

R-2024-RC-01

令和6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  
—第2報:フォールト診断により作動する安全保護機能について—
- ・電子機器の予知保全と車載用半導体への適用

附録A: IEC 63162/TR/Ed1:電気部品—信頼性—基準条件における  
故障率(2024年回付)

令和7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 2024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 本報と前報との関係 .....	8
2.2.1 機能安全と SOTIF との基本的関係 .....	8
2.2.2 安全制御機能と安全保護機能 .....	9
2.3 第1報で得られた主な結果 .....	10
2.3.1 用語の定義 .....	10
2.3.2 SOTIF 特性値のモデル化 .....	12
2.3.3 SOTIF に係る特性値の定式化 .....	12
2.3.3.1 平均検出時間(Average detection time), $\tau_0$ .....	13
2.3.3.2 非完遂確率(Non-accomplishment probability), $P_F$ .....	14
2.3.3.3 完遂率(Accomplishment rate), $\square^*$ .....	15
2.4 安全保護機能に係る SOTIF の評価 .....	15
2.4.1 安全制御機能と安全保護機能 .....	15
2.4.2 SOTI に起因する危険事象生起モデル .....	17
2.4.3 危険事象生起モデルに基づく HER, $\square$ [1/時間], の定式化 .....	18
2.5 考察 .....	19
2.5.1 規格間の概念及び用語の整合性 .....	19
2.5.1.1 反応時間 (FAT), 全システム停止時間, 機能完遂時間及びプロセス安全時間 (PST) .....	19
2.5.1.2 作動要求とプロセス安全時間 (PST), $T_P$ .....	20
2.5.2 作動要求, 作動要求状態, 完了 (完遂) 及び危険事象論理について .....	20
2.5.3 規格の要求事項と本報の定式化との関係 .....	22
2.6 結論 .....	23
3. 電子機器の予知保全と車載用半導体への適用 .....	26
3.1 はじめに .....	26
3.2 電子機器の予知保全 .....	26
3.2.1 保守技術の進化 .....	26
3.2.1.1 予知保全 .....	27
3.2.1.2 予知保全ツールと材料 <sup>1)</sup> .....	28
3.2.1.2.1 サイバーフィジカルシステム (Cyber-Physical System) .....	28
3.2.1.2.2 産業用モノのインターネット (Industrial Internet of Things) .....	28
3.2.1.2.3 ビッグデータ (Big Data) .....	29

3.2.1.2.4	デジタル ツイン (Digital Twin)	29
3.2.1.2.5	拡張現実 (Augmented Reality)	29
3.2.1.2.6	人工知能 (Artificial Intelligence)	29
3.2.1.2.7	機械学習とディープラーニング (Machine Learning and Deep Learning)	30
3.2.2	予知保全の課題 <sup>1)</sup>	30
3.2.2.1	財務および組織上の制限	31
3.2.2.2	データソースの制限	31
3.2.2.3	機械修理活動の制限	31
3.2.2.4	産業用予知保全モデルの展開における制限	32
3.2.3	予知保全ワークフロー	32
3.2.4	予知保全モデル	34
3.2.4.1	状態基準保全	34
3.2.4.2	予測と健全性管理	35
3.2.4.3	残存耐用年数	37
3.2.5	議論と推奨事項	38
3.3	予知保全の車載用半導体への適用	38
3.3.1	はじめに	38
3.3.2	ISO/TR 9839:2023 の概要 <sup>4)</sup>	39
3.3.2.1	扱っているフォールト	39
3.3.2.2	劣化フォールトのライフサイクル	39
3.3.2.3	劣化フォールトの基礎故障率の定量化	43
3.3.2.3.1	業界標準とモデル	43
3.3.2.3.2	フィールドデータ	43
3.3.2.3.3	専門家の判断	44
3.4	半導体のシリコンライフサイクル管理 (SLM)	44
3.4.1	はじめに	44
3.4.2	SLM の概念 <sup>8)</sup>	44
3.4.3	SoC (System on Chip) への適用例	46
3.4.3.1	SLM プラットフォームの概要	46
3.4.3.2	モニターの種類	47
3.4.3.3	モニターの例	47
3.4.3.4	分析例	48
3.5	まとめ	49
4.	まとめ	51

附録A IEC 63162/TR/Ed1:電気部品－信頼性－基準条件における故障率 (2024 年回付)

## 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、2024 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、2024 年度の電子部品信頼性調査研究委員会を実施する。

### 1.2 2024 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、2024 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 (2024 年 6 月、7 月、8 月、10 月、12 月、2025 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。

- IEC 61025(ed.3) (Fault tree analysis (FTA)) に向けた CDV が 2023 年に配布された。そこでは、新たにノンコヒーレント FTA が追加され、適用範囲が拡大された。但し、CDV に記載されたノンコヒーレント FTA の内容に疑義があり、日本は反対投票をした。本章はその反対投票の基本となる、FTA の理論的背景をまとめた。即ち、先ずノンコヒーレント FT、コヒーレント FT、最小カット/最

小パス集合などの理論的背景をあらためて整理し、それらを要約し定義として示した。次に、それらの定義に基づき、FT をコヒーレント FT とノンコヒーレント FT とに分類し、さらに、最小カット/最小パス集合の適用範囲を体系的に示した。これらの具体的内容が説明された。

- BTSP 進捗と今後の課題について議論した。
  - 最短経路探索ツール (BTSP) のによるハザード分析手法の進捗と今後の課題について報告された。
  - 追加した部分は、遷移作用の重み付け (距離で重み付け) である。例えば起こりにくさ (起こりやすさ) を故障率の逆数に基づき表す重み付け方法などが考えられる。
  - 追加した部分は、遷移作用の重み付け (距離で重み付け) である。例えば起こりにくさ (起こりやすさ) を故障率の逆数に基づき表す重み付け方法などが考えられる。
  - Li イオン試験装置の安全装置を例に、S-A プロセスチャートで、本来の目的の初期状態から危害事象への遷移経路分析の検討以外に、逆ルートの危害状態から安全状態への遷移経路分析を試みた。
  - 最短経路のみの条件を付けて、検索すると、迂回経路を通した経路を見落とす場合があり、工夫が必要であることが分かった。
- 車載用電子機器の信頼性試験設計の例の紹介と討議
  - IEC 62506 ED2 : 2023 「製品の加速試験方法」 附属書 B に記載の車載用電子機器の信頼性試験設計の例について検討した。
  - 対象の試験は、一定の故障率を仮定した信頼性適合性試験 (reliability compliance test) である。
  - 着目点は、1) 同一製品に、複数の加速試験 (高温試験, 温度サイクル試験, 湿度試験, 振動試験) を実施する際の、ストレス条件の設定方法, 2) 試験結果の取扱い方法 (加速係数の取扱い (掛け算か足し算かの問題である。))
  - 高温試験を、温度サイクル試験の高温部で代用し、温度サイクル試験のみで、高温試験と温度サイクル試験を実施する試験を採用。そのため、温度サイクル試験で、高温部の時間が長くなり、温度サイクル試験規格から逸脱しているのではとの疑問がある。
  - 4種類の加速試験を実施しているが、全体の加速係数は、4種類の試験の加速係数の掛け合わせではなく、類似の故障モードを加速する場合に掛け合わせ、それ以外の故障モードを加速する場合は、足し算になると説明されている。
- 自動車用安全規格の動向について検討
  - Riccardo Mariani (NVIDIA, イタリア) の 2022 年 IRPS で発表した内容の紹介。
  - 2015 年から 2022 年まで自動車 (AV) に対応する標準の数が爆発的に増加し、さらに多くの標準が活発に開発されている。業界の最先端に対応するには、どの標準に従う必要があるかの見極めが重要であろう。
  - IEC 61508, ISO 26262, その他関連する主要な規格の紹介があった。その中に記載のサイバーセキュリティ関連規格で、SAE J3061 は、ISO/SAE 21434:2021 (Road vehicles - Cybersecurity engineering) に替わっているとの指摘があった。
- 2023 年度報告書第 2 章の説明と討議
  - 報告書第 2 章 (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) の内容の説明がなされた。
  - 研究の背景と目的に関して説明があった。

- 本文では、不全残存リスク（当該システムに生ずる故障等に起因して、正常に設計上の機能を履行できない機能不全によって危険事象の抑制に失敗する残存リスク）と、SOTIF 残存リスク（安全機能の制御特性の範囲を逸脱した事象に起因する残存リスクを扱う SOTIF が対象とするリスク）について、共通リスクメトリックである危険事象率の比較を可能とするための方法論について提案されている。
- 対象とするハザード： 機能安全のスコープ外で、コントロールできないハザード（既知のハザードと未知のハザードを含む）を対象とし検討している。
- 「SOTIF 特性値のモデル化」の説明がなされた。
- 自動車 1（速度  $V1$ ）と自動車 2（速度  $V2$ ）の間隔  $L$  ( $V1 > V2 > 0$ ) の状況の例を基に、衝突ハザードが生成される際の E/E システムによるハザードの制御と危険事象の分析方法について説明された。
- 時系列では、最初に兆候が発生し、兆候状態になる → E/E 系が捕捉、検出し、安全機能が作動状態になる → 安全機能が完遂し、安全状態になる。あるいは、プロセス安全限界を超えて、危険事象が発生する。これらの状況をそれぞれ定式化する。
- 「2.5 SOTIF における確率変数の定式化, 2.6 数値解析例, 2.7 考察, 2.8 結論」の章の説明がなされた。
- 「2.5 SOTIF における確率変数の定式化, 2.6 数値解析例, 2.7 考察, 2.8 結論」の章の説明がなされた。
- 本報では、プロセス安全時間、機能遂行時間などを用いて SOTIF の特性値とモデル化を提案し、数値解析例を提示した。さらに、SOTIF 評価を相当 SIL と比較し、検討した。
- 自動車の予知保全 ISO TR 9839 の概要について紹介と討議
  - 2023 年に発行された ISO TR 9839 (Application of predictive maintenance to hardware with ISO 26262-5) の予知保全に関する標準の概要が説明された。
  - 適用範囲は、「安全関連の E/E ハードウェア要素の degrading fault (劣化フォールト) を検出するための予知方法の使用に適用することを目的にする」とある。
  - 使用している用語に違和感があり、特に degrading fault (劣化フォールト) の用語と定義に不一致があると思われる。定義では、通常の劣化 (normal degradation) と異なり、時間の経過と共に、エラーまたは故障を引き起こす異常な状態とある。例として示されている図では、通常の劣化より、短時間に劣化が現れる例をしめしている。これらの説明からすると、異常な劣化 (abnormal degradation) が適切な用語ではとの指摘があった。
  - この degrading fault (劣化フォールト) の対処方法について、ISO 26262-5 の概念が全て適用でき、degrading fault (劣化フォールト) に対する安全メカニズムを構築することにより、このフォールトに対処できるとの考えである。
  - この件に関して委員からさらにコメントがあったが、それらは省略する。
- シリコンライフサイクル管理 (SLM) について
  - Synopsys が提案している、シリコンライフサイクル管理 (Silicon Lifecycle Management(SLM)) の概要が説明された。
  - チップにセンサーとモニターを埋込み、設計からフィールドでの使用のあらゆる段階で、データを収集し、分析エンジンに取り込み、分析し、各段階で最適化をはかるというコンセプトである。このコンセプトの中には、予知保全も含まれている。

- 安全規格に基づくハザードの定義とその解釈について
  - 信頼性学会 秋のシンポジウムで発表予定の上記題名の資料について、説明された。
  - 各種安全規格が定義している「Hazard」の名称と内容について紹介された。ISO/IEC ガイド 51 が定義している「危険の潜在的な源 (potential source of harm)」が妥当である。
  - 機械分野におけるハザードの解釈例として、A.機械の稼働空間と B.人間の作業空間の概念図を用いて説明された。さらに、「挟まれ/巻込まれによる負傷」の FT への展開例も示された。
  - 固有（本質）安全について：ハザードを、全体ハザード (Full hazard) , 部分ハザード (partial hazard) , 組合せハザード (Combined hazard) に分類される。その分類につき、「溶剤乾燥中のガス爆発による負傷の FT」を例に説明された。
  - 安全には、全体固有安全、部分固有安全、受動的安全設計方策があり、その例を化学プラントと自動車の例について説明された。また、これらの方策と固有（本質）安全との関係について説明された。
- 機械類の安全関連制御系における故障診断及びフォールト反応機能について検討
  - ISO 13849-1 (機械の安全性 ~制御システムの安全関連部~ Part 1: 設計の一般原則) に記載されているカテゴリ 2 アーキテクチャを例について、IEC 61508 に基づく安全度水準の評価の観点から定式化し、危険事象率による SIL, PL の割当てを試みた。
  - ISO 13849-1 では、パフォーマンスレベル (PL) とし、単位時間当たりの危険側故障発生確率 (Probability of Dangerous Failure, PFHD) のみを規定し、これは、IEC 61508 高頻度要求に相当し、低頻度作動要求モードを規格の対象としていない。
  - 「故障診断」機能要素と「フォールト反応」機能要素から構成される安全機能の総合信頼性特性値の算出を、IEC 61508 に基づく安全度水準の評価の観点から、危険事象率、*PFH*, *PFDavg* の導出に関して定式化した。
  - これにより、危険事象率による PL の定量的な割り当てが可能となった。
- IEC TC56 が扱っている部品故障率モデルの現状について検討
  - TC56 が開発している部品故障率モデル (信頼性データブック) が説明された。
  - IEC/TR 62380 は、TR の期限切れで廃止された。現在、IEC63162/TR/Ed.1 (基準条件における故障率) と IEC 63142 (A global methodology for reliability data prediction of electronic components (源規格は FIDES) ) が開発されている。一時、IEC 63142 の開発中止が発表されたが、2024 年 12 月の TC56 委員会で、開発再開が決定された。
  - IEC63162/TR/Ed.1 に関し、最初の CD は、2018 年 7 月に回付された。部品の種類毎の基礎故障率を提示するのが目的であるが、多くの部品で、空白のデータがあり、問題視された。その後、4 年ほど、提案が無かったが、2022 年 10 月に、DTR(Draft Technical Report)として回付された。さらに、2024 年 2 月に、新たに、改訂版が DTR として回付された。最新版 DTR では、多くの部品で、空白のデータが埋まっているが、まだ空白のデータも残されており、完全なデータとはなっていない。
- 保全の種類と予知保全の挑戦について討議
  - 機器の保全技術の年代による進化についてのレビュー論文の紹介。内容は、保全技術の進化と特に現在注目されている予知保全の課題と解決策についてのレビューである。
  - 保全技術は、年代とともに、事後保全、予防保全、状態基準保全 (状態監視保全) , 予知保全、処方保全 (prescriptive maintenance) と進化している。

- 予知保全では、①異常データとノイズの区別、②異常データから残存寿命の推定方法と妥当性が問題である。近年の IIoT（インダストリアル IoT）の普及により、大量のデータ収集が可能となり、収集されたデータは、統計的分析と機械学習（ML）技術と組み合わせて、残存寿命の予測に活かしている。
- 一部のメーカ（イグス社（ドイツ本社））では、自社製品について、残存寿命の計算ツールを提供している。
- IEC 61508 ed.3（CDV）の内容について紹介と討議
  - IEC 61508 ed.3（CDV（-3 と-6 を除き））が近々配布予定である。Ed.2 より大きく変更された点が2点あり、今回は、その1点について説明された。
  - IEC 61508-1 の7.4 節（ハザードとリスク分析）の7.4.1 項で、目的は、EUC 及び EUC 制御システム（全ての動作モード）に関連するハザード、ハザード事象及びハザードな状況を決定することであるとし、対象を「EUC 及び EUC 制御システム」と明記した。
  - EUC 制御システムと E/E/PE 安全関連システムは、独立したものとして割り当てるのが原則である。これができない場合、7.6.2.8 項に、割り当ては、EUC 制御システム、E/E/PE 安全関連システムに関連する共通原因故障を考慮しなければならないとあり、注記 3 で、パート 6 B.4 を参照が追記された。

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。