

R-26-RC-01

平成26年度

電子部品信頼性調査研究委員会
研究成果報告書

ハードウェアの SIL (ASIL) 評価例及び
— FIDES (電子部品故障率モデル) の解説と算出例 —

平成27年3月

一般財団法人 日本電子部品信頼性センター

目次

1. まえがき	1
2. 自動車エアバッグシステムの機能安全アセスメント事例	3
2.1 安全な状態と相反潜在危険	3
2.2 用語及び記号の定義	4
2.3 システム設定	5
2.4 潜在危険の同定とフォールト（故障）モード	6
2.5 信頼性ブロック図と故障の同定	6
2.6 潜在危険の定性的分析と定量的解析	8
2.7 解析結果	12
2.8 考察	14
3. 安全機構を組み込んだ MPU、ASIC の SIL（ASIL）算出例	16
3.1 ハードウェア機能安全に関する用語	16
3.1.1 機能安全に関する用語	16
3.1.2 アイテム、部品に関する用語	16
3.1.3 故障、フォールトに関する用語	16
3.1.4 安全対策に関する用語	23
3.1.5 評価方法に関する用語	26
3.2 安全機能を組み込んだ MPU の ASIL の計算例	28
3.2.1 ハードウェアアーキテクチャーの定量的評価	28
3.2.2 ハードウェアアーキテクチャーメトリックス	28
3.2.2.1 ハードウェアエレメントの故障モードの分類	28
3.2.2.2 安全関連ハードウェアエレメントで発生するフォールトの分類	29
3.2.2.3 シングルポイントフォールトメトリックス	32
3.2.2.4 レイテントフォールトメトリックス	32
3.2.3 プロバビリスチックハードウェアメトリックス	33
3.2.4 安全 MPU の ASIL 評価例	33
3.2.4.1 設計	33
3.2.4.2 故障率評価	34
3.2.4.3 ダイアゴカバレッジ評価	34
3.2.4.4 定量的評価メトリックスと ASIL レベル決定	35
3.2.5 まとめ	36
3.3 IEC 61508-6 に従った ASIC の SIL 評価方法	37
3.3.1 はじめに	37
3.3.2 IEC で用いる SIL の指標	37
3.3.3 ハードウェアの危険側故障率の算出方法（IEC 61508-6）	40
3.3.3.1 手順	40
3.3.3.2 選定した構造のブロックダイアグラムの明確化	40
3.3.3.3 故障率の推定（故障率モデルを使用）	41
3.3.3.4 安全ファクターS の決定	43

3.3.3.5	ダイアグカバレッジ (DC) の推定	43
3.3.3.6	ベータファクターの推定	43
3.3.3.7	SFF、PFD、PFF の計算	44
3.3.3.7.1	冗長構成による危険側故障率の求め方 (IEC 61508-6)	44
3.3.3.7.2	SFF、PFD、PFF の計算例	46
3.3.3.8	SIL の評価	48
3.3.4	まとめ	48
4.	FIDES の概要及び各種電子部品の故障率算出例と IEC/TR 62380 との比較	50
4.1	はじめに	50
4.2	FIDES モデルの概要	50
4.2.1	基本式	50
4.2.2	$\lambda_{physical}$ の一般式	50
4.2.3	Π_{PM} ファクター	52
4.2.4	$\Pi_{Process}$ ファクター	53
4.2.5	ライフプロファイル	54
4.3	FIDES を用いた故障率算出例	55
4.3.1	集積回路	57
4.3.1.1	低消費電力 SRAM の例	62
4.3.1.1.1	FIDES を用いた故障率予測	62
4.3.1.1.2	IEC/TR 62380 モデルを用いた故障率予測	68
4.3.1.1.3	FIDES と IEC/TR 62380 モデルとの比較	69
4.3.1.2	ゲートアレー (0.3 μ m CMOS)–1.9Mgate, パッケージ 504pin pBGA	69
4.3.1.2.1	FIDES を用いた故障率予測	69
4.3.1.2.2	IEC/TR 62380 モデルを用いた故障率予測	74
4.3.1.2.3	FIDES と IEC/TR 62380 モデルとの比較	75
4.3.2	ダイオード、トランジスタ	75
4.3.2.1	低電力ダイオード	79
4.3.2.1.1	FIDES モデルによる故障率予測	79
4.3.2.1.2	IEC/TR 62380 モデルによる故障率予測	84
4.3.2.1.3	FIDES と IEC/TR 62380 モデルとの比較	84
4.3.2.2	低電力トランジスタ	85
4.3.2.2.1	FIDES による故障率予測	85
4.3.2.2.2	IEC/TR 62380 による故障率予測	89
4.3.2.2.3	FIDES と IEC/TR 62380 モデルとの比較	90
4.3.3	コンデンサ	90
4.3.3.1	セラミックコンデンサ	92
4.3.3.1.1	FIDES による故障率推定	93
4.3.3.1.2	IEC/TR 62380 による故障率推定	94
4.3.3.1.3	FIDES と IEC/TR 62380 モデルとの比較	95
4.3.3.2	タンタルコンデンサ	95
4.3.3.2.1	FIDES による故障率推定	96
4.3.3.2.2	IEC/TR 62380 による故障率推定	98

4.3.3.2.3	FIDES と IEC/TR 62380 モデルとの比較.....	98
4.3.3.3	アルミ電解コンデンサ（非固体）.....	98
4.3.3.3.1	FIDES による故障率推定.....	99
4.3.3.3.2	IEC/TR 62380 による故障率推定.....	100
4.3.3.3.3	FIDES と IEC/TR 62380 モデルとの比較.....	101
4.3.4	抵抗.....	101
4.3.4.1	固定、低消費電力フィルム抵抗器－高安定（rs）、一般用（rc）、”MINIMELF”.....	103
4.3.4.1.1	FIDES による故障率推定.....	103
4.3.4.1.2	IEC/TR 62380 による故障率推定.....	104
4.3.4.1.3	FIDES と IEC/TR 62380 モデルとの比較.....	104
4.3.4.2	低電力巻き線抵抗器.....	105
4.3.4.2.1	FIDES による故障率推定.....	105
4.3.4.2.2	IEC/TR 62380 による故障率推定.....	106
4.3.4.2.3	FIDES と IEC/TR 62380 モデルとの比較.....	107
4.3.5	インダクタ.....	107
4.3.5.1	低電流巻線インダクタ.....	108
4.3.5.1.1	FIDES による故障率推定.....	108
4.3.5.1.2	IEC/TR 62380 による故障率推定.....	109
4.3.5.1.3	FIDES と IEC/TR 62380 モデルとの比較.....	110
4.4	まとめ.....	110
5.	故障率と故障数の関係の考察.....	112
5.1	はじめに.....	112
5.2	EFR に基づく故障発生件数の予測.....	112
5.2.1	偶発故障発生メカニズム.....	112
5.2.2	市場の平均故障数予測.....	113
5.2.3	故障発生数の区間推定.....	114
5.3	生産計画と故障発生件数の関係.....	115
5.4	まとめ.....	117
6.	まとめ.....	119

1. まえがき

一般財団法人日本電子部品信頼性センター（RCJ）では、機能安全(Functional Safety)とくに自動車電子制御に関わる機能安全規格 ISO 26262¹⁾そして基本安全規格 IEC 61508²⁾(JIS C 0508^{3)~6)}等の理解を深め、機能安全活動を効果的に実践するため、平成 25 年度に「電子部品信頼性研究委員会」を設置し、平成 26 年度において引き続き電子部品の故障、故障率及び機能安全との関係について検討した。

さて、20 世紀の半ばを過ぎて登場した電気・電子・プログラマブル電子 (E/E/PE) 技術は、製品・システム・プロセスの利便性を著しく向上させているが、同時にそれらの技術上の複雑化の度合を深化させてきた。当初、E/E/PE 技術は、市場の製品において、安全以外の機能を実現するためにのみ用いられてきた。しかし、20 世紀の終盤には、安全性に関わる機能すなわち安全機能をも実現するために用いられるようになった。

このような状況において、E/E/PE 技術を用いた安全確保を確実にするために、E/E/PE システムの安全ライフサイクルを対象として技術・マネジメント・プロセスを規定する指針が必要とされるに至った⁷⁾。そこで、IEC 国際技術委員会は、そのような指針の策定に着手し、をおおよそ 10 年間費やして、2000 年に E/E/PE 安全関連系の機能安全規格 IEC 61508 を発行した。その約 10 年後には自動車分野の機能安全規格 ISO 26262 が発行されたことになる。

機能安全に係る基本規格 IEC 61508 が発行して 15 年ほど経過するが、最近の機能安全に関連する注目すべき動向について次があげられる。すなわち、機能安全の原則(Functional Safety Principle)による本質的安全設計方策(Inherently Safe Design Measure)の実現が活発化してきたことである⁸⁾。

従来、例えば、産業用ロボットはそれ自体の制御機能には安全機能が含まれていなかった。すなわち、産業用ロボットは、人の接近を認識して、人に危害を与えないように自らの動作を制御する安全機能を持たないため、その実用化にあたっては、人が産業用ロボットに接触する可能性のある危険領域の周囲に、人と産業用ロボットとを分離するための柵やインターロック等を設けなければならなかったのである。このような柵やインターロックによる安全方策は安全防護といわれ、製品自体すなわちここでは産業用ロボット自体の安全設計による本質的安全設計方策とは異なる方策として認識されてきた。

ところが最近、人の存在を認識して、人に危害を与えないように自らの動作を制御し、さらに人との協働作業をも可能とする産業用ロボットが実用化されるに至った。ここで、人の存在を認識して、人に危害を与えないように自らの動作を制御する機能は、機能安全規格では安全(制御)機能として規定される。このような安全(制御)機能は、機能安全原則が産業用ロボットの本質的安全設計方策として実現される。この傾向は、介護ロボットなど生活支援ロボット等では一層顕著である。このように、機械類の分野においても本質的安全設計方策が機能安全規格に適合することが要求されるようになったのである。

これまで、自動車分野においては、多様な予防安全技術が開発・実用化されている。予防安全技術は、車両の安定性を確保する技術(車両運動制御)及びドライバーの事故回避を支援する技術(運転支援)に分類できよう。

車両運動制御を行う予防安全方策として、ABS、ブレーキアシスト、トラクションコントロール(TRC)、車両安定制御システム(VSC)、走行安全カルテット(VDIM)、坂道発進制御(HAC/DAC)、タイヤ空気圧警報システム(TPMS)などの方策が実用化されている。

運転支援を行う予防安全方策として、レーダークルーズコントロール、レーンキーピングアシスト、ナビ・ブレーキアシストなど、視界支援として、フロント&サイドモニター、マルチアングル全周囲モニター、インテジエント AFS、ナイトビューなど、車両近接情報装置として車両近接情報装置など、また衝突回避システムとしてプリクラッシュ(セーフティ)システムなどが実用化されている。これらの予防安全技術は、本質的安全設計方策、安全防護の方策又はそれらの中間的な方策として位置づけられようが、いずれも機能安全の原則すなわち安全機能によりリスク低減・軽減を行うという原則によって実現されている。

今後、15～20年の間に予防安全技術は、車両の完全自動運転技術として統合されていくであろう。これにより、自動車の本質安全設計が完遂し、機能安全の原則が自動車分野において100%実現されることになる。現在は、このマイルストーンに向けた途上にあると考えられ、予防安全技術力の切磋琢磨とともに車両の完全自動運転化にも対応可能な機能安全規格の的確な改正と実践力の向上を養う期間ともいえよう。

本報告書は、以上の状況を踏まえ、平成26年度の電子部品信頼性研究委員会における検討結果をまとめたものである。

参考文献

- 1) ISO 26262: Road vehicles—Functional safety—, Part 1～9、ISO、Nov. 2011 (Geneva).
- 2) IEC 61508 Ed.2: Functional safety of electrical/electronic/programmable electronic safety-related systems、Part 1～7、IEC、April 2010 (Geneva).
- 3) JIS C 0508-1: 電気・電子・プログラマブル電子安全関連系の機能安全—第1部: 一般要求事項 (2012年10月) .
- 4) JIS C 0508-2: 電気・電子・プログラマブル電子安全関連系の機能安全—第2部: 電気・電子・プログラマブル電子安全関連系に対する要求事項 (2014年2月) .
- 5) JIS C 0508-3: 電気・電子・プログラマブル電子安全関連系の機能安全—第3部: ソフトウェア要求事項 (2014年2月) .
- 6) JIS C 0508-4: 電気・電子・プログラマブル電子安全関連系の機能安全—第4部: 用語の定義及び略語 (2012年10月) .
- 7) 佐藤吉信著、機能安全／機械安全規格の基礎とリスクアセスメント—SIL、PL、自動車用 SIL の評価法、日刊工業新聞社、2011年8月 (東京) .
- 8) 佐藤吉信著、機能安全の基礎、日本規格協会、2014年6月 (東京) .