

R-2023-RC-01

令和5年度

電子部品信頼性調査研究委員会
研究成果報告書

- ・SOTIFを考慮した機能安全評価のための確率モデルと定式化
- ・FTA技法の理論的背景とその適用範囲について
- ・電子機器の信頼性向上に使用される高加速試験方法(HALT)

附録A: IEC 62506 ED2:2023 製品の加速試験方法

令和6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
1.1 本事業の目的	1
1.2 2023 年度電子部品信頼性調査研究委員会の計画	1
1.2.1 事業内容	1
1.2.2 実施方法	1
1.3 電子部品信頼性調査研究委員会の実施結果	1
2. SOTIF を考慮した機能安全評価のための確率モデルと定式化	6
2.1 研究の背景と目的	6
2.2 機能安全基本規格 IEC 61508 における SOTIF 関連の要求事項	7
2.3 リスク低減戦略における機能安全及び SOTIF の位置づけ	8
2.4 SOTIF 特性値のモデル化	12
2.4.1 前期プロセス安全時間と後期プロセス安全時間	12
2.4.2 その他の用語の定義	13
2.4.3 各事象間の時系列的関係と動作完遂率	15
2.4.4 兆候状態と非兆候状態	16
2.5 SOTIF における確率変数の定式化	17
2.5.1 平均検出時間, τ_0	17
2.5.2 不可逆遷移確率, P_F	18
2.5.3 作動要求状態完遂率, μ^*	19
2.5.4 危険事象率 (HER), η	20
2.6 数値解析事例	21
2.6.1 高兆候率システム	21
2.6.2 低兆候率システム	21
2.6.3 SIL 換算による SOTIF の評価	22
2.7 考察	22
2.8 結論	22
3. FTA 技法の理論的背景とその適用範囲について	24
3.1 はじめに	24
3.2 構造関数, コヒーレント FT 及びノンコヒーレント FT の定義	24
3.2.1 2 状態構造関数	24
3.2.2 コヒーレント FT の定義	26
3.2.3 ノンコヒーレント FT の定義	27
3.3 最小カット集合及び最小パス集合の定義	27
3.3.1 カットベクトル/カット集合及びパスベクトル/パス集合の定義	27
3.3.2 最小カット集合の定義	28
3.3.3 最小パス集合の定義	28
3.4 FT の分類と最小カット集合/最小パス集合の適用範囲	31
3.5 まとめ	33

4. 電子機器の信頼性向上に使用される高加速試験方法 (HALT)	34
4.1 はじめに	34
4.2 HALTとHASSの概要	37
4.3 加速試験法の基本	38
4.4 高加速限界試験 (HALT)	40
4.4.1 HALTの主な原則	41
4.4.2 ストレスの種類と適用	44
4.5 高度に加速されたストレススクリーニングまたは監査 (HASS または HASA)	46
4.6 HALT および HASS の利点と欠点	46
4.6.1 HALTとHASSの利点	46
4.6.2 HALTとHASSの欠点	47
4.7 HALTとHASSの事例	47
4.7.1 デンマークにあるSPM(信頼性・環境試験協会)の報告	47
4.7.1.1 試験試料	47
4.7.1.2 HALTの目的	48
4.7.1.3 HALTの試験手順と結果	48
4.7.1.4 他の品質向上手法との比較と結論	52
4.7.2 米国QualMark社が実施した33社の47製品に関するHALT試験の報告	52
4.7.2.1 HALT試験プロジェクトに参加した企業と装置	52
4.7.2.2 HALTプロセス	53
4.7.2.2.1 温度ステップストレス	54
4.7.2.2.2 急激な温度変化	55
4.7.2.2.3 振動ステップストレス	55
4.7.2.2.4 複合環境	55
4.7.2.3 HALT試験条件	55
4.7.2.4 HALT結果	56
4.7.2.5 HASS	60
4.7.2.5.1 HASS開発	60
4.7.2.5.2 スクリーニングの検証(プルーフオブスクリーン)	61
4.7.2.5.3 生産段階でのHASS	61
4.8 まとめ	61
5. まとめ	64

附録A IEC 62506 ED2:2023 製品の加速試験方法

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、2023 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）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、2023 年度の電子部品信頼性調査研究委員会を実施する。

1.2 2023 年度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 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、2023 年度は、現在進行中の IEC 61508 の改定状況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（2023 年 6 月、7 月、8 月、10 月、12 月、2024 年 1 月、2 月、3 月）の委員会の審議を経て事業を遂行する。
- ② リモート開催と RCJ の会議室の併用で、審議を行う。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

次のようなテーマについて調査、検討、議論した。

- ・ 2022 年度成果報告書 R-23-03 について解説・討議を実施
 - 3 章について 2022 年度の委員会で説明していない追記項目について内容説明と討議
 - 3 章のタイトルに記載の事象と状態との違いについて解説と討議
 - 状態：英語で State 一時間幅のあるアイテムの特性

- 事象：英語でEvent—時間幅がなく行われる、ある状態から他の状態への変化
- Fail（不良、失敗など）を事象と状態に分けると次のようになる。
 - 状態：Failした状態のこと（Faultで表す）
 - 事象：Fail状態に変わった瞬間のこと（Failureで表す）
- 3.2.3節に余事象の定義を追加した。
- ハザード分析の自動処理ソフトを作る件の進捗を確認した。
 - 試作ソフトによる解析結果を確認し、その結果で修正点を明確にする。
 - 修正をソフトに組み込んでいく。
 - これを繰り返しながら、ソフトをブラッシュアップしていく。
- 2022年度成果報告書 R-23-04 について解説・討議を実施
 - FIDES の 2022 年版の概要を説明した。
 - 故障率モデルは 2010 年版と同じであるが、加速係数の見直しがされている。
 - 故障率の算出結果は 2022 年版の方が約 20%低くなることを SRAM への適用例で説明
 - FIDES で計算した故障率は、機能安全を判断するための値としては有効であるが、実際の故障率より 1/10~1/20 倍と低く算出される場合がある。
- 2022 年度成果報告書 R-23-02 の説明・討議を実施
 - 2 章は、これまでの未発表の研究成果を中心に纏めたもの
 - 機能安全を理解するための用語の解説に関し、次が議論された。
 - 同族ハザードについての提案に対して、『同等の危険事象をもたらす』でいいのか？『同等の危害をもたらす危険事象』もしくは『同等の危害事象』の方が適しているのではないのか？などの議論があった。→危険事象はある危害をもたらす可能性のある事象と定義しおり、危害事象は危害の開始（事象）であるので、危険事象と危害事象の違いは、可能性が 100%になった時点を危害事象、可能性が 100%でない時点が危険事象である。同族ハザードは、定量的なレベルは問題にせず、危害の可能性についてのみ言及するので危険事象と危害事象はどちらでもよいことになる。
 - 理解を進めるための危険事象と危害事象の具体例として、「怪我をする、又は死亡する可能性のある飛行機の墜落が起こります」は危険事象、「その墜落で怪我しました、死亡しました」は危害事象となる。
- 2022 年度成果報告書 R-23-05 の説明・討議を実施
 - 内燃機関と EV 用半導体のミッションプロファイルの比較の解説
 - Semiconductor Digest 誌に TI、Bosh の連名で投稿のあった“ZVEI Robustness Validation Process for Assessing Semiconductor IC Mission Profiles”の内容を紹介している。
 - EV 用途の IC のミッションプロファイルは、目標寿命に対して PO（Power On）の Duty は 100%となる（131,000PDH）。これは、充電時間に充電制御用の IC が駆動していることを考慮する必要がある。
 - これを考慮すると、AEC Q100 グレード 0 の高温連続動作試験でも寿命試験としては時間が不足してしまうことが問題点である。これを克服するための手段として、各故障メカニズムに対して、それぞれに特化した加速性を考慮し判定時間を決定することも考慮する必要がある。
 - 抵抗などの受動素子はシステム当たり約 1k 個搭載するものもあったが、これまでの POH や寿

命、故障率の要求に対しては十分な余裕があった。しかしながら、今回の提案値（131,000PDH）となると、その余裕を食い潰してしまう可能性があり、受動素子に対しても高ストレスに対する寿命、故障率などの検討が必要となるという議論があった。

- 2022 年度成果報告書 R-23-02 の説明・討議を実施（前回の続き）
 - ベータファクタ以降の用語の定義について解説
 - 2.2 節（1oo3 システムの信頼性特性値）、2.3 節（1oo2 システムの MTTFT/修復率/リスク特性値）まで解説。
 - λ と μ が等価な場合と異なる場合、最初の故障までの遷移モデルと定常状態の遷移モデルそれぞれにおける際について解説
 - 図 3 において P3→P1 及び P3→P2 への修復がないのは何故か？→図 1 において最初の故障までの遷移モデルのため C/D 間で μ が存在しないことによる。
- システムの初期状態から最終状態に至る最短経路群の導出方法の解説・討議を実施
 - 最短経路導出のためのプログラム作成の進捗状況報告
 - 72 状態の状態遷移経路の導出まで可能となっていることを確認
 - 最短経路選択をプログラムで実施することが何故重要なのか？との疑問があり。→すべての経路を手書きで準備し、その中から力づくで最短経路を抽出することも可能であるが、系の増加に伴って状態が増えるため困難さは増大し、正しく選択できる確率が減少するため、これを排除するためには、プログラムによる抽出が重要となるとの議論があった。
- IEC 61508 の改訂状況について説明・討議を実施
- 住宅環境における協調システムの機能安全規格の動向の紹介・討議
- 危険事象の生起が故障の生起順序／ハザードに依存するシステムの FTA の解説・討議
 - 相反ハザードの事例による説明
 - 事例 1：ガス爆発を頂上事象とする FT の展開の紹介
 - 事例 2：恒温槽のオーバーヒート（又はヒータ常時 ON）を頂上事象とする FT の展開の紹介
- 最短経路探索ツール『BTSP（Back Track & Shortest Paths）』の進捗と今後の課題について解説・討議を実施
 - 次の機能の検討している。
 - 機能 1：最短経路の検索
 - 機能 2：Directed Acyclic Graph の作成
 - 機能 3：BTSP 経路群のサブセットの作成
 - 機能 4：Pre-Critical 状態の一覧の表示
 - 今後の課題は次の 2 項目
 - システム状態数が増加することで最短経路の増加した場合の経路の重み付け手法の検討
 - BTSP 手法が効果を発揮するハザードを特定するための分析事例の追加
- トヨタ（デンソー）の燃料ポンプのリコールについて解説・討議を実施
 - 『トヨタ（デンソー）の燃料ポンプのリコールー2020 年以降、現在も続いている---』をもとに、公知の事実から、原因、再発及び解決までに長期間を要した要因について分析した結果を報告
 - 次の技術的・人的な要因が絡み合う要因を同定した。
 - 物理的な現象：燃料ポンプの動作不具合。燃料圧送する樹脂部品の特性欠陥

- ・ 物理的な原因：PPS 樹脂部品の成型温度が低く低密度となり、燃料中では膨潤。気体中で変形
- ・ 技術的な要因：製造条件・検査条件の検討不十分。使用環境の設定ミス
- ・ 人的な要因：メーカ・ユーザ間での仕様確認などの情報共有不足
 - ✓ 製造のばらつきの認識不足
 - ✓ 良品解析による製品のウイークポイントの検知能力不足
- ・ 再発要因：不具合の発生メカニズムまでの追及が不足した状態で、量産を再開したことか？
 - リコール対象は 1,245 万台。リコール費用 2,900 億円（日経クロステック情報）
- ・ 2022 年度成果報告書 R-23-02 の説明・討議を実施（前回の続き）
 - 2.4 節の MooN システム（安全関連系）の定常状態での信頼性/リスク特性値について説明・討議
 - 2.5 節の PT で検出・事後保全関連系の信頼性/リスク特性値について説明・討議
- ・ データ解析トライアルについて報告・討議の実施
 - 高温恒湿試験機の不具合（冷凍機のコンプレッサの過熱異常）についてデータの解析について紹介
 - データ解析ツールとしてプログラミング言語 Python を用いた数理解析ソフト（ツール）を開発
 - モニターしている各種パラメータの相関係数の確認、回帰予測と変数、クラスタリング、PCA による異常検知の各項目の解析結果で、故障前後で変動がみられるパラメータが存在することを紹介いただき、解析ツールが有用であることが示された。
- ・ HALT 及び HASS の現状の解説を実施
 - HALT（Highly Accelerated Limit Teat）：高加速限界テストについて解説
 - ✓ 定義されたストレス環境において製品で発生する可能性が最も高い故障モードを特定することを目的として実施するテストのこと
 - HASS（Highly Accelerated Stress Screening）：高加速ストレススクリーニングについて解説
 - ✓ 製造プロセスまたは工程管理エラーに起因する製品の潜在的な欠陥を特定することを目的としたスクリーニングのこと
 - 2013 年に IEC 62506 に信頼性関係で初めて HALT という用語が出現した。
 - HALT および HASS は、目的達成のために設計上下限以上のストレスを印加するテストである。
 - HALT 手法を有効に利用できる一例として、外部リードのダメージが実使用に耐え得るかの振動試験による評価結果などの紹介があった。
- ・ 2022 年度成果報告書 R-23-02 の説明説明・討議を実施（前回の続き）
 - 2.5 節 PT で検出・事後保全される安全関連系の信頼性/リスク特性値について説明と討議を実施。
- ・ HALT 及び HASS の留意点について解説・討議を実施
 - HALT 及び HASS について知っておくべき 10 項目の解説
 - HALT 及び HASS の効果の例の紹介を実施
 - ✓ 故障モードが重要なため、その故障モードに対し故障検出率の高いプログラムの準備が必要。つまり、HALT や HASS 試験を実施するためには、すべての回路に対して故障検出率の高いテストプログラムが準備されていることが前提で

ある。

- ✓ スクリーニングとして HASS を使用する場合は、単に高加速で試験を実施すれば良いというのではなく、製品寿命を食い潰すことのないように最適なストレス時間を設定する必要がある。
- フォールトツリーに関する用語の定義について解説・討議を実施
 - IEC 61025 ed.3: Fault tree analysis (CDV) の状況について紹介
 - CDV に対し日本は反対投票を行った（反対は CZ、DK、JP の 3 か国）が賛成多数で '23 年 12 月に承認された。
 - 日本の修正提案（次の項目）が CDV に反映されるか否かは RVC レポート待ちの状況である。
 - 各 FT の関連性と最小カットセットアプローチが可能な FT の図の修正を提案した。
 - ✓ コヒーレント FT の定義の追加
 - ✓ コヒーレント FT の定義の追加
- HALT のケーススタディと 車載用電子機器の信頼性試験設計の例の紹介・討議を実施
- 多状態を持つ要素を含むシステムの構造関数の解説・討議を実施

以上

本年度は、昨年度に引き続き長引くコロナ感染状況によって、ほとんどの委員会をリモートで実施した。このため、外部専門家を招いての講演と討論などを思う通りには実施できなかったものの、外部の IEC 61508 関係の有識者のオブザーバー参加を得て講演をいただいた。

以上の報告のように、本調査研究委員会は、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努力を重ねている。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。