

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

この資料には、弊社のノウハウ、営業機密等が含まれておりますので、お取り扱いには十分ご留意願います。この資料およびその内容を、弊社に無断で使用、複写、破壊、改ざんすること、ならびに第三者へ開示すること、漏洩すること、あるいは使用させることは、固くお断り申し上げます。

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

- 故障率バジレ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)

ハザード	想定状況	場所	道路状況	視界	走行状態	結果	ASILの算定				
							発生頻度	制御難易度	危害度		
ハザードx							E3	C3	S3	C	ASIL B

「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。

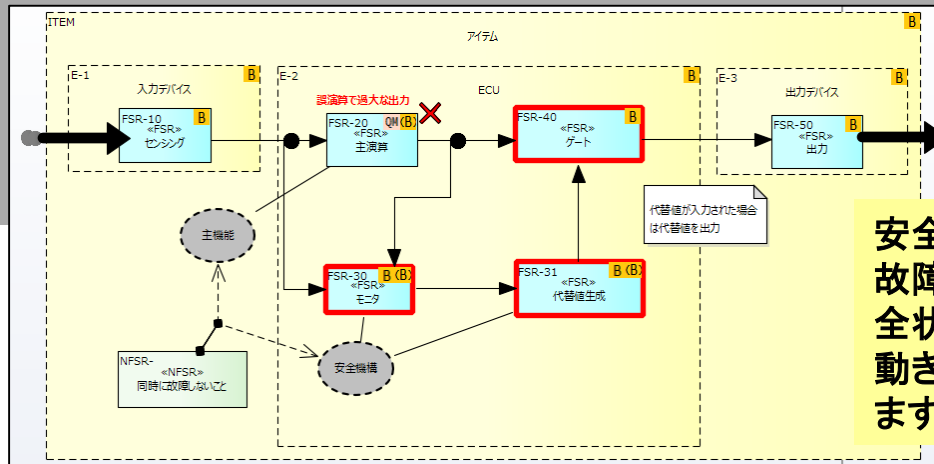
SCDLへのエクスポート

設計管理 Part3 安全目標の設定 Part4 Part5 Part6 安全要求検証 変更管理 FaultTrees FTAの内容 データ連携 データ連携設定(管理者用)

SCDL連携

連携するSCDLデータファイルを選択して、インポート/エクスポートボタンをクリックしてください。(新規は空行を挿入しインポート):

データファイル	含まれるダイアグラム	取り込みダイアグラム一覧		
		名称	説明	安全目標
1. C:\Users\miyamoto\Desktop\test-out.xml	1. SG1 FSR	1. SG1 FSR		1. SG1



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

設計管理 Part3 安全目標の設定 Part4 Part5 Part6 安全要求検証 変更管理 FaultTrees ユーザ定義シート Data Check

機能安全要求の分析

機能安全要求の詳細と安全分析

成込表示する安全目標IDを指定: (未指定時は全安全目標を表示):

名称	ID(FR)	ID	種別	要求事項	処理時間	安全分析			回避する安全要求	潜在化を防ぐ安全要求
						安全目標侵害に至る機能不全	安全目標	安全方策		
センシング	FR-10	FSR-10	IF							
主演算	FR-20	FSR-20		【FSR-10】からセンシング真正しく受信し、制御量を演算する。 制御量を【FSR-30】に出力する。		誤演算で過大な出力	SG1	モニタしてゲートする	250ms	モニタ 代替値生成 ゲート
モニタ		FSR-30		センサからの入力と比較し異常を検知	100ms					
代替値生成		FSR-40		異常を受け取り代替値を生成	100ms					
ゲート		FSR-50		代替値が入力された場合は代替値を出力	50ms					
出力	FR-30	FSR-60		制御値をアクチュエータを制御						
同時に故障しないこと		NFSR-								

特定の安全目標侵害に関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



故障率バジレ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。

設計管理 | **安全目標の設定** | Part5(回路) | Part5(評価) | 変更管理 | FaultTrees | FTAの内容 | データ連携 | データ連携設定(管理用)

OEMによるASIL指定 | 安全目標の集計設定 | 集計単位一覧

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 1.3. ACC部	3FIT 2FIT
SG2	SG2							

設計管理 | 安全目標の設定 | Part5(回路) | **Part5(評価)** | 変更管理 | FaultTrees | FTAの内容 | データ連携 | データ連携設定(管理用) | ユーザ定義シート | Data Check | Settings

メトリクス集計 | PMHF分析 | AnnexE | AnnexF

PMHF集計-エレメント毎目標と分析結果

集計単位	目標・想定パラメータ			ΣASPF	ΣARF	ΣADPF	APMHF	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 1.3. ACC部	3FIT 2FIT	4.9FIT 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)

設計管理 | 安全目標の設定 | Part5(回路) | Part5(評価) | 変更管理 | FaultTrees | FTAの内容 | データ連携 | データ連携設定(管理者用) | ユーザ定義シート | Data Check | Settings

ブロック構成 | 安全メカニズムの情報

検知、判断、安全状態への移行、維持など全ての安全メカニズムを定義してください。検出する安全メカニズムはカバレッジの評価、故障の通知機能の登録も行ってください。:

カバレッジの評価(検知するSMのみ登録)

ID	安全メカニズム	処理時間	適用カバレッジ		AnnexDによる評価							検知後通知する安全メカニズム			
			検出率	(直接指定)	コメント	対象エレメント	対象エレメントグループ	参照テーブル	分析故障モード	安全メカニズム/計測			技術の概観	Typical DC	備考
SM1	出力監視	100ms	Medium	90%		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	出力監視	D. 2.4.4	High	99%	ダイアグテスト期間内でデータフローが変化する場合のみ	none
SM4	WD	200ms				ブロック	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	個別のタイムベース及びタイムウィンドウを持ったウォッチドッグ	D. 2.7.2	Medium	90%	タイムウィンドウに対する時間制限に依存する。	OTで通知
SM5	共通のSM	50ms				システム	一般的なエレメント	D.2	利用可能な一般的なフォールトモデルがない。詳細な分析が必要である。	オンライン監視による故障の検出	D. 2.1.1	Low	60%	故障検出のダイアグカバレッジに依存する。	

FHTIチェック用処理時間入力を追加

カバレッジ一覧表(ISO26262DCライブラリ_v7_0_0)にAnnexDの変更を反映しました

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システム	一般的なエレメント	D.2		利用可能な一般的な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		過電又は過熱をしない。個々の接点の電流。
端子及びコネクタを含むハブ	電気的エレメント	D.3		接続不良 端子接続 アースへの短絡(4ヶ所) 100%への短絡 隣接するピン間の短絡 ピンの接続ドリフト
専用ソフトウェアを含むセンサー	電気的エレメント	D.9		詳細な分析が必要。 特定の故障モード解決を含む。 -ソフトウェア -ソフトウェア -ハードウェア
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		利用可能な一般的な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		ドリフト及び短絡 過電又は過熱電圧 過電圧 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も参照
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も参照
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5.2, 表36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
データ連携(ISO 26262-4:2018の附録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ンの誤ったセージ接続 許容できないメモセージ送信メサセージ喪失 重要なメモセージ送信 誤ったメモセージのシフトレジスタメサセージの挿入 メモセージなりすまし 誤ったメモセージのアドレスラッピング

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	Medium	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	—
		二つの独立ユニット間でのソフトウェアの相互交換によるセルフテスト	D. 2.3.3	Medium	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	ソフトウェ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	Medium	セルフテストの質に依存
		二つの独立ユニット間でのソフトウェアの相互交換によるセルフテスト	D. 2.3.3	Medium	セルフテストの質に依存
		ハードウェ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	Medium	セルフテストの質に依存
		ソフトウェアにより多様化した冗長性 (1ハードウェアチャンネル)	D. 2.3.4	High	多様性の質に依存。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。
		ソフトウェアによる相互比較	D. 2.3.5	High	比較の質に依存
		ハードウェア冗長性(例えば、デュアルコア型ロックスステップ、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
		重複ハードウェア監視	D. 2.3.9	High	不正なハードウェ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のためのコード保護	D. 2.4.2	Medium	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	ダイアグテスト期間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	ダイアグテスト期間内でデータフローが変化する場合のみ
D.6	Communication bus	1ビットのハードウェア冗長	D. 2.5.1	Low	—

FHTI時間内安全状態への移行チェック

設計管理 | 安全目標の設定 | Part5(回路) | Part5(評価) | 変更管理 | FaultTrees | FTAの内容 | データ連携 | データ連携設定(管理者用) | ユーザ定義シート | Data Check | Settings

ブロック構成 | FMEDA(SM登録)

設計システム: 1.2. 処理部

安全目標侵害を回避する安全メカニズム、また故障モードの影響により故障する安全メカニズムとそのとき検知する安全メカニズムを登録してください。:

コンポーネント	コンポーネントの機能	サブ	適用故障率	潜在的故障モード	発生比率	潜在的な故障の影響	車両への影響	安全目標侵害		安全メカニズムを回避する安全メカニズム		安全メカニズムへの影響(故障)		検知する安全メカニズム				
								ID	安全目標算出単位	ID	安全メカニズム	ID	安全メカニズム	ID	安全メカニズム			
μC		内部	100	all 1	50%	判断不能	誤った指示の出力	SG1	SG-AnnexE1	200	260	SM4	WD	SM1	出力監視	SM4	WD	
				all 2	50%					SM5	共通のSM							
		A入力ピン	2	all 1	50%													
				all 2	50%													
		B出力ピン	3	all 1	50%													
				all 2	50%													

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

AnnexE

集計単位: 1. SG-AnnexE1

故障率集計
故障率合計: 162
故障率合計(SPF+RF): 10.15

故障率合計(安全関連): 149
カバー率(SPFM): 93.188%

故障率合計(LF): 14.07
故障率合計(安全非関連): 13
カバー率(LFM): 89.867%

ブロック	コンポーネント	SR	サブ	FIT	潜在的故障モード	発生比率	IF-SPF			FIT (SPF+RF)	MPF			FIT(LF)
							IF-SPF	安全メカニズム	カバーレッシュ		MPF	安全メカニズム	カバーレッシュ	
SEN部	R3	SR	R3	3	open	30%	-			0	-			0
					closed	10%	-			0	-		0	
					drift 0.5	30%	-			0	-		0	
					drift 2	30%	X	none	0%	0.9	-		0	
					open	90%	X	none	0%	1.8	-		0	
					closed	10%	X	none	0%	0.2	-		0	
C13	SR	C13	2	open	20%	X	none	0%	0.4	-			0	
				closed	80%	-			0	-		0		
				open	20%	-			0	-		0		
				closed	10%	-			0	-		0		
				open	20%	X	none	0%	0.4	-		0		
				closed	80%	-			0	-		0		
C23	SR	C23	2	open	20%	-			0	-			0	
				closed	80%	X	none	0%	1.6	-		0		
処理部	μC	SR	内部	100	all 1	50%	X	SM4	90%	5	X	SM4	100%	0

AnnexEにシート名を変更

AnnexF

集計単位: 1. SG-AnnexE1

故障率集計
故障率合計: 162
故障率合計(SPF+RF): 10.15
故障率合計(SPF): 4.9

故障率合計(安全関連): 149
カバー率(SPFM): 93.188%
故障率合計(RF): 5.25

故障率合計(LF): 14.07
故障率合計(安全非関連): 13
カバー率(LFM): 89.867%
PMHF: 10.153

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)

ブロック	コンポーネント	SR	サブ	FIT	潜在的故障モード	発生比率	IF-SPF			FIT (SPF+RF)	MPF			FIT(LF)	FIT (DET)	PMHF	PMHFへの寄与率
							IF-SPF	安全メカニズム	カバーレッシュ		MPF	安全メカニズム	カバーレッシュ				
SEN部	R3	SR	R3	3	open	30%	-			0	-			0	0	0.0000	0.00%
					closed	10%	-			0	-		0	0	0.0000	0.00%	
					drift 0.5	30%	-			0	-		0	0	0.0000	0.00%	
					drift 2	30%	X	none	0%	0.9	-		0	0	0.9000	8.86%	
					open	90%	X	none	0%	1.8	-		0	0	1.8000	17.73%	
					closed	10%	X	none	0%	0.2	-		0	0	0.2000	1.97%	
R13	SR	R13	2	open	90%	X	none	0%	1.8	-			0	0	0.0000	0.00%	
				closed	10%	-			0	-		0	0	0.0000	0.00%		
R23	SR	R23	2	open	90%	-			0	-			0	0	0.0000	0.00%	
				closed	10%	-			0	-		0	0	0.0000	0.00%		
C13	SR	C13	2	open	20%	X	none	0%	0.4	-			0	0	0.4000	3.94%	
				closed	80%	-			0	-		0	0	0.0000	0.00%		
C23	SR	C23	2	open	20%	-			0	-			0	0	0.0000	0.00%	

Annex Fシートを追加。故障モード毎のPMHFとその寄与率の表示を追加。

故障率(メトリクス、PMHF)概算集計、抽出シートの追加

設計管理 | 安全目標の設定 | Part5(回路) | **Part5(評価)** | 変更管理 | FaultTrees | FTAの内容 | データ連携 | データ連携設定(管理者用) | ユーザ定義シート | Data Check | Settings

AnnexF(抽出)

集計単位: 1. SG--AnnexE1

故障率合計: 162 故障率合計(安全関連): 149 故障率合計(LF): 14.07 故障率合計(安全非関連): 13
 故障率合計(SPF+RF): 10.15 カバー率(SPFM): 93.188% 故障率合計(LFM): 89.867%
 故障率合計(SPF): 4.9 故障率合計(RF): 5.25 故障率合計(DPF): 0.002983 PMHF: 10.163

抽出条件と結果

抽出対象カバレッジ: 抽出対象寄与率: 2% 評価コメント:

PMHF(抽出対象): 9.9502 PMHF寄与率(抽出対象): 98.00%

Part5(評価)の集計結果を抽出する(抽出対象カバレッジシートを適用)

エレメント/回路ブロック	コンポーネント	サブ	適用故障率	潜在的故障モード	発生比率	IF-SPF			FIT (SPF+RF)	PMHF	PMHFへの寄与率
						IF-SPF	安全メカニズム	カバレッジ			
SEN部	R3	R3	3	drift 2	30%	X	none	0%	0.9	0.9000	8.86%
SEN部	R13	R13	2	open	90%	X	none	0%	1.8	1.8000	17.73%
SEN部	C13	C13	2	open	20%	X	none	0%	0.4	0.4000	3.94%
SEN部	C23	C23	2	closed	80%	X	none	0%	1.6	1.6000	15.76%
処理部	μC	内部	100	all 1	50%	X	SM4	90%	5	5.0001	49.25%
ACC部	T71	T71	5	short circuit	50%	X	SM 11	90%	0.25	0.2501	2.46%

特定カバレッジ以下、もしくは特定寄与率以上の故障モードを抽出可能としました。