

R-2019-RC-01

令和元年

電子部品信頼性調査研究委員会
研究成果報告書

安全の諸原則とリスクの分類とに基づく
機能安全と SOTIF の位置づけ、及び
— 米国における信頼度予測方法の動向 —
(MIL-HDBK-217F の後継)

付録： MIL-HDBK-217F Notice 2 (Feb 1995)

令和 2 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. 安全の諸原則とリスクの分類とに基づく機能安全と SOTIF の位置づけ	6
2.1 はじめに.....	6
2.2 安全の諸概念.....	6
2.3 安全機能性能の範囲とハザードの予見性に基づくハザードの分類.....	9
2.4 安全機能性能・ハザード・リスク源 (Risk Source) の予見性に基づくリスクの分類.....	10
2.5 AI を実装したシステムの多重防護層の SIL とリスクアセスメント.....	11
2.6 機能安全規格と SOTIF 規格の企図する範囲.....	12
3. アイテムの非動作状態の故障率を考慮した総合信頼性性能特性値評価.....	15
3.1 要旨.....	15
3.2 はじめに.....	15
3.3 規格による主要な総合信頼性性能の定義と特性値.....	15
3.3.1 非修理(修理がない)アイテム.....	15
3.3.2 修理(修理のある)アイテム.....	16
3.4 非動作状態の故障率を考慮した総合信頼性性能及び特性値.....	17
3.4.1 非修理アイテム.....	17
3.4.2 修理(修理のある)アイテム.....	18
3.5 まとめ.....	21
[参考文献].....	21
4. 米国における信頼度予測方法の動向 (MIL-HDBK-217F の後継)	22
4.1 はじめに.....	22
4.2 米国における MIL-HDBK-217 のその後の経緯.....	23
4.3 ANSI / VITA 51.1-2013(信頼度予測方法 MIL-HDBK-217 の補助仕様書)の内容.....	25
4.3.1 はじめに.....	25
4.3.1.1 目的.....	25
4.3.1.2 概要.....	25
4.3.1.3 用語.....	26
4.3.1.3.1 仕様書のキーワード.....	26
4.3.1.3.2 定義.....	27
4.3.1.3.3 データソースの品質.....	27
4.3.1.4 引用文書.....	28
4.3.1.5 参考文献.....	28
4.3.2 MIL-HDBK-217F Notice2 の標準的方法.....	28
4.3.2.1 部品ストレス法の標準デフォルト.....	29
4.3.2.1.1 一般.....	29
4.3.2.1.2 集積回路(IC).....	29
4.3.2.1.3 半導体.....	35
4.3.2.1.4 抵抗器.....	36

4.3.2.1.5	コンデンサ	38
4.3.2.1.6	インダクタ	41
4.3.2.1.7	リレー	42
4.3.2.1.8	スイッチ	42
4.3.2.1.9	コネクタ	43
4.3.2.1.10	相互接続アセンブリ、表面実装技術	44
4.3.2.1.11	メータ	45
4.3.2.1.12	結晶	45
4.3.2.1.13	発振器	46
4.3.2.1.14	電子式フィルター	46
4.3.2.1.15	MEMS	47
4.3.2.2	部品点数法の標準デフォルト	47
4.3.2.2.1	一般	47
4.3.2.2.2	集積回路(マイクロサーキット)	47
4.3.2.2.3	ディスクリート半導体	47
4.3.2.3	調整ガイドライン	47
4.3.2.3.1	モジュール設計	48
4.3.2.3.2	品質ファクター	48
4.3.2.3.3	フィールド経験の活用	48
4.3.2.3.4	製造業者の試験データ	49
4.3.2.3.5	他のモデルと方法の混合	49
4.3.3	附属書 A 謝辞 — 省略	50
4.3.4	附属書 B 偽造部品	50
4.3.5	附属書 C 「権威付けされた」のガイドライン	51
4.3.6	附属書 D MOSFETs	51
4.3.7	附属書 E タンタルコンデンサ	52
4.3.8	附属書 F めっきスルーホールを備えた相互接続アセンブリの故障物理予測アプローチ	55
4.3.9	附属書 G MEMS 振動子の計算	58
4.3.10	附属書 H 製造業者データからの変換方法	59
4.3.11	附属書 I 摩耗及び偶発故障	61
4.	まとめ	64
付録: MIL-HDBK-217F Notice 2 (Feb 1995)		65
1.0	適用範囲	65
1.1	目的	65
1.2	適用	65
2.0	参考文献	65
3.0	序論	65
3.1	信頼性エンジニアリング	65
3.2	信頼度予測の役割	65

3.3	信頼度予測の限界.....	66
3.4	部品ストレス解析予測法.....	67
3.4.1	適用可能性.....	67
3.4.2	部品品質.....	67
3.4.3	適用環境.....	68
3.4.4	部品故障率モデル.....	70
3.4.5	熱の観点.....	70
4.0	信頼度解析の評価.....	70
5.0	マイクロサーキット、序論.....	72
5.1	マイクロサーキット、ゲート/ロジックアレイ 及びマイクロプロセッサ.....	73
5.2	マイクロサーキット、メモリ.....	74
5.3	マイクロサーキット、VHSIC/VHSIC 類似及び VLSI CMOS.....	77
5.4	マイクロサーキット、ガリウム砒素 MMIC およびデジタルデバイス.....	78
5.5	マイクロサーキット、ハイブリッド.....	78
5.6	表面弾性波デバイス.....	79
5.7	マイクロサーキット、磁気バブルメモリ.....	79
5.8	マイクロサーキット、すべてに適用される π_T 表.....	80
5.9	マイクロサーキット、すべてに適用される C_2 表.....	81
5.10	マイクロサーキット、すべてに適用される π_E 、 π_L と π_Q 表.....	82
5.11	マイクロサーキット、 T_J の決定、(ハイブリッドを除くすべて).....	84
5.12	マイクロサーキット、 T_J の決定、(ハイブリッドに対する).....	84
5.13	マイクロサーキット、例題.....	86
6.0	ディスクリート半導体、序論.....	90
6.1	ダイオード、低周波.....	90
6.2	ダイオード、高周波(マイクロ波、RF).....	92
6.3	トランジスタ、低周波、バイポーラ.....	93
6.4	トランジスタ、低周波、シリコン FET.....	95
6.5	トランジスタ、ユニジャンクション.....	95
6.6	トランジスタ、低雑音、高周波、バイポーラ.....	96
6.7	トランジスタ、高電力、高周波、バイポーラ.....	98
6.8	トランジスタ、高周波、GaAs FET.....	99
6.9	トランジスタ、高周波、シリコン FET.....	100
6.10	サイリスタと SCR.....	101
6.11	光電子デバイス、受光素子、光結合素子、エミッタ.....	102
6.12	光電子デバイス、英・数字ディスプレイ.....	103
6.13	光電子デバイス、レーザダイオード.....	104
6.14	ディスクリート半導体、 T_J の決定法.....	105
6.15	ディスクリート半導体、例題.....	107
7.0	電子管.....	108

7.1	電子管、進行波管とマグネトロンを除くすべてのタイプ	108
7.2	電子管、進行波管	109
7.3	電子管、マグネトロン	110
8.0	レーザ、序論	111
8.1	レーザ、ヘリウムとアルゴン	112
8.2	レーザ、炭酸ガス、シールド	113
8.3	レーザ、炭酸ガス、フローイング	114
8.4	レーザ、固体、ND:YAG とルビーロッド	115
9.0	抵抗器	117
9.1	抵抗器	117
10.0	コンデンサ	119
10.1	コンデンサ	119
10.2	コンデンサ、例題	122
11.0	インダクティブデバイス	122
11.1	インダクティブデバイス、変成器	122
11.2	インダクティブデバイス、コイル	124
11.3	インダクティブデバイス、ホットスポット温度の決定	125
12.0	回転機器	126
12.1	回転機器、モータ	126
12.2	回転機器、シンクロとレゾルバ	128
12.3	回転機器、経過時間計	129
13.0	リレー	129
13.1	リレー、メカニカル	129
13.2	リレー、ソリッドステートおよび時間遅延	131
14.0	スイッチ	132
14.1	スイッチ	132
14.2	スイッチ、サーキットブレーカ	133
15.0	コネクタ	134
15.1	コネクタ、一般用	134
15.2	コネクタ、ソケット	136
16.0	接続実装(インターコネクションアセンブリ)	136
16.1	電解めっきスルーホール接続	136
16.2	表面実装接続	137
17.0	接続	140
17.1	接続	140
18.0	メータ	140
18.1	メータ、パネル	140
19.0	水晶発振子	141
19.1	水晶発振子	141
20.0	ランプ	142

20.1 ランプ	142
21.0 電子式フィルタ.....	142
21.1 電子式フィルタ、非同調形.....	142
22.0 ヒューズ	143
22.1 ヒューズ.....	143
23.0 その他の部品	144
23.1 その他の部品	144
付属書 A: 部品点数信頼度予測法.....	146
付属書 B: VHSIC/VHSIC 類似品および VLSI CMOS(詳細モデル).....	161
付属書 C: 参考文献.....	164

1. まえがき

一般財団法人の本電子部品信頼性センター（RCJ）では、2019年度において次の目的と計画に基づき事業を実施し、調査研究成果を得た。本書はその報告書である。

1.1 本事業の目的

電子制御機器の利用拡大に伴い、電子制御機器の機能安全が注目されている。機能安全関連規格の調査、及び機能安全で重要な指標のハードウェアの安全度水準（SIL: Safety Integrity Level）の概念、及びその評価で必要となる「電子部品の故障率予測」に関する調査研究を行う。これらの調査結果を基に、電子部品故障率予測に関するガイドライン作成し、システムの信頼性向上に資することを目的として、電子部品信頼性調査研究委員会を実施する。

1.2 電子部品信頼性調査研究委員会の計画

1.2.1 事業内容

(1) 機能安全規格（IEC 61508、ISO 26262）の特にハードウェアの機能安全についての理解

IEC 61508 及び ISO 26262 で規定しているハードウェアの SIL 及び ASIL（Automotive SIL）の概念、各種機器構成と SIL（ASIL）との関係、その求め方などの調査研究を行う。特に、2019年度は、ISO 26262 第2版の内容についての検討を行う。

(2) SIL（ASIL）算出の基本となる構成電子部品の故障率の求め方についての調査

公表されている各種故障率モデルの調査を継続する。モデル間の比較やモデルの妥当性の検討などを行う。また、故障率モデルを使用しない故障率予測方法についての調査も行う。

(3) 外部専門家を招いての講演と討論

車載、ロボット、鉄道分野などの専門家を招いての講演と討論を行う。

1.2.2 実施方法

- ① 学識経験者、企業の信頼性技術者、設計技術者等で構成する電子部品信頼性調査研究委員会を設置し、年8回程度の委員会の審議を経て事業を遂行する。
- ② 審議場所は原則として、当センターの会議室で行う。時間は原則 13:30～17:00 とする。

1.3 電子部品信頼性調査研究委員会の実施結果（委員会での審議概要）

- ISO 26262 第2版と自動運転の安全性に関連して2019年3月開催の IRPS（信頼性物理国際会議）で、Riccardo Mariani 氏（Intel、イタリア）より発表された“Reliability Year Review（Functional Safety、Reliability、Availability）”の内容が紹介された。主な内容は、以下の通り。
 - ISO 26262 第2版での変更点の概要
 - ISO 26262 - 11（半導体）の概要

- 自動運転
 - Uber 社の自動運転の死亡事故
 - SOTIF (Safety of intended functionality) (本件の詳細は本書第 2 部「安全の諸原則とリスクの分類とに基づく機能安全と SOTIF の位置づけ」参照)
 - RSS (Responsibility – sensitive safety)
 - Cybersecurity and safety
- 機能安全関連の発表論文数の国別比較
- ISO 26262 第 2 版での変更点の一つとして、Part 8 で、ハードウェアコンポーネントの分類の明確化があるが、その内容が紹介された。次が認識できた。
 - 第 2 版では、クラス 1 (抵抗、コンデンサ等のエレメントレベル)、クラス 2 (安全機構が組み込まれていないコンポーネントレベル (温度センサ、ADC 等)、クラス 3 (安全機構が組み込まれているコンポーネントレベル) に分類され、クラス 3 には、ISO 26262 が要求される。
- 世界的な自動車用半導体規格開発の体制として最近設立された自動車用半導体規格開発体制 (TRACE) が紹介された。
 - 最近、ドイツが中心になり、自動車用半導体の規格開発のためのコンソーシウム (TRACE と称している) が設立された。
 - SEMI (Semiconductor Equipment and Materials International)、IPC (Institute for Interconnecting and Packaging Electronic Circuits)、IEEE EPS (electronics packaging society) を巻き込んでコンソーシウムを設立している。
 - 今後の活動に注意が必要と思われる。
- 2019 年 6 月の IEC/TC 56 国際会議で議論となった、FIDES の IEC 規格への改訂素案が紹介された。
- 米国で開発された故障率モデルの経緯と現状が説明された (本件の詳細は、本書第 4 部に「米国における信頼度予測方法の動向」として報告されている)。
 - MIL-HDBK-217 (電子機器の信頼度予測方法) は、1961 年に発表され、世界的に有名であり、良く用いられてきた。但し、最終版は、F 版 notice2 (1995 年) であり、これ以降改定が中止された。
 - F 版 notice2 (1995 年) 以降、217 の G 版の改定版検討のためのプロジェクトチームが 2008 年に結成されたと報告されたが、この活動は中断され、G 版は発行されていない。但し、その検討過程で、217 の後継版となる 2 つの規格が発行されている。
 - VITA51.1 は、217 の補足版と称され、基本構造は変更なく、 π ファクターの見直しが主である。これは、米軍でも民生品の使用が必須となり、民生品対応が必要となったためと思われる。
 - VITA51.2 は、故障物理に基づく予測方法で、ボード、パッケージ、コンポーネントレベルで、故障モード毎に使用環境を考慮し、故障率を評価し、設計に反映させる。この手法は、JEDEC (JEP148B)、SAEJ1879 と同じ系列と見なせる。
- 2019 年 10 月の IEC/TC 56 国際会議で議論となった、動作状態の故障率と非動作状態での故障

率とを考慮した故障間平均時間など総合信頼性性能特性値評価の問題点が議論された（本書第3部「アイテムの非動作状態の故障率を考慮した総合信頼性性能特性値評価」参照）。

- 部品故障率に関し、動作状態と非動作状態で異なる故障率がある場合の総合信頼性性能特性値の求め方について議論があった。
 - 動作状態（動作時間 T_a 、故障率 λ_a ）、非動作状態（非動作時間 T_b 、故障率 λ_b ）、歴時間（ T_a+T_b ）とした場合、一般に、全体の故障率 λ は、 $(T_a \lambda_a + T_b \lambda_b) / (T_a + T_b)$ として求めている。しかし、これは近似式であり、より正確には、状態遷移図（（正常、非動作）、（正常、動作）、（故障、非動作）、（故障、動作））を考慮する必要がある。
- 安全状態は電気/電子/プログラマブル電子安全関連系が生成する状態であり機能安全の基礎であるが次の問題が提示された。
 - IEC61508、ISO26262 にも安全状態の定義がない（IEC TR 63039 に記述）。
 - 安全状態には、不変（Invariable）安全状態、可変（Variable）安全状態があると考えている（IEC TR 63039 に記述）。
 - 今年度発行の JISZ 8115:2019 ディペンダビリティ(総合信頼性)用語 - 安全と信頼性関係用語の中で、安全と信頼性関係用語を中心に議論した。JIS C 0508-4:2012(機能安全規格の用語)、ISO 26262-1:2011 との対比も行った。
 - 以前より議論のあったフォールトと故障の関係について JISZ 8115、192-03-01 の“故障”注記 1 に、「アイテムの故障とは、そのアイテムのフォールトを発生させる事象である。」とあり、ISO 26262-1 の“フォールト”では、「エレメント (1.32) 又はアイテム (1.69) の故障を引き起こす可能性のある、異常な状態」とある。すなわち、JIS では、故障→フォールトであり、ISO では、フォールト→故障の関係であり、混乱する。
 - ISO 26262 のエレメント 1.32 の定義は、「コンポーネント (1.15)、ハードウェア、ソフトウェア、ハードウェア部品 (1.55) 及びソフトウェアユニット (1.125) を含むシステム (1.129) 又はシステムの一部」とあり、アイテム (1.69) の定義は、「ISO 26262 が適用される、車両レベルの機能を実装するシステム (1.129) 又はシステム群」とあり、最上位の概念を示している。コンポーネントレベルのフォールト（故障原因により発生した）が上位システムの故障原因となると解釈すればよいのではとの指摘があった。
 - その他、なじみのある初期故障や偶発故障が除かれている。但し、バスタブ曲線 (192J-13-129) との関連で、初期故障期間 (192-02-28)、偶発故障期間 (192J-02-106) は掲載されている。
 - 委員長の信頼性学会（2019年11月11日）で発表予定内容の紹介「アイテムの動作状態と非動作状態とで故障率が異なる場合でのアベイラビリティについて」説明があった。前回の委員会で議論のあった、動作状態と非動作状態で異なる故障率がある場合の MTTF、MTBF、アベイラビリティ等の求め方について検討している（本書第3部参照）。
 -
 - 国立情報学研究所石川冬樹教授の講演「AIの品質、品質のためのAI」をいただいた。概要は次のようであった。
 - AIソフトウェア（が入ったシステム）の品質の一般的議論

- AI をソフトウェア（例えば、自動運転の経路判断器）の検査等に用いる場合の留意点
- AI の品質の指標：正解率で、90%とかの数値であり、100%は無い。
- SOTIF（Safety of intended functionality）には、センサーと AI の組み合わせ（センサーで画像を取り込み、AI で認識する）が含まれている。
- ISO 26262 には、まだ AI に関する記述はない。IEC 61508 では、SIL 1 で、AI（フォールト診断）の使用を許容している。

● SN 29500-2:2010 部品の故障率 第 2 部 集積回路の期待故障率の内容と IEC TR 63162:2018（CD 段階）の数値比較が示された。次が議論された。

- 基礎故障率の値は、IEC TR 63162:2018 の方が SN 29500-2:2010 より大きい値を採用している。その理由は不明。
- ストレスプロファイルファクター π_w として、非動作状態も考慮した故障率の求め方を提示している。この式の妥当性について疑問が出された。

$$\lambda_w = \lambda \times \pi_w \quad (4.8)$$

$$\pi_w = W + R \times \frac{\lambda_0}{\lambda} \times (1 - W) \quad , \quad R = 0.08$$

W: 部品にストレスが印加される動作時間比率 $0 \leq W \leq 1$

R: 定数。ストレスが印加されていない部品の故障する可能性を考慮している。

$\lambda_0 = \lambda_{ref} \times \pi_T(\theta_0)$: 待機状態温度での故障率。待機状態の温度 (θ_0) は、ストレスの無いフェーズでの接合部の温度である。

λ は、実際の動作温度での故障率

- 上式を極端な条件に適用すると以下ようになる。
 - (1) 全時間に渡り動作状態の場合 (W=1) λ (これは妥当である)
 - (2) 全時間に渡り非動作状態の場合 (W=0) $\lambda_w = \lambda \times \pi_w = \lambda \times R \times \frac{\lambda_0}{\lambda} = R \times \lambda_0$
- 全時間に渡り非動作状態の場合 (W=0) の故障率は、 λ_0 になるはずで、R 定数の意味合いが不明である。

● IEC 61508 改定版の審議状況の紹介があった。診断機能 (Diagnostic function) と対応機能 (Fault reaction function) とに係る SIL の定義に関する提案である。これは、委員長の提案であり、内容は次となる（詳細については 2020 年度調査研究委員会ですらに検討する）。

- 全体システムには、不変安全状態と可変安全状態とがある。従来の規格では、不変安全状態の冗長構成を扱っている。
- 冗長系には Load-shared redundancy（荷重分割冗長）及び Active (Passive) redundancy（アクティブ冗長）が存在する。
- 可変安全状態を 2 チャネルで冗長系を構成する場合、アクティブ冗長を用いる必要がる。
- アクティブ冗長構成では、フォールトが発生した場合、サブチャネルに切り替えるかどうかの診断と切り替え動作が必要である。この診断機能と切り替え動作に SIL を割り当てる必要がある。その他、多重防護系でも SIL を考慮する必要がある（詳細については 2020 年度調査研究報告書

にまとめる)。

- 米国における故障率モデル—MIL - HDBK - 217 の後継版の VITA51.1 の概要が紹介された。次が議論された。
 - MIL-HDBK-217F のモデル式はそのまま、 π_Q ファクター (品質ファクター) の見直しと、集積回路の大規模化に合わせた複雑度ファクター C_1 の見直し・追加が主な変更である。
 - この規格の発行の背景に、1995 年の改定終了後も、MIL-HDBK-217F Notice 2 を引き続き使用して、故障率の予測を行っている現状があるため、信頼性エンジニアは、MIL-HDBK-217F Notice 2 方法論を変更して、故障率の予測を実際に合わせるように変更する必要があった。VITA51.1 は、MIL-HDBK-217F Notice 2 を使用して現実的な MTBF 値を得るための入力ファクター (特に品質ファクター) を見直した規格である。

本研究委員会は、機能安全において最も基本的な技術要素である電子部品の信頼性について調査研究を実施して、我が国のこの方面の技術の基盤を支え、さらに技術水準を底上げするための機能を担っている。従って、今後も地道ではあるが活動を継続し、さらに発展させていくことに大いに意義があろう。