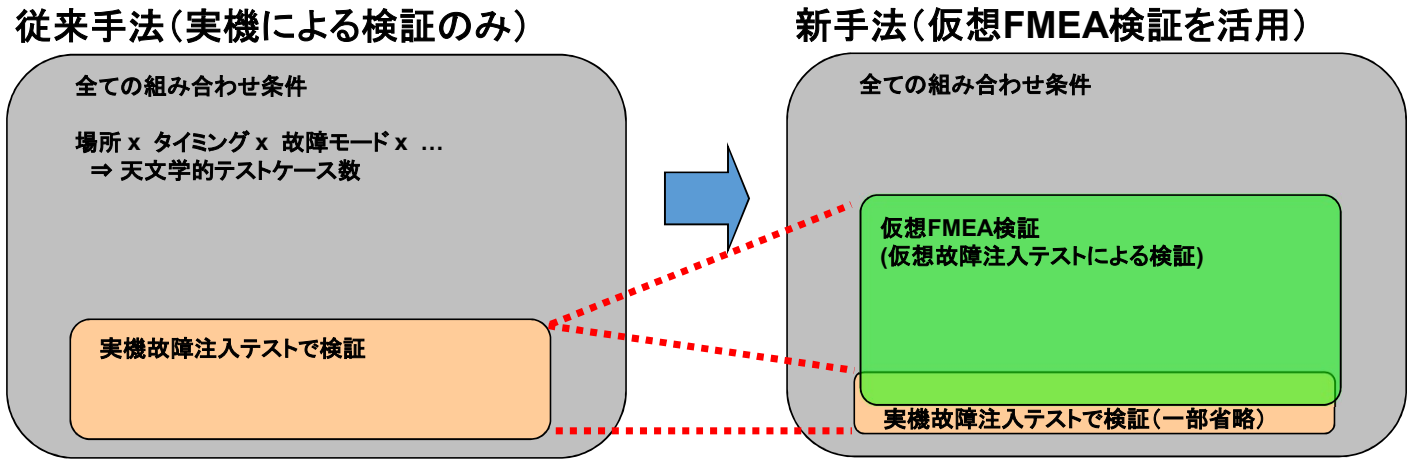
テストカバレッジ向上

＊任意の場所やタイミングで故障注入が可能
＊システム内部状態の任意の挙動を可視化可能

効率向上
開発工程短縮

＊実機を壊さずに検証可能
＊再現性・観測性に優れているので、再テストやトラブル解析が容易
＊クラウド技術活用（並列処理）により短時間で検証可能
＊実機テストでのテスト項目を削減可能

テストカバレッジ向上のイメージ



Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

HITACHI
Inspire the Next

4. まとめ

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

まとめ

■車載電子制御システムの高度化および複雑化が進む中で、機能安全規格
・ISO26262対応を含めて、従来以上に安全、高品質、高効率な設計・検証要
⇒最新の開発手法・ツール活用により、さらに高効率・高品質な開発をめざす

■新たな開発手法・ツールの一例： 仮想ECUテスト環境
・仮想FMEA(vFMEA)検証環境を構築し、機能安全規格に対応した故障注入をシミュレーションで実施可能にした
・仮想FMEA検証を、電動式パワーステアリングの故障注入テストに適用
・ECU回路モデルの作成・実行にSimscape Electrical™を活用
・従来の実機ベースでは困難なテスト項目(例：中間値故障)もカバーできた

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved

ご清聴ありがとうございました

Copyright © Hitachi Automotive Systems, Ltd. All rights reserved