

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.

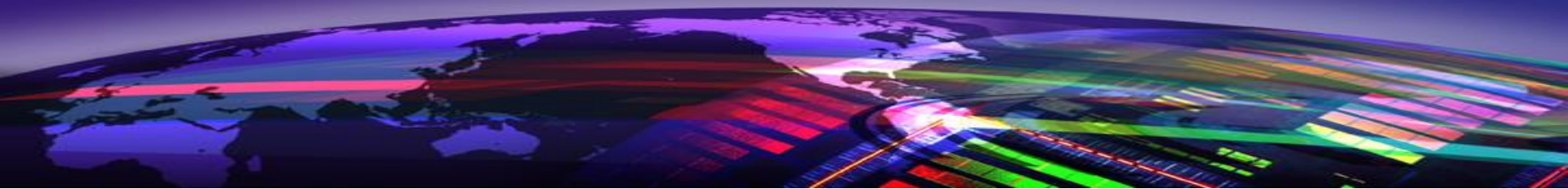
IMPORTANT NOTICE

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機能安全活用の実例(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

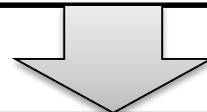
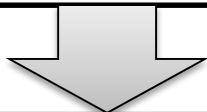
機能安全
コンセプト



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

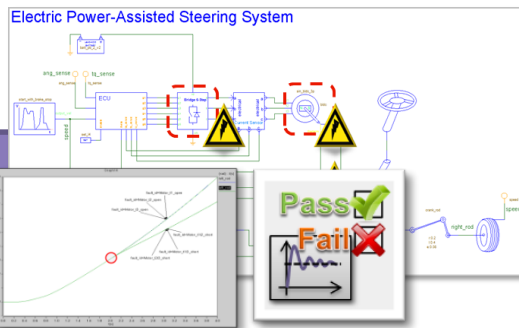
精度

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？

システム設計

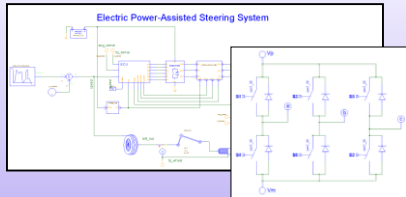
何がどう接続されており、なに
が正常動作、異常動作？

故障モードと影響解析
(FMEA)

どのようにハードウェア部品
が故障するのか？

安全目標を阻害する
主な故障状態

Saberの設計



Saberの試験

```
Workspace  spas3_at_3ch (0)  MotorFaultExp x
k2 = [r-tend 4-step tu-progress 500-order 1-order 10]
NoFaultTurnAngle = [uf-read-pfile tr2-signal spas3_left_rod]
fault-progress 500-File MotorPinFaults-queue "Multi-core"-parallel 6-timeout No
r1 = [r-tend 4-step tu-order 1-order 10]
FaultTurnAngle = [uf-read-pfile tr1-signal spas3_left_rod]
ErrorAngle = NoFaultTurnAngle - FaultTurnAngle
MaxOverSteerErrorAngle = [minimum -of ErrorAngle -log yes]
MF015 = MaxOverSteerErrorAngle > -0.1
MaxUnderSteerErrorAngle = [maximum -of ErrorAngle -log yes]
NF015 = MaxUnderSteerErrorAngle < 0.1
MotorPinFaults = [graph-title "MotorPinFaults"]
sig1 = [graph-plot -of NoFaultTurnAngle]
sig2 = [graph-plot -of tr1-signal spas3_left_rod-newregion no]
```

Saberで欠陥定義

Include ID	Fault	Type	Severity	Max Fail	Min Fail	Exp	Description
MF015	MaxOverSteerErrorAngle > -0.1	Warning	1	1000	1	1000	Max OverSteerErrorAngle > -0.1
NF015	MaxUnderSteerErrorAngle < 0.1	Warning	1	1000	1	1000	Max UnderSteerErrorAngle < 0.1
MotorPinFaults	MotorPinFaults	Warning	1	1000	1	1000	MotorPinFaults

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)

特定の動作条件での故障による
ハザードイベント

Item	Exposure	Consequence	ASIL	Safety Goal	Safety Date	Speed
HE000	any	steered dry road	any	high-density traffic	all other	IMF005 Steering support is provided without request (self steering)
HE001	any	steered dry road	any	high-density traffic	all other	sudden unintended change of direction
HE002	any	steered dry road	any	high-density traffic	all other	
HE003	any	steered dry road	any	high-density traffic	all other	
HE004	any	steered dry road	any	high-density traffic	all other	
HE005	any	steered dry road	any	high-density traffic	all other	
HE006	any	steered dry road	any	high-density traffic	all other	
HE007	any	steered dry road	any	high-density traffic	all other	
HE008	any	steered dry road	any	high-density traffic	all other	
HE009	any	steered dry road	any	high-density traffic	all other	
HE010	any	steered dry road	any	high-density traffic	all other	
HE011	any	steered dry road	any	high-density traffic	all other	
HE012	any	steered dry road	any	high-density traffic	all other	
HE013	any	steered dry road	any	high-density traffic	all other	
HE014	any	steered dry road	any	high-density traffic	all other	
HE015	any	steered dry road	any	high-density traffic	all other	
HE016	any	steered dry road	any	high-density traffic	all other	
HE017	any	steered dry road	any	high-density traffic	all other	
HE018	any	steered dry road	any	high-density traffic	all other	
HE019	any	steered dry road	any	high-density traffic	all other	
HE020	any	steered dry road	any	high-density traffic	all other	
HE021	any	steered dry road	any	high-density traffic	all other	
HE022	any	steered dry road	any	high-density traffic	all other	
HE023	any	steered dry road	any	high-density traffic	all other	
HE024	any	steered dry road	any	high-density traffic	all other	
HE025	any	steered dry road	any	high-density traffic	all other	
HE026	any	steered dry road	any	high-density traffic	all other	
HE027	any	steered dry road	any	high-density traffic	all other	
HE028	any	steered dry road	any	high-density traffic	all other	
HE029	any	steered dry road	any	high-density traffic	all other	
HE030	any	steered dry road	any	high-density traffic	all other	
HE031	any	steered dry road	any	high-density traffic	all other	
HE032	any	steered dry road	any	high-density traffic	all other	
HE033	any	steered dry road	any	high-density traffic	all other	
HE034	any	steered dry road	any	high-density traffic	all other	
HE035	any	steered dry road	any	high-density traffic	all other	
HE036	any	steered dry road	any	high-density traffic	all other	
HE037	any	steered dry road	any	high-density traffic	all other	
HE038	any	steered dry road	any	high-density traffic	all other	
HE039	any	steered dry road	any	high-density traffic	all other	
HE040	any	steered dry road	any	high-density traffic	all other	
HE041	any	steered dry road	any	high-density traffic	all other	
HE042	any	steered dry road	any	high-density traffic	all other	
HE043	any	steered dry road	any	high-density traffic	all other	
HE044	any	steered dry road	any	high-density traffic	all other	
HE045	any	steered dry road	any	high-density traffic	all other	
HE046	any	steered dry road	any	high-density traffic	all other	
HE047	any	steered dry road	any	high-density traffic	all other	
HE048	any	steered dry road	any	high-density traffic	all other	
HE049	any	steered dry road	any	high-density traffic	all other	
HE050	any	steered dry road	any	high-density traffic	all other	

実験解析機能に登録された
安全に影響するハザードおよび
不具合

```

EPSselfsteer
tr1 = [tr -tend 6 -tstep 1m -progress 500 -triter 30]
TurnAngleNom = [wf:read -pfile C:\Users\caden\Dropbox\Work\FuncSafety\
TorqueNom = [wf:read -pfile C:\Users\caden\Dropbox\Work\FuncSafety\EP
fault -progress 500 -ffile torque_flt
tr2 = [tr -tend 3 -tstep 1m -siglist :epas3:ang_sense :epas3:right_rod :
TurnAngleFault = [wf:read -pfile tr2 -signal :epas3:right_rod]
TorqueFault = [wf:read -pfile tr2 -signal :epas3:tq_sense]
ErrTurnAngle = TurnAngleFault-TurnAngleNom
ErrTurnAngleMAX = [maximum -wf ErrTurnAngle]
Hazzard = ErrTurnAngleMAX<0.05
ErrTorque = TorqueFault-TorqueNom
ErrTorqueMIN = [minimum -wf ErrTorque]
Malfunction = ErrTorqueMIN>2
graph1 = [graph -title "Steering Angle and Steering Torque"]
sig1 = [graph:plot -wf TorqueNom -linestyle 3 -width 2]
sig2 = [graph:plot -pfile tr2 -signal :epas3:tq_sense -newregion no]
sig3 = [graph:plot -pfile tr2 -signal :epas3:right_rod -newregion no]
    
```

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

type filter text

Component Comment Failure Rate (in FIT) Total Failure Rate (in FIT) Potential Failure Modes Failure Category Failure Rate Distribution (in %) Failure Rate Fraction (in FIT)

Steering Motor or		0.0	0.0	Functional failure	NoPart	0.0	0.0
				Short in coil	NoPart	0.0	0.0
				Open circuit (in coil)	NoPart	0.0	0.0
				Open circuit (star point)	NoPart	0.0	0.0
				Short coil to ground	NoPart	0.0	0.0
				Short between coils or input			
				Short between power and data	NoPart	0.0	0.0
				Open circuit in data	NoPart	0.0	0.0
				Short in data	NoPart	0.0	0.0
				Short data to ground	NoPart	0.0	0.0

サンプルFMEA
テーブル

サンプルSaber欠陥定義

故障モード

Fault Set MotorPinFaults

Configure Faults

Include	ID	Fault	Type	Parameter	Non-Fault Value	Fault Value	Fault Begin	Fault End	Description
<input checked="" type="checkbox"/>	Motor_t1_open	/sin_bldc_3p.bldc t1 open	Analog Pin	rnom	.01m	100m	inf	inf	Medini Fault(Steering Motor: Open circuit (in coil))
<input checked="" type="checkbox"/>	Motor_t2_open	/sin_bldc_3p.bldc t2 open	Analog Pin	rnom	.01m	100m	inf	inf	Medini Fault(Steering Motor: Open circuit (in coil))
<input checked="" type="checkbox"/>	Motor_t3_open	/sin_bldc_3p.bldc t3 open	Analog Pin	rnom	.01m	100m	inf	inf	Medini Fault(Steering Motor: Open circuit (in coil))
<input checked="" type="checkbox"/>	Motor_t1t2_short	/sin_bldc_3p.bldc t1,t2 short	Analog Pin	rnom	100meg	0.1m	2	inf	Medini Fault(Steering Motor: Short between coils or input)
<input checked="" type="checkbox"/>	Motor_t1t3_short	/sin_bldc_3p.bldc t1,t3 short	Analog Pin	rnom	100meg	0.1m	2	inf	Medini Fault(Steering Motor: Short between coils or input)
<input checked="" type="checkbox"/>	Motor_t2t3_short	/sin_bldc_3p.bldc t2,t3 short	Analog Pin	rnom	100meg	0.1m	2	inf	Medini Fault(Steering Motor: Short between coils or input)

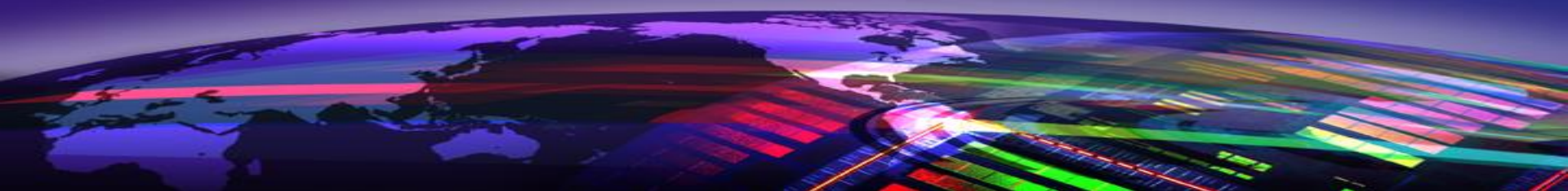
100~1000の想定される故障モード

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

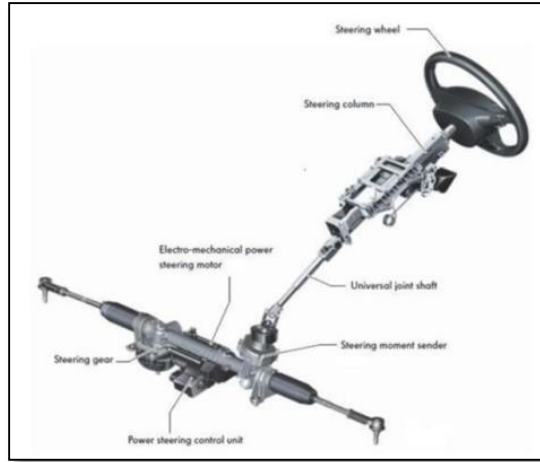
Saberによる故障モードと影響解析(FMEA)

- 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

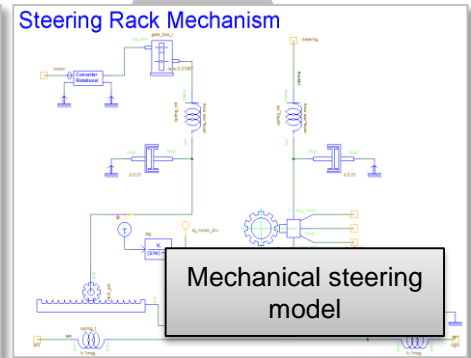
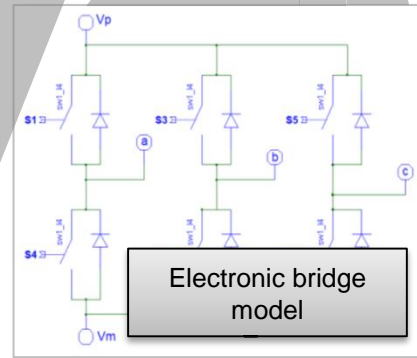
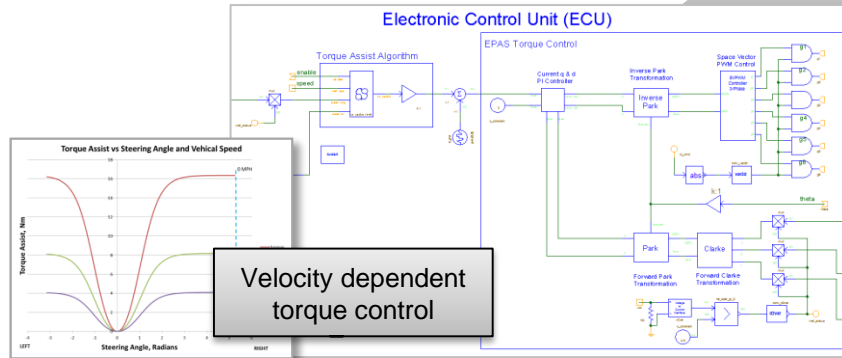
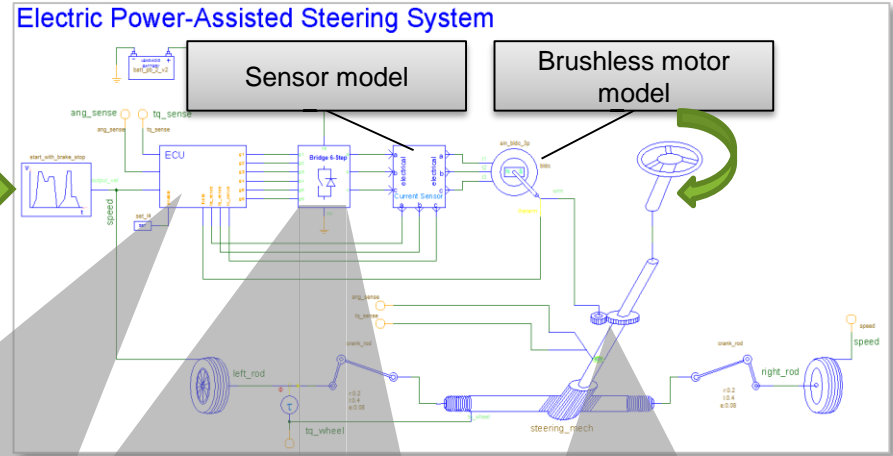
電動アシストステアリングの事例



EPSシステムモデル



Model inputs



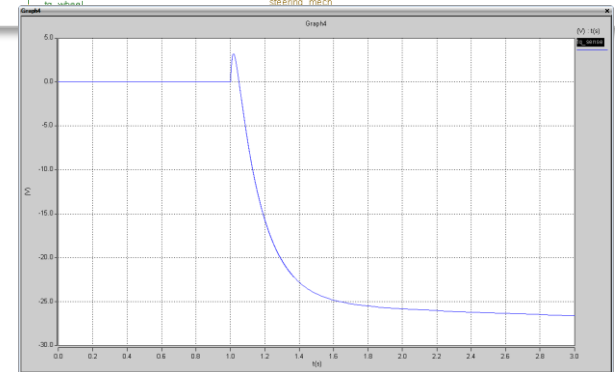
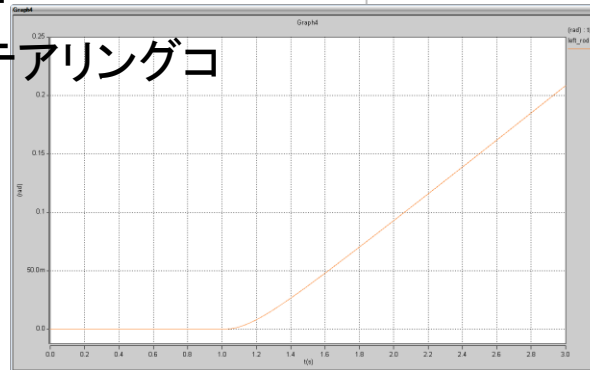
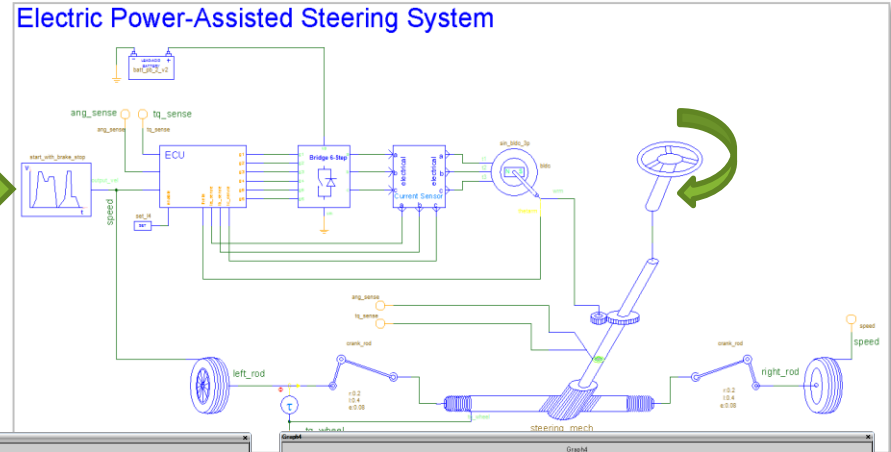
安全シミュレーションシナリオ

- 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



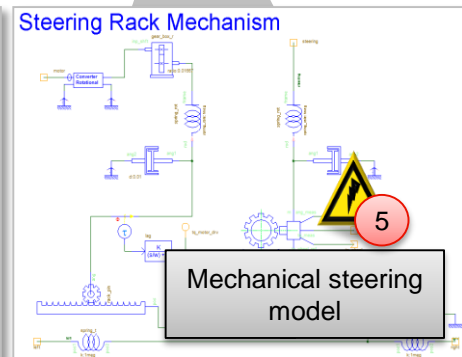
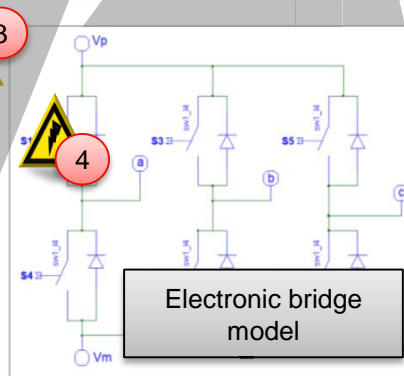
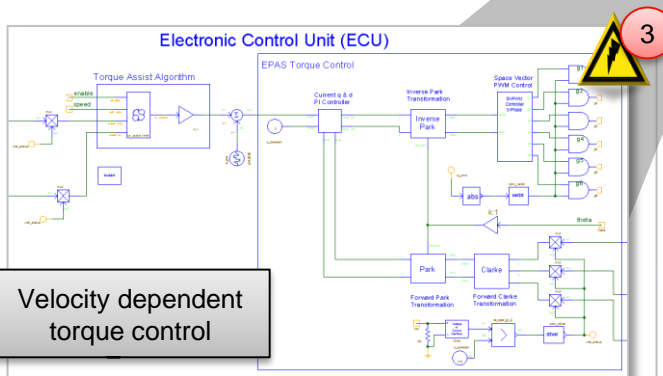
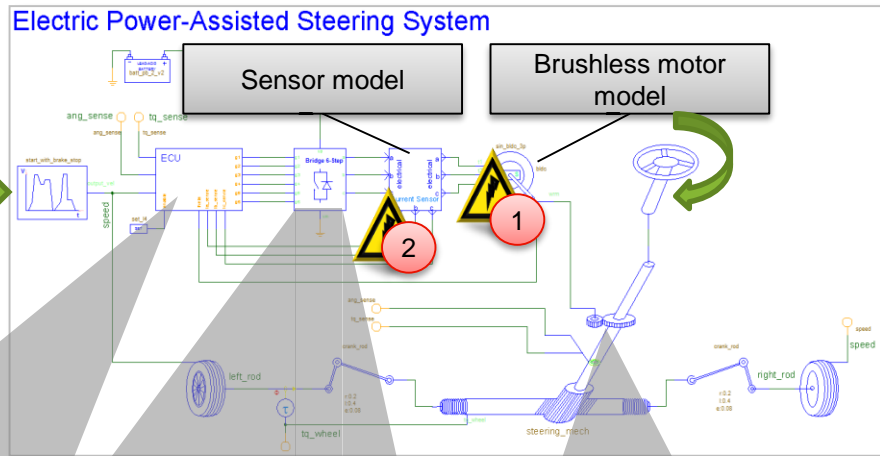
定常モデル性能

- 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

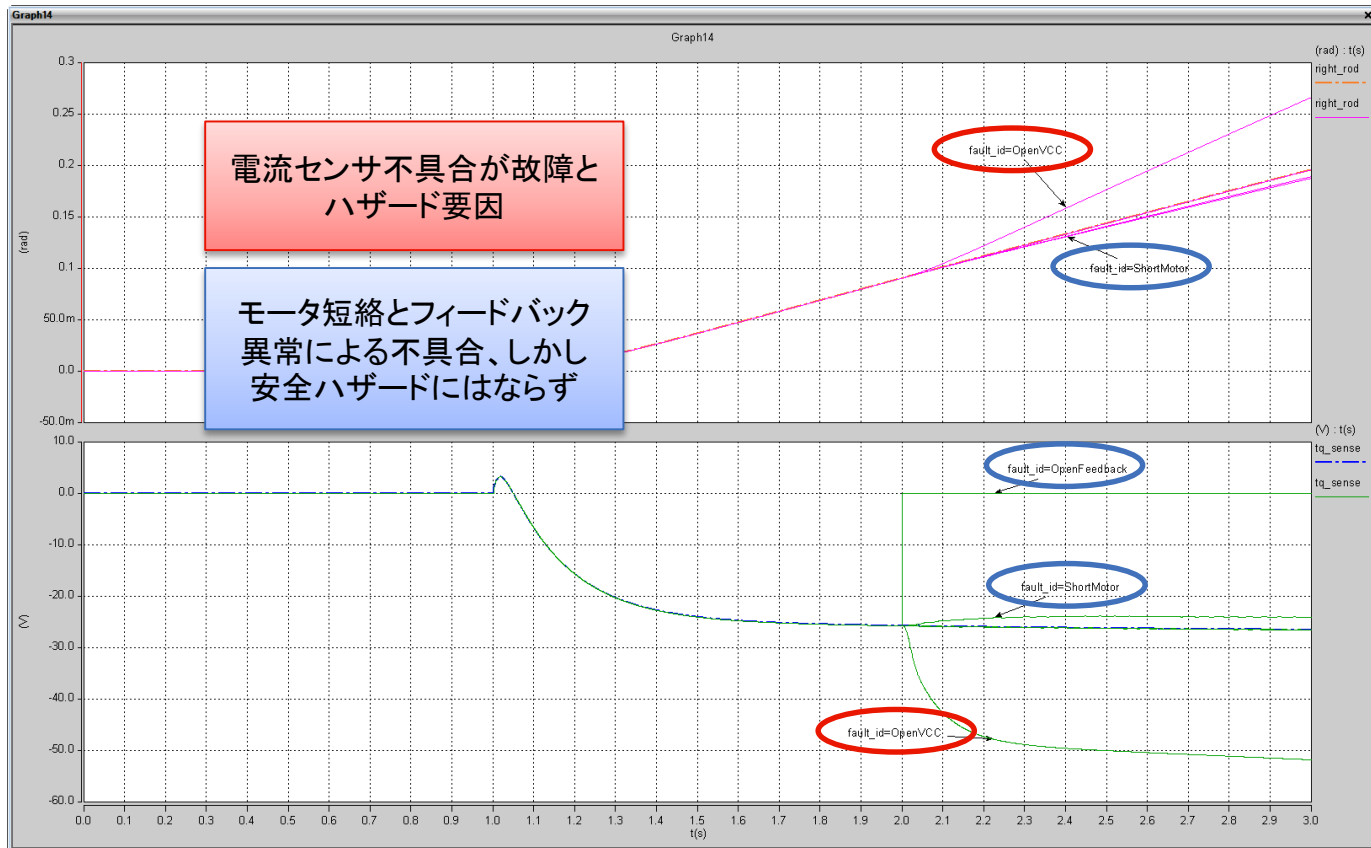


故障モード記述

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

Task Label	Task Definition	Description	Task Result	Task Status
fault	fault -progress 500 -file torque_fits		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_J4.and2_J4_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