STATURE ISO26262安全分析・故障率解析テンプレート
2nd エディションへの対応、主な更新内容のご案内

2019年10月29日

株式会社構造計画研究所

新バージョン(v7)の主な更新内容

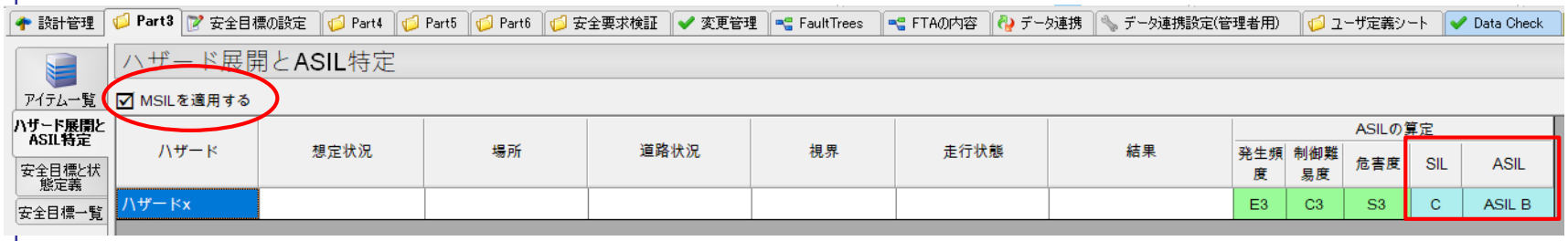
- 安全要求展開テンプレート(SG-FSR-TSR-HW/SWSR)
  - MSIL評価、およびASIL変換の追加(二輪向けHARA)
  - SCDLモデルの初期モデル生成機能の追加
    - ➡ 要求一覧表から手早くモデルを作成
  - SCDLモデル上での安全分析結果プレゼン機能の追加
    - ➡ クライアント様への安全論証を効率・効果的に

(※)SCDL:
安全コンセプト記述言語

- 故障率解析テンプレート
  - 故障率バジェットの割り当てと集計の追加
  - 故障率(メトリクス、PMHF)概算集計、抽出シートの追加
    - ➡ AnnexFに相当する概算集計と抽出。目標到達のメドや影響の大きい箇所を掌握しやすく
  - AnnexD ダイアグカバレッジ表の変更を反映(変更は主に表の構成)
  - IEC61709/SN29500 故障率算出シートの提供開始
    - ➡ IEC62380規格の廃版に対応。IEC62380 IC算出は残存。
- システムレベルにおける分析強化
  - 形式検証ツールの提供開始(本セッション後に詳しくご紹介)

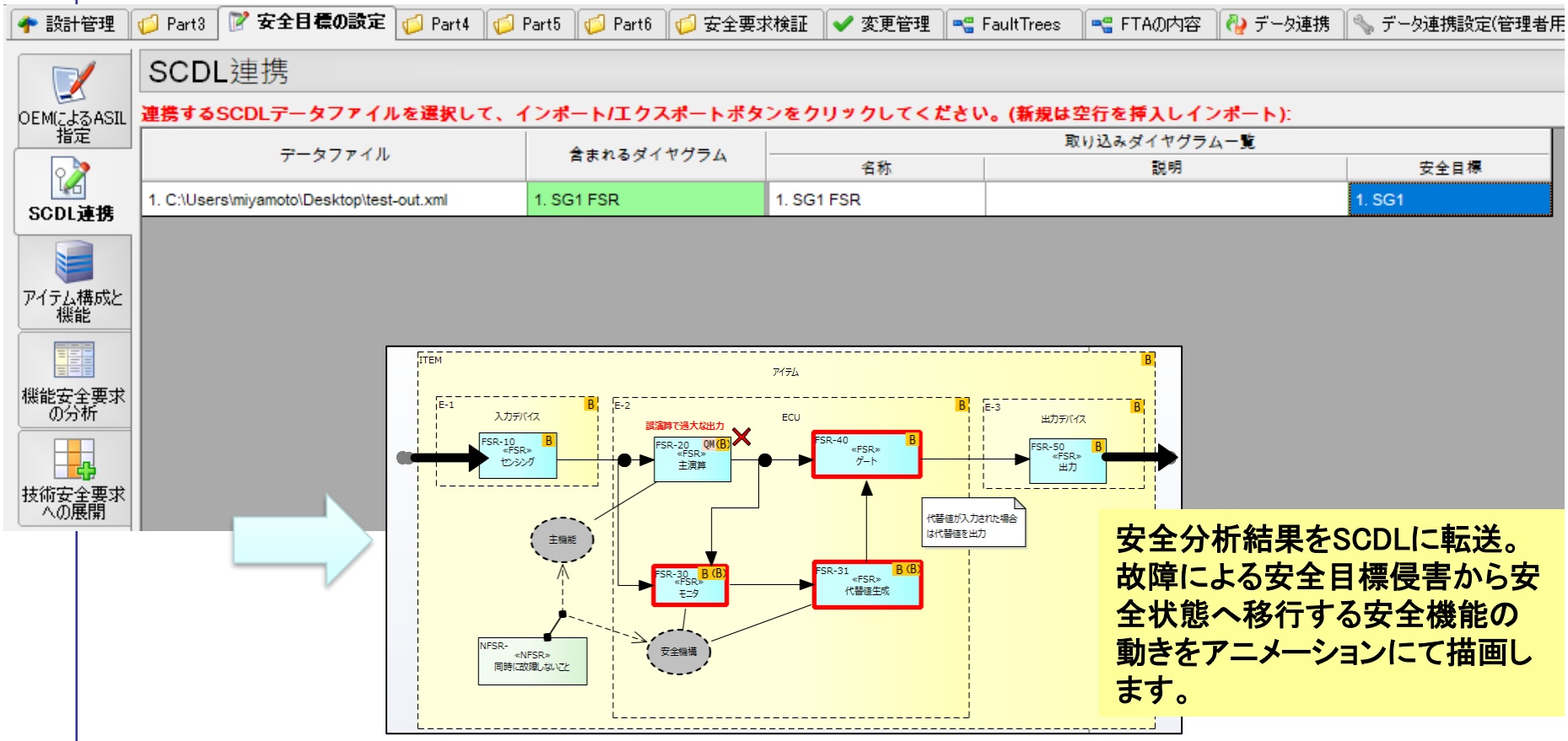
安全要求テンプレート
主な変更箇所

MSIL評価、およびASIL変換の追加(二輪向けHARA)



「MSILを適用する」をチェックした場合、SIL評価からASILへの変換が1つレベルダウンとなります。

SCDLへのエクスポート



安全分析結果をSCDLに転送。故障による安全目標侵害から安全状態へ移行する安全機能の動きをアニメーションにて描画します。

安全要求分析画面

特定の安全目標侵害に関係する要求のみ表示するフィルタを用意しました。

要求種別を設定可能としました。

処理時間を合計し、FHTI内に安全状態に移行できるかチェックを追加しました。

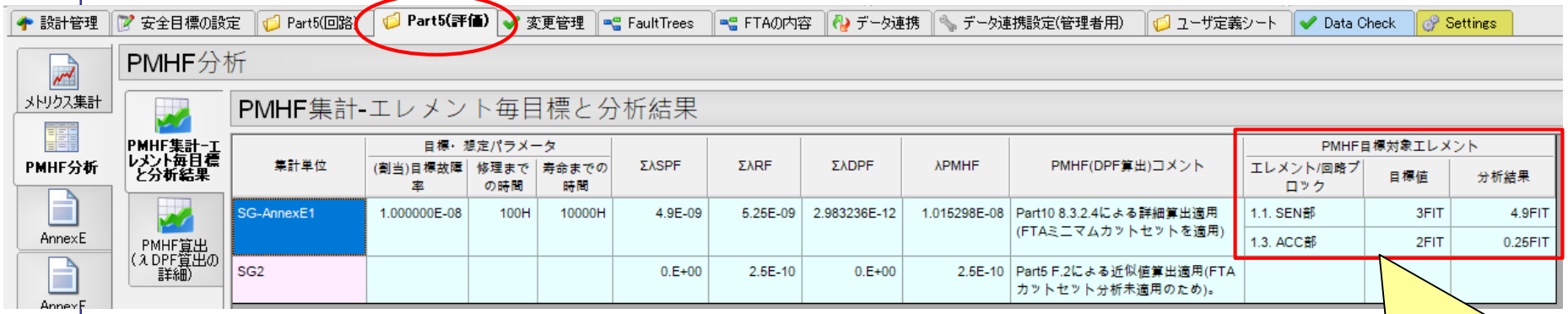
上記操作性の改善は、技術安全要求事項など他の要求事項の画面にも実施されています。

故障率解析テンプレート
主な変更箇所

故障率バジェットの割り当てと集計の追加

安全目標の設定時に、エレメントに対しPMHFの目標値を設定可能としました。

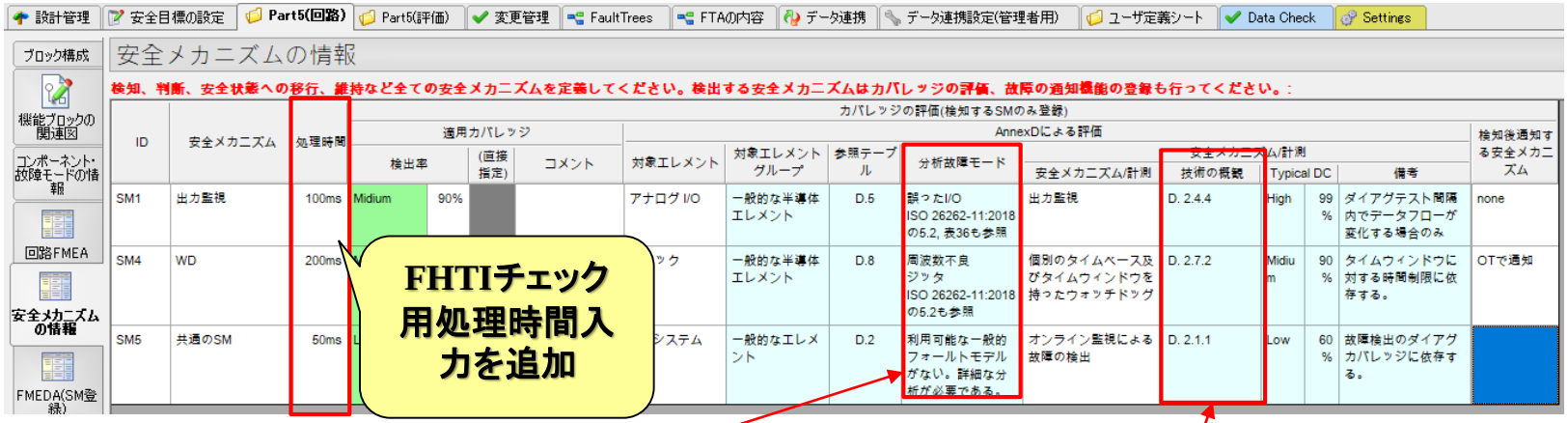
SG故障率集計			目標・想定パラメータ				PMHF目標対象エレメント	
ID	集計単位	詳細	FHTI	(割当)目標故障率	修理までの時間	寿命までの時間	エレメント/回路ブロック	目標値
SG1	SG-AnnexE1		200ms	1.000000E-08	100H	10000H	1.1. SEN部	3FIT
							1.3. ACC部	2FIT
SG2	SG2							



集計単位	目標・想定パラメータ			ΣλSPF	ΣλRF	ΣλDPF	λPMHF	PMHF(DPF算出)コメント	PMHF目標対象エレメント		
	(割当)目標故障率	修理までの時間	寿命までの時間						エレメント/回路ブロック	目標値	分析結果
SG-AnnexE1	1.000000E-08	100H	10000H	4.9E-09	5.25E-09	2.983236E-12	1.015298E-08	Part10 8.3.2.4による詳細算出適用(FTAミニマムカットセットを適用)	1.1. SEN部	3FIT	4.9FIT
									1.3. ACC部	2FIT	0.25FIT
SG2				0.E+00	2.5E-10	0.E+00	2.5E-10	Part5 F.2による近似値算出適用(FTAカットセット分析未適用のため)。			

評価時に、エレメントに対するPMHFの目標値と集計値を対比可能としました。

AnnexD ダイアグカバレッジ表の変更を反映(変更は主に表の構成)



カバレッジー覧表(ISO26262DCライブラリ_v7_0_0)にAnnexDの変更を反映しました

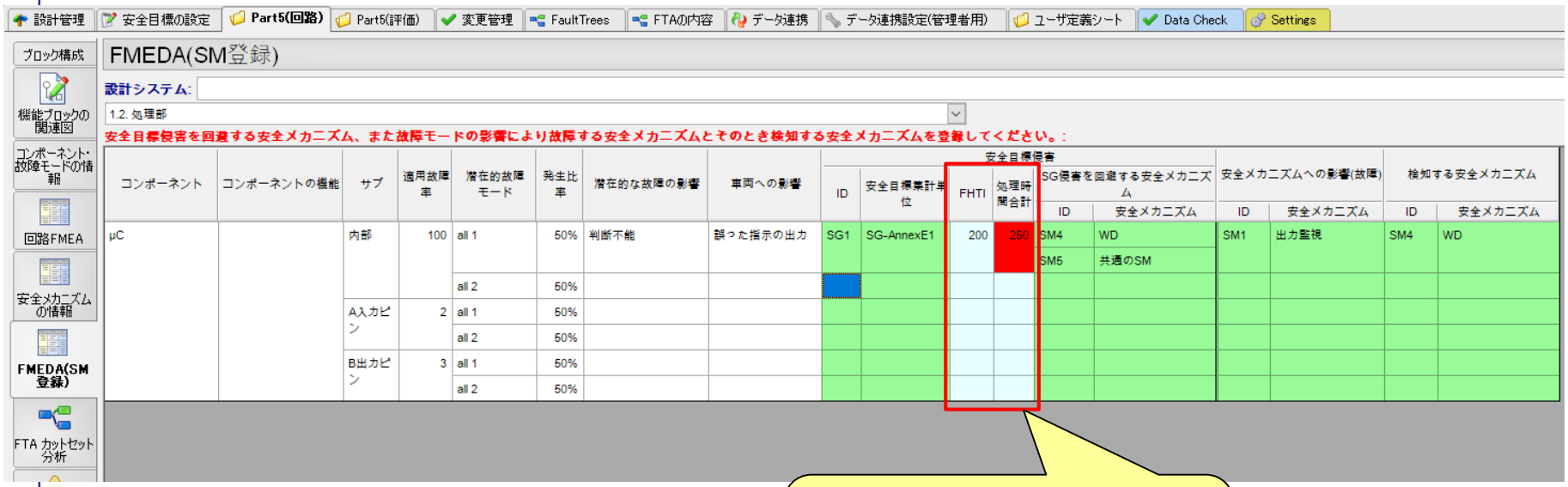
Table D.1 | Table D.2- | 設定

対象エレメント	対象エレメントグループ	参照テーブル	DCレベル	分析故障モード
E E システム	一般的なエレメント	D.2		利用可能な一般的フォールトモデルがない。詳細な分析が必要である。
リレー	電気的エレメント	D.3		通電又は切断をしない。個々の接点の溶着。
継手及びコネクターを含むハーネス	電気的エレメント	D.3		回路開放 接点抵抗 アースへの短絡 (d.c 結合) Vbatへの短絡 隣接するピン間の短絡 ピン間の抵抗性ドリフト
信号用スイッチを含むセンサー	電気的エレメント	D.9		詳細な分析が必要。 典型的な故障モードは次を含む: -レンジ外 -オフセット -レンジ内固着 -発振 組込みセンサ及びトランスデューサについては, ISO 26262-11:2018の6.5も参照。
最終エレメント(アクチュエータ、ランプ、ブザー、スクリーンなど)	電気的エレメント	D.10		利用可能な一般的フォールトモデルがない。詳細な分析が必要。
電源	一般的な半導体エレメント	D.7		ドリフト及び発振 低電圧及び過電圧 出力スパイク ISO 26262-11:2018の5.2も参照
クロック	一般的な半導体エレメント	D.8		周波数不良 ジッタ ISO 26262-11:2018の5.2も参照
不揮発性メモリ	一般的な半導体エレメント	11-32		ISO 26262-11:2018の5.1, 表29参照
揮発性メモリ	一般的な半導体エレメント	11-33		ISO 26262-11:2018の5.1, 表29参照
デジタルI/O	一般的な半導体エレメント	D.5		誤ったI/O ISO 26262-11:2018の5.1,表30も参照
アナログ I/O	一般的な半導体エレメント	D.5		誤ったI/O ISO 26262-11:2018の5.2, 表36も参照
演算処理ユニット	一般的な半導体エレメント	D.4 D.8		誤った出力 ISO 26262-11:2018の5.1, 表30も参照
データ通信(ISO 26262-6:2018の附属書D.2.4にて分析される)	特定の半導体エレメント	D.6		コミュニケーションピアの喪失メッセージ破損 許容できないメッセージ遅延メッセージ損失 意図しないメッセージの反復 誤ったメッセージのシーケンシングメッセージの挿入 メッセージなりすまし 誤ったメッセージのアドレッシング

Table D.1 | Table D.2- | 設定

参照テーブル	テーブル名	安全メカニズム/計測	技術の概観	Typical DC	備考
D.2	Systems	オンライン監視による故障の検出	D. 2.1.1	Low	故障検出のダイアグカバレッジに依存する。
		コンパレータ	D. 2.1.2	High	比較の質に依存
		多数決	D. 2.1.3	High	投票の質に依存
		動作検査法	D. 2.2.1	Midium	故障検出のダイアグカバレッジに依存する。
		デジタル信号のアナログ監視	D. 2.2.2	Low	—
		ニつの独立ユニット間でのソフトウエアの相互交換によるセルフテスト	D. 2.3.3	Midium	セルフテストの質に依存
D.3	Electrical elements	オンライン監視による故障の検出	D. 2.1.1	High	故障検出のダイアグカバレッジに依存する。
D.4	Processing units	ソフトウエアによるセルフテスト：限定されたパターン数（1チャンネル）	D. 2.3.1	Midium	セルフテストの質に依存
		ニつの独立ユニット間でのソフトウエアの相互交換によるセルフテスト	D. 2.3.3	Midium	セルフテストの質に依存
		ハードウエアにより支援されたセルフテスト（1チャンネル）	D. 2.3.2	Midium	セルフテストの質に依存
		ソフトウエアにより多様化した冗長性（1ハードウエアチャンネル）	D. 2.3.4	High	多様化の質に依存。共通モード故障はダイアグカバレッジを低減させることがある。
		ソフトウエアによる相互比較	D. 2.3.5	High	比較の質に依存
		ハードウエア冗長性(例えば、デュアルコア型ロックステップ、非対称冗長性、コード化処理）	D. 2.3.6	High	冗長性の質に依存する。共通モード故障はダイアグカバレッジを低減させることがある。
		コンフィグレーションレジスタテスト	D. 2.3.7	High	コンフィグレーションレジスタのみ
		スタックオーバーフロー/アンダーフローの検出	D. 2.3.8	Low	スタック境界テストのみ
		集積ハードウエア整合監視	D. 2.3.9	High	不正なハードウエア例外のカバレッジのみ
D.5	Analogue and digital I/O	オンライン監視による故障の検出 (デジタル I/O)	D. 2.1.1	Low	故障検出のダイアグカバレッジに依存する。
		テストパターン	D. 2.4.1	High	パターンのタイプに依存する。
		デジタルI/Oの為のコード保護	D. 2.4.2	Midium	コーディングのタイプに依存する。
		マルチチャネル並行出力	D. 2.4.3	High	—
		出力監視	D. 2.4.4	High	ダイアグテスト間隔内でデータフローが変化する場合のみ
		入力比較/多数決（1oo2, 2oo3又はより高い冗長性）	D. 2.4.5	High	ダイアグテスト間隔内でデータフローが変化する場合のみ
D.6	Communication bus	1ビットのハードウエア冗長	D. 2.5.1	Low	—

FHTI時間内安全状態への移行チェック



SMの処理時間を合計し、FHTI内に安全状態に移行できるかチェックを追加しました。

故障率(メトリクス、PMHF)概算集計、抽出シートの追加

故障率(メトリクス、PMHF)概算集計、抽出シートの追加