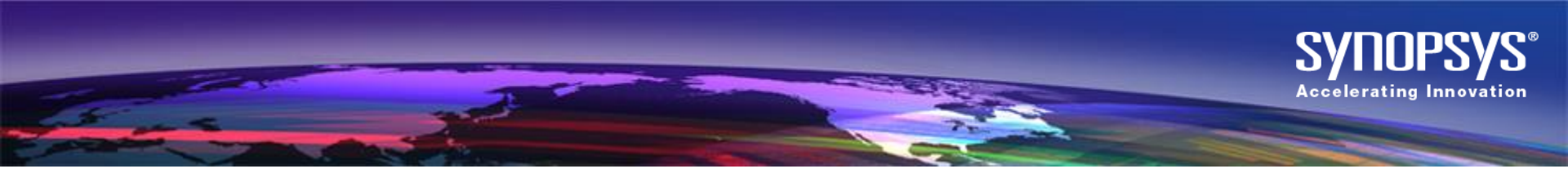


機能安全アプリケーションの
モデリングとシミュレーション

CONFIDENTIAL INFORMATION

The following material is confidential information of Synopsys and is being disclosed to you pursuant to a non-disclosure agreement between you or your employer and Synopsys. The material being disclosed may only be used as permitted under such non-disclosure agreement.

IMPORTANT NOTICE

In the event information in this presentation reflects Synopsys' future plans, such plans are as of the date of this presentation and are subject to change. Synopsys is not obligated to develop the software with the features and functionality discussed in these materials. In any event, Synopsys' products may be offered and purchased only pursuant to an authorized quote and purchase order or a mutually agreed upon written contract.

目的

- Saberの機能安全アプリケーションの有用性の説明
- Saber機能安全活用の実際（ボッシュ社の例）
  - ツール固有の課題
  - フローおよびインターフェースの課題
- その他のアプリケーションの事例
  - 安全機構の開発および検証
  - システムの診断およびカバレッジ
  - シミュレーションによる安全分析の加速化

課題と解決

課題の定義

設計が安全に関する仕様をみたしているかどうか？

OEM

アイテム定義

ハザード＆リスク
アセスメント

機能安全
コンセプト

Tier-1

システム設計
技術安全要求仕様

故障モードと影響
解析(FMEA)

- システムに期待される動作
- **システムに「期待されない」動作**

?

- 設計仕様
- 使用部品
- **故障モード**

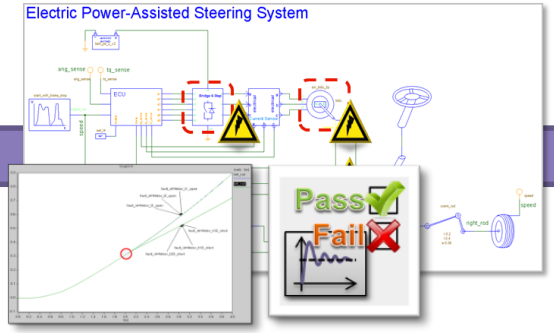
カバレッジ

精度

コスト

Saberによる機能安全ソリューション

Saber FS (機能安全オプション)により、不具合がどの故障モードから生じたかを即座に提示



- システムに期待される動作
- **システムに「期待されない」動作**

- 設計仕様
- 使用部品
- **故障モード**

Saberによる26262安全規格対応

アイテム定義
ハザード分析と
リスクアセスメント
安全目標

どの動作状態でどんな
ハザードが問題となるか？

安全目標を阻害する
主な故障状態

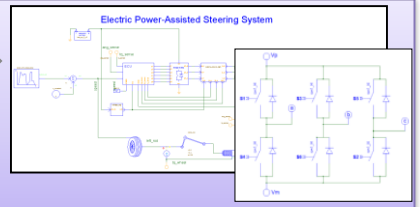
システム設計

何がどう接続されており、なに
が正常動作、異常動作？

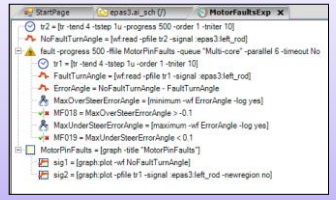
故障モードと影響解析
(FMEA)

どのようにハードウエア部品
が故障するのか？

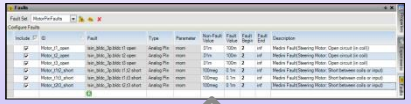
Saberの設計



Saberの試験

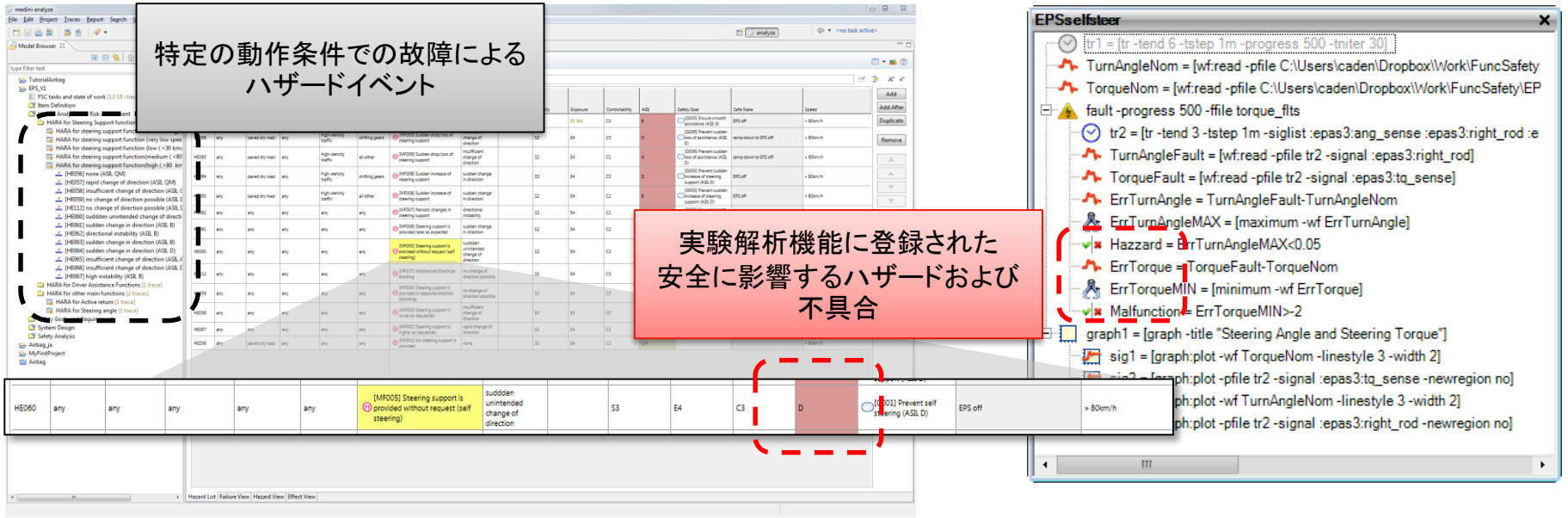


Saberで欠陥定義



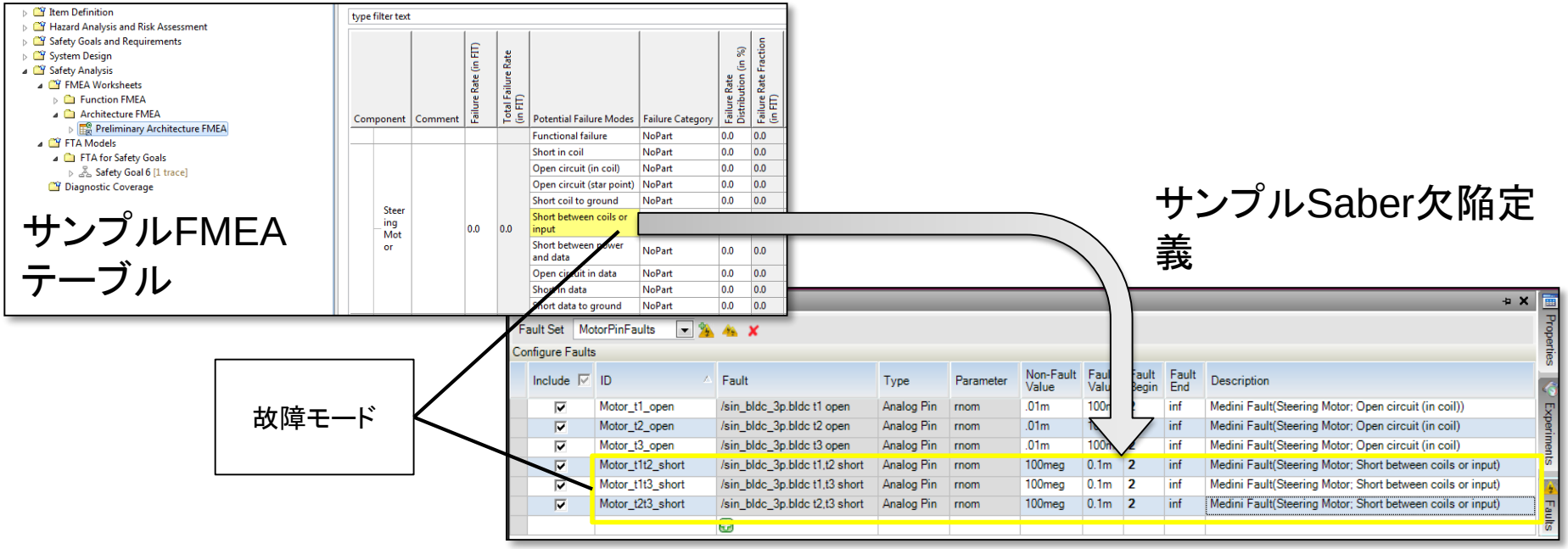
故障モード

Saberによるハザード分析・リスクアセスメント（HARA）



数10～数100に及ぶ安全に影響する故障状態を定義

Saberによる故障モードと影響解析（FMEA）欠陥の記述



100～1000の想定される故障モード

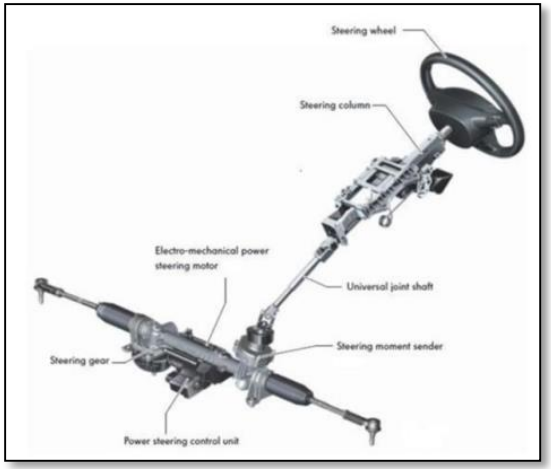
故障モードと効果解析は10万に及ぶ安全評価シナリオに対応

Saberによる故障モードと影響解析(FMEA)

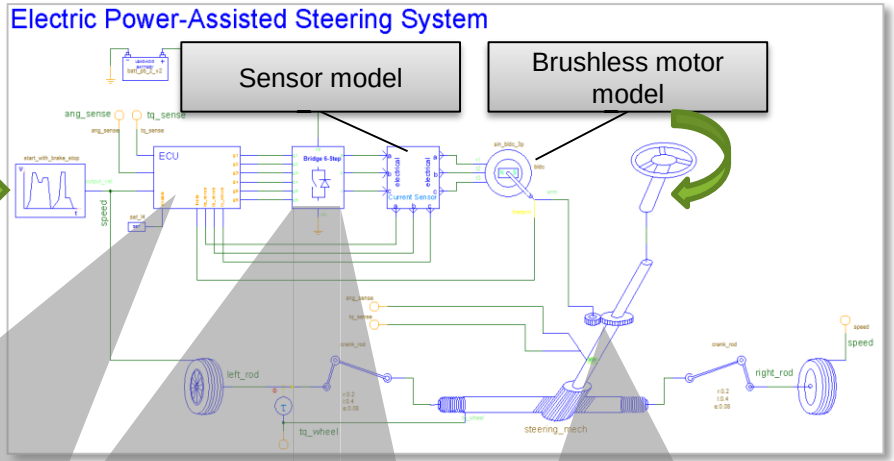
- 一つのSaberデザインで多数のハザード・不具合ケースをシミュレーション可能
- 各種のハザード・不具合をテストするSaberによる評価実験を即座に用意
- FMEA故障モードにSaberの欠陥記述が対応
- Saberシミュレーション結果により:
  - 支配的な故障モードと効果・不具合を明確に判別
  - 安全機構の設計および検証が可能

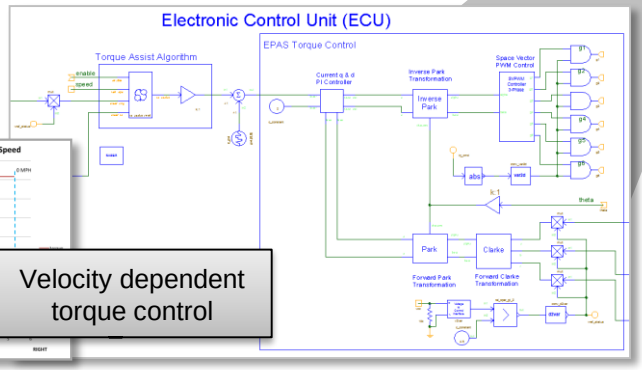
電動アシストステアリングの事例

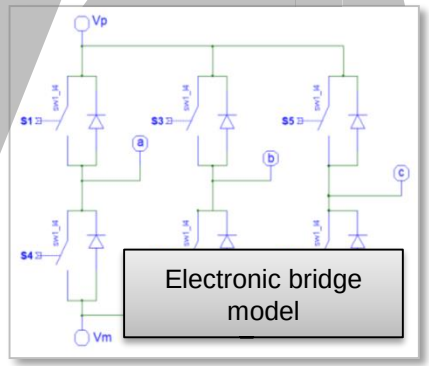
EPSシステムモデル

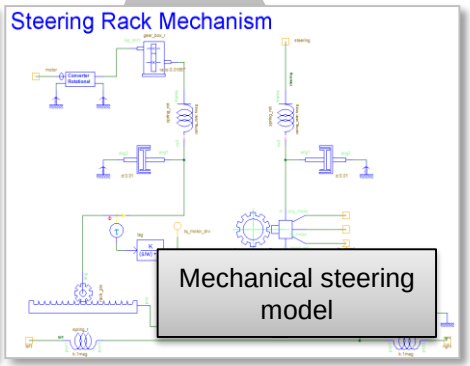


Model inputs







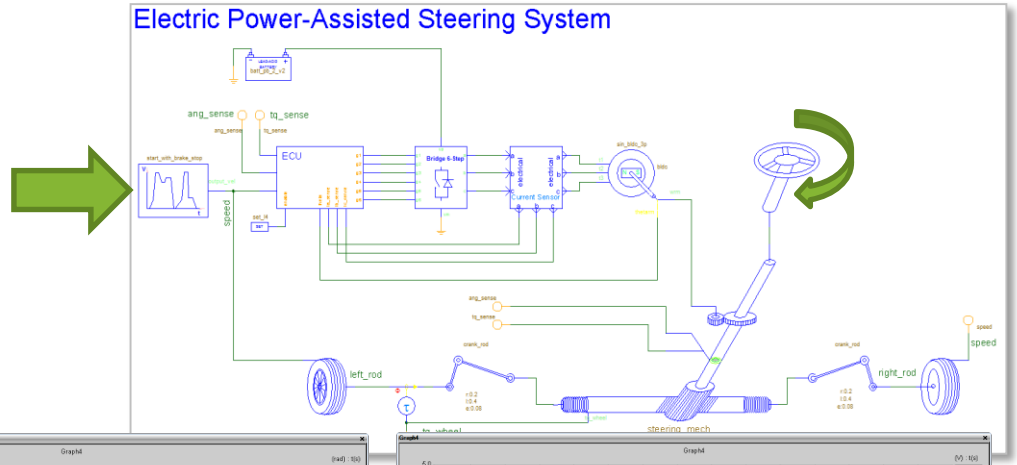


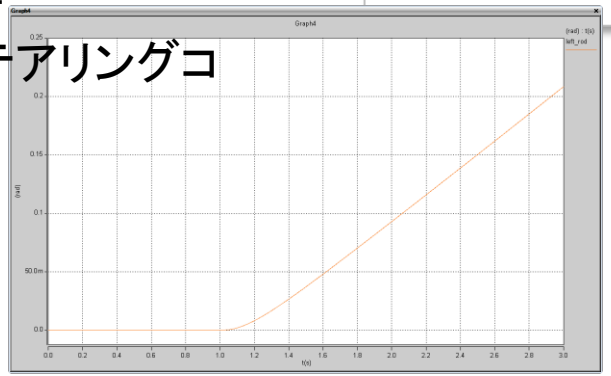
安全シミュレーションシナリオ

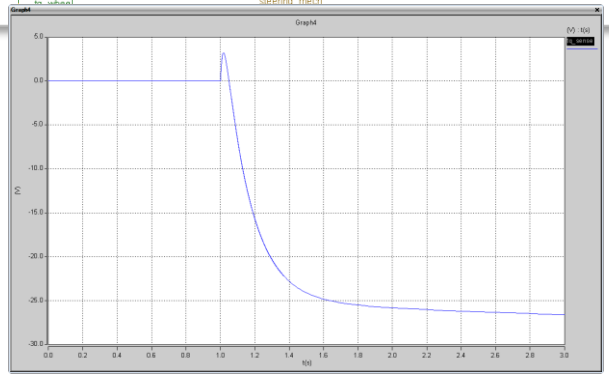
- ハザード：30km/h走行時のセルフステアリング
- リスクアセスメント: ASIL D
- 主要故障状態：意図しないトルクアシスト
- 想定される故障モード:
  - モータ巻線ショート
  - モータ運転状態の縮退故障
  - ECUリファレンス電圧ピンの開放
  - モータ運転スイッチの短絡
  - トルクフィードバック回路の開放

定常モデル性能

- 30 km/h一定速度入力
- 運転者による5Nmトルク指令
- 主な計測
  - 車輪の角度変位
  - モータからのステアリングコラムへのトルク

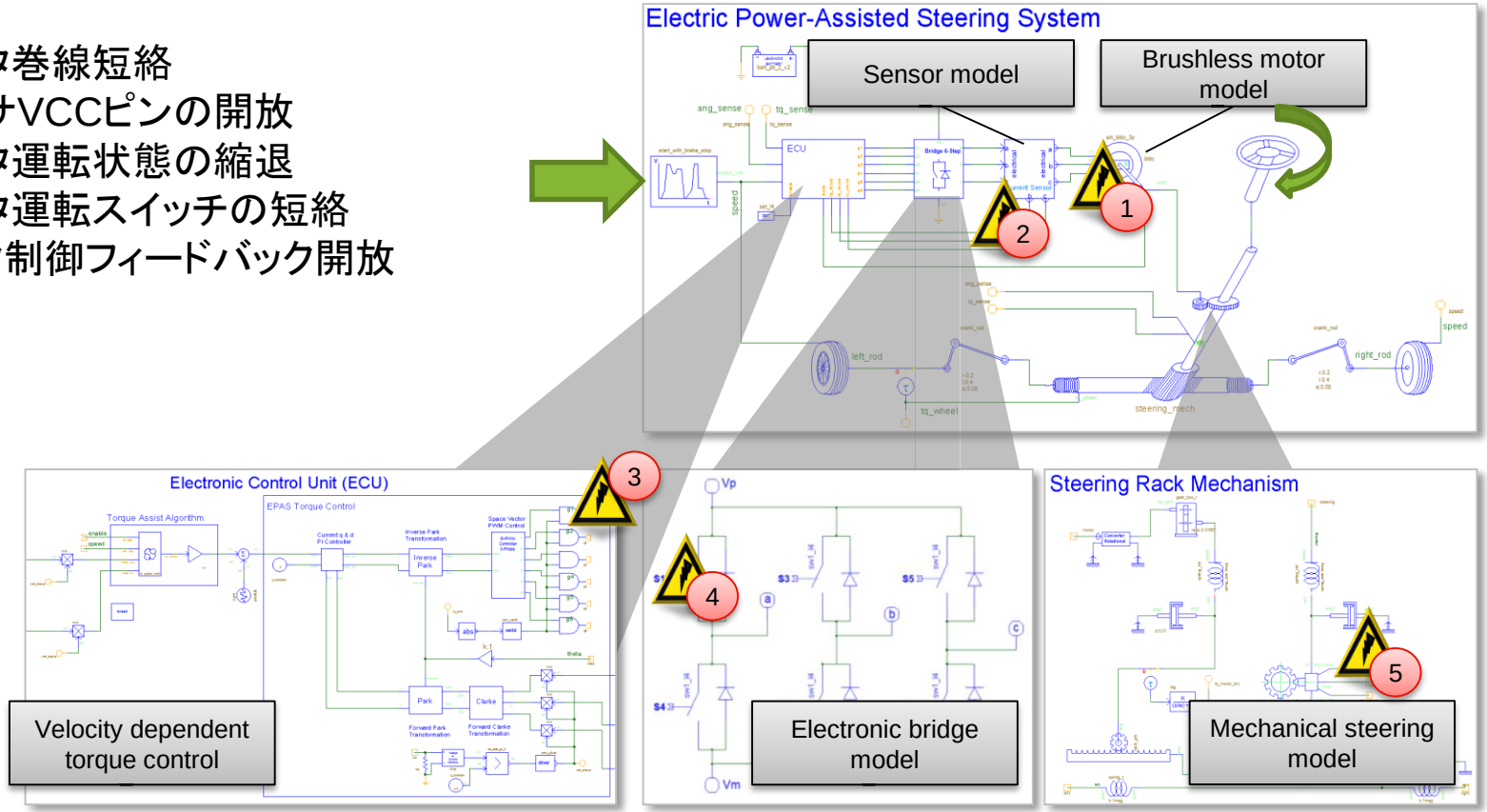




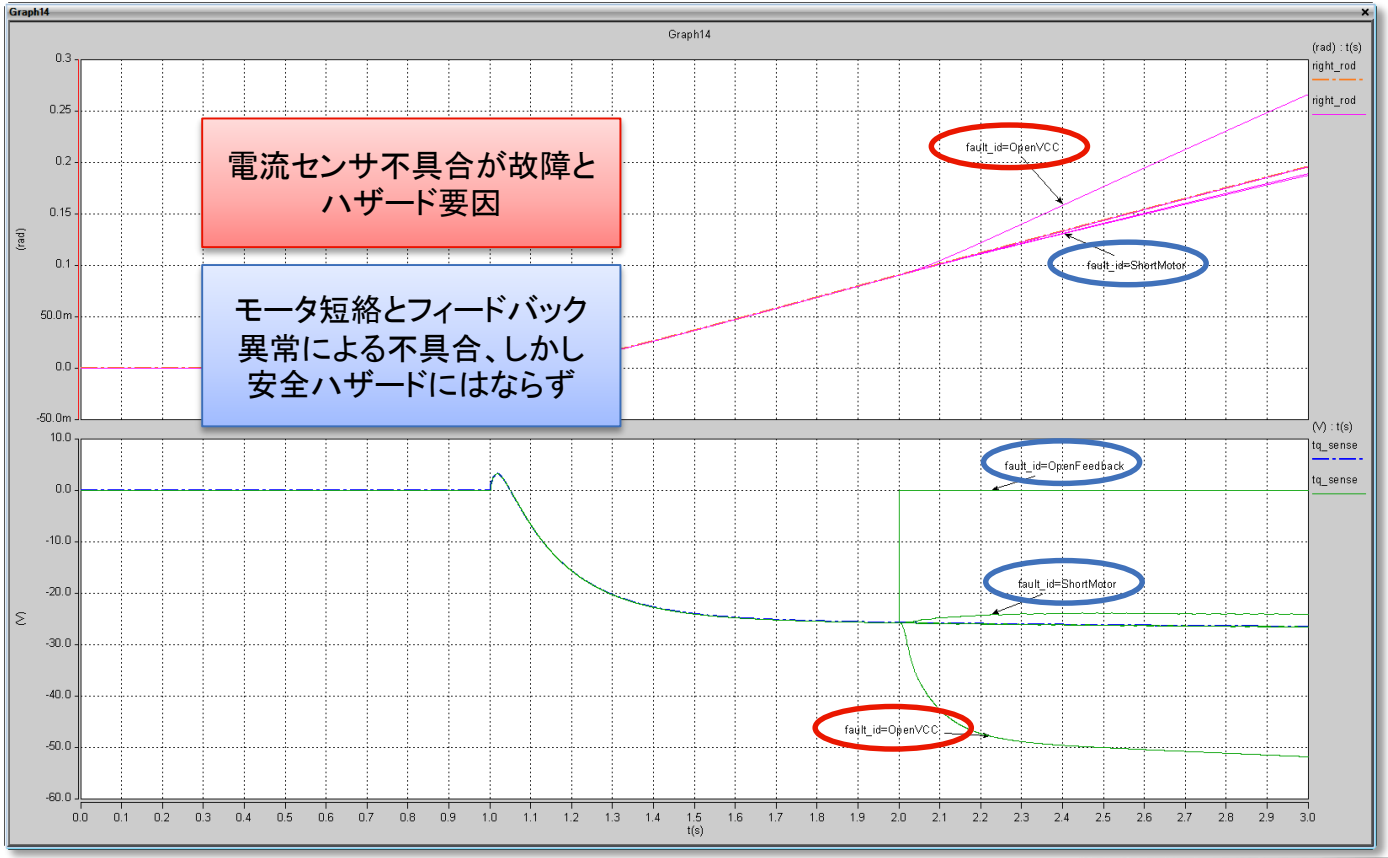


故障モード記述

1. モータ巻線短絡
2. センサVCCピンの開放
3. モータ運転状態の縮退
4. モータ運転スイッチの短絡
5. トルク制御フィードバック開放



欠陥シミュレーション結果



欠陥シミュレーション結果

EPSselfsteer.ai_exptlog

Task Label	Task Definition	Description	Task Result	Task Status
fault	fault -progress 500 -ffile torque_flts		1 Failed	Complete w/ Failures
fault=OpenVCC	Fault=/isense vcc open, Fault Value=1...	current sensor loses power		Fail
Hazzard	Hazzard = ErrTurnAngleMAX<0.05		0	Fail
Malfunction	Malfunction = ErrTorqueMIN>-2		0	Fail
fault=OpenMotor	Fault=/sin_bldc_3p.bldc t1 open, Fault..	open circuit motor windings		Complete
Hazzard	Hazzard = ErrTurnAngleMAX<0.05		1	Pass
Malfunction	Malfunction = ErrTorqueMIN>-2		1	Pass
fault=ShortMotor	Fault=/sin_bldc_3p.bldc t1,t2 short, Fa...	short circuit motor windings		Complete
Hazzard	Hazzard = ErrTurnAngleMAX<0.05		1	Pass
Malfunction	Malfunction = ErrTorqueMIN>-2		1	Pass
fault=StuckLogic	Fault=/ecu_cntrl/and2_l4.and2_l4_1 ou...	digital control failure		Complete
Hazzard	Hazzard = ErrTurnAngleMAX<0.05		1	Pass
Malfunction	Malfunction = ErrTorqueMIN>-2		1	Pass
fault=OpenFeedback	Fault=/mechanism steer_col_tq open,...	broken feedback		Complete
Hazzard	Hazzard = ErrTurnAngleMAX<0.05		1	Pass
Malfunction	Malfunction = ErrTorqueMIN>-2		1	Pass