R-2021-RC-01

令和 3 年度

電子部品信頼性調査研究委員会
研究成果報告書

機能安全における危険事象の起こり易さの尺度と算出方法、自動車の日米におけるリコール状況 ― 及び自動車用半導体のゼロディフェクトへ向けて ― の取り組み

附録 A：AEC−Q004：2020　自動車用ゼロディフェクトフレームワーク

令和４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

一般財団法人の本電子部品信頼性センター（RCJ）では、2021 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。これに鑑みて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、ASIL: Automotive 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、電子部品信頼性調査研究委員会を実施する。

1.2 2021 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、2021 年度は、ISO 26262 改訂第 2 版、及び、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（2021 年 6 月、7 月、8 月、10 月、12 月、2022 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 審議場所は原則として、RCJ 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

- FIDESの成り立ち、今後の計画、宇宙への適用（資料R-21-03）について検討した。
  - AIRBUSのS. Bourbouseの論文を基に、FIDESの成り立ち、今後の計画、宇宙への適用について紹介された。

- FIDES は、フランスの産業界のコンソーシアム（DGA（フランス国防総省）と防衛・航空宇宙産業界）によって、第 1 版が 2004 年に発表、第 2 版が 2009 年に発表された。仏をはじめ欧州の防衛・航空宇宙産業界での使用が推奨されている。
- FIDES は、IEC TC56（デペンダビリティ）に提案され、IEC 63142（A global methodology for reliability data prediction of electronic components）として、2022 年発行を目指している。
- FIDES の故障率モデルは、物理的ストレス（温度や温度サイクル）の他、Π_{PM}（部品の信頼性保証レベル）、Πprocess（信頼性プロセスのコントロールレベル：171 項目の質問表への回答に基づく評点づけ）が考慮されている。

• サイバーセキュリティ（資料R-21-04）に基づいて議論した。
  ➢ 6月16日に日本規格協会主催で開催されたサイバーセキュリティに関する規格開発状況に関するセミナー資料第一部を基に、サイバーセキュリティの規格状況を検討した。
  - 主な規格には、国連の UNR155（Cyber Security）と ISO/SAE 21434（Cybersecurity Engineering）であり、各国で導入が進められている。
  - ISO/SAE 21434 の詳細な内容を説明しているセミナー資料第二部については、引き続き検討を継続することにした。

• サイバーセキュリティ（資料R-21-05）に基づいて議論した。
  ➢ 6月16日に日本規格協会主催で開催されたサイバーセキュリティに関する規格開発状況に関するセミナー資料第二部その他を基に、サイバーセキュリティの規格状況を検討した。
  - セミナー資料第二部の構成は、第 2 部：組織のサイバーセキュリティ（プロセス認証部）、第 3 部：製品開発における要件（プロダクト認証部）、第 4 部：附属書の概要となっている。
  - これらの第 2 部、3 部、4 部についてセミナー受講した藤井委員より解説いただいた。
  - 脅威シナリオに対して、サイバーセキュリティの保証レベルの 4 段階（CAL（Cybersecurity assurance level）、CAL1～CAL4）が規定されている。

• IEC 61508 vs ISO 26262（資料R-21-07）について議論した。
  ➢ 委員長より、IEC 61508 vs ISO 26262の用語と目指すところの違いについて説明があり、これに基づき議論した。
  - まず、IEC 61508 改訂に向けて、国際改訂委員会（MT 61508 委員会）で検討している内容の紹介があった。
  - 機能安全の定義、適用範囲の違いには次があげられる。
    ✓ IEC 61508では、対象はEUC（Equipment under control）及びEUC制御システムであり、電気/電子システムのみでなく、アクチュータ等の機械系を含めた全体のシステムの機能安全を扱っている。
    ✓ 一方、ISO 26262では、電気/電子システムのみであり、安全系を構成する機械系を含めていない。
    ✓ 対象とするハザードの相違について議論した。
      - IEC 61508 では、電気/電子システムの正常な機能発動の失敗が原因となるハザードを対象とする。
      - ISO 26262 では、電気/電子システムの（正常な機能発動の失敗も含む）異常な挙動が原因となるハザードを対象とする。
    ✓ 対象とするリスクの相違について議論した。

- IEC 61508 では､単一の被制御機器及び EUC 制御系から生じるリスクのみを対象とする。
- ISO 26262 では、複数の被制御機器及び EUC 制御系から生じるリスクも対象とする。

✓ 自動車用エアーバッグシステムのシステム構成、ハザード例について説明があり、これに基づき議論した。

- S-A プロセスチャートから導出される FT (Fault Tree)による事象生起順序を考慮したハザード分析（資料R-21-08、09）の紹介があり、これに基づき議論した。
  - 本技法の開発者の柴垣委員より、本技法の長年の研究成果について発表して頂いた。
  - 本技法は、ハザードの同定及び分析を系統的に実施可能とするもので、特に、事象の生起順序に着目した方法論を提供する。

    ・技法を適用した実システム事例として、溶剤乾燥器の相反ハザード（ガス濃度に爆発限界があり、下限値より低い場合と上限値より大きい場合は爆発が起こらない）等を例に、S-A プロセスチャートの作成方法、FT への展開方法が説明された。

    ・S-A プロセスチャートの利点は、複数の状態がある複雑システムの分析に有利であり、FT へ展開して FTA (Fault Tree Analysis)を実施する場合、ハザード分析の抜けを防止できることが分かった。
- 塩野委員より、米国と日本における自動車のリコール台数と内容の年次推移について解説があった。
  - 米国、日本とも、2014年から急激にリコール台数が増えた。その後一旦リコール台数が減少したが、最近は増加傾向にある。
  - 2014年の急激なリコール台数の増加の主な原因は、GMのイグニッションスイッチ不具合、タカタ製エアバックの異常破裂であった。
  - 最近のリコール原因は、運転支援技術、外装照明、電動化に関するものが多く、電子部品とその制御に使用するソフウエア不具合も多くなっている。
- IEC 63142-CD概要（後半部分）（プロセスファクターの求め方）（資料R-21-11）について検討した。
  - IEC 63142-CD（故障率予測）の後半部分は、プロセスファクターの求め方について記述されており、塩野委員より概要が説明された。
  - アセンブリのライフサイクルにわたる品質と技術管理（仕様書、設計、製造、サポート等の7つフェーズにつき）について、チェックシートを用いて評点付けしている。
  - チェックシートは、156項目準備されており、同じチェックシートを各フェーズで重複して使用する場合もある。
  - 内容は、ISO 9001に類似しており、また、製造工程は、有鉛はんだを使用した実装工程に特化している。これは、ISO 9001等の品質システム評価と類似しており、この規格で取り上げる必要が無いとの意見が、CDに対するコメントとして出されている。
- 危険事象の起こりやすさの尺度について（資料R-21-12）検討した。
  - 委員長より、リスク概念と定義及び安全への適用について、数式による定量的評価方法について説明があった。
  - 具体的な適用事例として、ロボットの各種安全動作状態を基に、A-Cモデルから状態遷移図への変換、故障率、修復率の説明と、故障と修理が繰り返し起こる過程の数理モデルが説明された。

- これにより、低頻度動作要求モードから高頻度作動要求（連続動作）モードまで全領域にわたり、機能失敗確率を求めることができる。

- 217Plus（PRISM）とIEC 63142（FIDES）の比較検討した（資料R-21-13）。
  - 塩野委員より、217Plus（PRISM）とIEC 63142（FIDES）の比較（システムマネジメントモデルを中心）が説明された。
  - 217Plusのシステムモデルは、部品単体レベルでなく、電子機器レベルの故障率推定に適用（製造業者のマネジメント側面を評価し、装置の故障率を推定する）する。
  - 一方、FIDESのシステムモデルは、部品レベルの故障率推定に適用する（主に部品のマネジメントレベルを評価し、部品故障率に反映させる。）
  - 217Plusを中心に、モデル式、Πファクター（プロセスグレードの関数）の求め方、プロセスグレードの査定方法（チェックシートによる査定）の概要が説明された。
- 危険事象の起こりやすさの尺度について（資料R-21-14）検討した。
  - 前回に引き続き、委員長よりリスク概念と定義及び安全への適用について、数式による定量的評価方法について説明された。
  - 危険事象の起こりやすさの尺度は、初期状態から危険事象が起こるまでの平均時間T_Mの逆数$[1/T_M]$を危険事象率として定義され、単位は[1/hr]である。
  - ロボットの危険事象の各種想定シナリオを示し、その事象に対するA-Cモデル図を明示し、危険事象と制御作用の例が説明あり、質疑応答、議論した。
- 部品故障率モデルの概要と故障率予測データ比較（資料R-21-16）を実施した。
  - 塩野委員より、IEC/TR 62380、217Plus（PRISM）、FIDES（IEC 63142）の部品レベルの故障率モデルと数品種についての計算結果の比較が説明され、議論した。
  - いずれのモデルも、主要な故障メカニズムとして、温度加速性と温度サイクル加速性を取り上げている。
  - 温度加速性で、IEC/TR 62380とFIDES（IEC 63142）は、動作状態のみの加速性を考慮し、非動作状態では、故障率を0に設定している。
  - 一方、217Plus（PRISM）は、非動作状態でも温度加速性があり、有限の故障率を設定している。
  - 各種部品の予測故障率の比較では、チップの故障率よりも、パッケージやはんだ接続の故障率が高く設定されている。特に、IEC/TR 62380の集積回路のパッケージ故障率が大きく見積もられている。
- 危険事象の起こりやすさの尺度について議論した（資料R-21-14（前回委員会配布資料））。
  - 前回に引き続き、委員長よりリスク概念と定義及び安全への適用について、数式による定量的評価方法について説明された。
  - 修復が無い場合の故障率、故障強度、およびMTTF、修復がある場合の修復率、修復強度、およびMTTR、故障・修理の繰り返しがある場合の故障・修復頻度、MTBFの数理モデルについて議論した。
- 非故障事象に着目したハザード分析のためのFTA技法について検討した（資料R-21-17）。
  - 柴垣委員よりFTAの2例を基に、有効なFTA技法について説明された。
    ・事例のマルチタスク-ガス漏れ警報システムでは、入力に、失敗（プロセスシャットダウンの失敗、電力遮断の失敗）だけでなく、システム要素の正常な要求事項の履行（この例では、警報）

等も含めるようにする必要がある。

・事例 2 の電気式暖房器の例では、失敗の「加熱しない（暖房しない)」と「過熱する（オーバヒート)」とが互いに排反事象であるにもかかわらず、OR ゲートで機能不全として結合しているが、問題である。それぞれを切り離し、別々に機能不全として扱い、FTA を実施すべきである。

- 米国における2020年リコールの状況について検討した（資料R-21-18）。
  - 塩野委員より、米国における2020年リコールの状況が説明された。
    ・100万台以上のリコール件数が5件あり、その中の4件が日本車である。
    ・大半のリコール原因が品質管理の問題であり、日本の品質管理の弱体化が懸念される。
    ・テスラEV車搭載の「メディアコントロールユニット（MCU）の故障によるバックカメラの機能喪失事故」が注目される。
    ・MCUの構成は、8GB eMMC NANDフラッシュメモリ装置を内蔵したNVIDIA Tegra 3プロセッサである。
    ・eMMC NANDフラッシュデバイスは、プログラム/消去（P/E）サイクルの回数に基づき、有限の寿命がある。この有限寿命を見落とした（軽視した）設計ミスと思われる。
- 自動車用ゼロディフェクトフレームワークについて検討した。
  - AEC-Q004の資料で、2020年2月26日に発行されたものである。
  - ゼロディフェクトを達成するための枠組みをまとめた資料である。
  - ゼロディフェクトに着目した品質管理システム（IATF 16949）の詳細手順とみなせる。
- 自動車リコール報告書（ドラフト）第3章及び第4章に基づき、リコール状況について検討した（附録A 自動車ゼロディフェクトフレームワークも含む）。
- ノンコヒーレントFTA技法について検討した。
  - 柴垣委員から、ノンコヒーレントFTAについて解説があった。
    ・コヒーレントシステムとは、システム要素がアップからダウンに移行したとき、システムがダウンからアップに移行することがないシステムである。
    ・コヒーレントでないシステムをノンコヒーレントシステムという。これは、例えば、システムに互いに排他的な事象が存在する場合、システム要素が 2 状態でなく 3 状態以上の多状態を持つ場合、事象の生起順序がシステムの状態を支配する場合などにみられる。
    ・ノンコヒーレントシステムの FTA では、最小カット集合のアプローチが適用できないので、インプリカント（プライムインプリカント）の方法論を持ちなければならない。

本年度は、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 ISO 26262 関係のオブザーバーの参加を得て意見をいただいた。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。