R-2020-RC-01

令和 2 年

電子部品信頼性調査研究委員会
研究成果報告書

人の操作を含む多層電気・電子・プログラマブル電子安全関連系群の機能安全評価モデルと介護ロボットへの適用、及び故障物理手法による信頼度予測方法の動向

付録 1：ZVEI（第 2 版：June 2013）自動車用電気/電子モジュールのロバストネス検証ハンドブック
付録 2：ANSI/VITA 51.2 － 2016　故障物理に基づく信頼度予測
付録 3：SAE J3168：2019「航空−自動車業界が推奨する電気、電子、電気機械コンポーネントの信頼性物理分析の実践」

令和３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、2020 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 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、2020 年度は、 ISO 26262 改訂版、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。

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）

- 自動車使用環境（ミッションプロファイル）の各規格の比較を行った。
  - 各種規格（AEC Q100、Q101、IEC TC47 の提案（日本からの提案）、217Plus、IEC TR 62380、ZVEI）が提案している自動車用ミッションプロファイルの内容と規格間の差異を検討した。主な検討内容は、以下の通り。

- AEC Q100、Q101 は、エンジン部だけの定義、標準試験条件がミッションプロファイルの動作条件とどのように対応しているかに注目している。動作温度（エンジン on、エンジン off（アイドリング））、温度サイクル、湿度を考慮している。高温動作試験の加速は、温度加速のみ考慮している。
- IEC TC47 の提案（IEC 63287-2 Ed.1 CD（47/2636/NP）：ミッションプロファイルのガイドライン）は、エンジン部とキャビン部を考慮している。但し、温度プロファイルだけを考慮している。また、温度加速の他、電圧加速も考慮している。
- 217plus は、温度、温度サイクル、湿度の他、非動作状態を考慮し、非動作状態でも有限の故障率を割り当てている。
- EC TR 62380 は、温度、温度サイクルを考慮し、非動作状態では故障率=0 としている。
- ZVEI（SAE J1879 と同等）は、15 年寿命、エンジン on 時間：12,000h、エンジン off 時間：3,000h、非稼働時間：116,400h を提案し、AEC Q100、Q101 のモデルの元になっている（Q100、Q101 が、参考資料として引用している）。

- 217plus（米国）が非動作状態でも故障率は有限としているのに対し、IEC TR 62380（欧州系）では、故障率=0、と設定している。この差について議論があった。
  - ➢ 欧州系では、非動作状態では、動作状態に比べ、故障率が小さいので、無視できると考えているのではとの指摘があった。
  - ➢ また、OEM により、非動作状態（休止状態）の取扱が異なるようだとの指摘もあった。

- 安全の諸原則とリスクの分類とに基づく機能安全と SOTIF の位置づけについて議論した。昨年度の最後の委員会がパンデミックにより中止となったため、新年度において改めて議論したもので、安全機能の性能範囲及びハザード/リスク源の予見性に基づく分類は以下の表のように分類される。SOTIF が対象とするハザード及びリスクのタイプは、予見可能リスク源の範囲外（コントロール不可能）、及び予見不能リスク源の範囲外（コントロール不可能）である。

5．機能安全規格とSOTIF規格の企図する範囲

表 3 安全機能の性能範囲及びハザード・リスク源の予見性に基づくリスクの分類

安全機能性能の (the safety functionis)	予見可能リスク源 (risk due to known risk source)	予見不能リスク源 (risk due to unknown risk source)
範囲内 (controllable)	限界内ハザード不具合リスク [1]	限界内ハザード不具合メタリスク [2] 限界内メタハザード不具合メタリスク [2]
範囲外 (uncontrollable)	限界外ハザードリスク [3] 対象外ハザードリスク [4]	限界外ハザードメタリスク [3] 対象外ハザードメタリスク [4] 限界外メタハザードメタリスク [3] 対象外メタハザードメタリスク [4]

[1] 機能安全規格でのランダムハードウェア故障SILを適用
[2] 機能安全規格での決定論原因能力(SC)を適用
[3] SOTIF規格の対象
[4] リスクアセスメントの対象

- IEC 61508 改訂国際委員会に対するドイツからの提案案件「電気・電子・プログラマブル電子安全関連系の故障（不具合）診断機能への SIL 付与」について討議した。
  - ISO 26262 は、電気・電子・プログラマブル電子安全関連系の概念（用語）を持たず、代わりにアイテムすなわち電気・電子・プログラマブル電子安全関連系の電気・電子部分のみを対象とした部分についての機能安全を規格化している。このため、ISO 26262 では、安全機能という概念はなく、要素安全安全機能という概念もない。
  - このため、ASIL はアイテムにも、アイテムの部分にも自由に付与することができるようだ。例えば、アイテムのデコンポジッションでは、アイテム全体及びアイテムの冗長部分に ASIL を割り当てている。
  - もっとも、デコンポジッションがアイテムの冗長部分なのか、元のアイテムとは全く独立した多層化したアイテム群なのかの区別も不明確ではある。自動車の現状から鑑みれば、多層化したアイテム群はコスト的に実現が困難と思えるので、デコンポジッションはアイテムの冗長部分意味しているのではないかと解釈するのが妥当かもしれない。
  - ドイツからの提案は、この ISO 26262 と日々格闘している機関からのものであるが、ISO 26262 では故障（不具合）診断機能への ASIL 付与の方法が規定されていないので、IEC 61508 に規定してほしいというものである。
  - IEC 61508 において、「電気・電子・プログラマブル電子安全関連系」の定義は「安全機能を遂行するシステム」であり、「安全機能」の定義は「電気・電子・プログラマブル電子安全関連系によって遂行される機能」となっている。
  - 本案件は、上記の定義が理解されていないことと、ISO 26262 と IEC 61508 とのギャップから生じた提案であると推量できる。
  - 討議の内容は次であった。
    ① 基本的に、SIL は、安全機能に付与する、つまり、電気・電子・プログラマブル電子安全関連系の全体が遂行する機能に付与するものであり、電気・電子・プログラマブル電子安全関連系のセンサー部、論理部、アクチュエータ部などのサブシステム、及びそれらの部品など電気・電子・プログラマブル電子安全関連系を構成する要素が行う要素安全機能に SIL を付与することは上記の定義に矛盾する。
    ② 診断機能のみでは安全機能に対して何ら貢献しない。診断の結果、警報を出す、修理を行う、運転を続けるために不具合チャネルから正常チャネルの切り替える、運転を停止するためにシャットダウン機能を発動するなどの対応措置が成功することで意味がある。つまり、診断結果とその結果への対応との組み合わせにより安全機能に貢献するので、診断（要素安全）機能とそれらの対応（要素安全）機能との組み合わせで評価する必要がある。
    ③ ただし、現状の Part 6 のシステムモデルでは、ほとんど対応機能が考慮されていないので、Part 6 を改訂するにはかなりの作業量が必要になるだろう。
  - 現状、上記①は国際委員会で理解されつつある。しかし、上記②、③はほとんど理解されていない範囲にとどまる。
  - 今後の本提案に対する改訂委員会の対応の推移に注目していくこととなった。

- 故障物理に基づく信頼性予測方法について検討し、次の認識を得た。
  - SAE が提案している故障物理に基づく信頼性予測方法（SAE J3168）が検討した。

- この規格は、使用期間内に摩耗故障が発生しないように故障物理に基づくシミュレーションを行い、設計する手法であり、故障率を推定する手法ではない。
- ハンドブック予測に基づかない故障率推定方法については説明されていない。

- コヒーレント FT(fault tree)とノンコヒーレント FT について検討した。
  - 信頼性ブロック図から FT 図を導く方法が示された。複雑なブロック図も FT 図に変換することができる。
  - コヒーレント FT とは、「基本事象が故障状態（フォールト）からアップ状態に修復すると、システムがアップ状態にあればアップ状態を維持し、故障状態にはならない」という条件、及び、「基本事象がアップ状態から故障状態に遷移すると、システムが故障状態状態にあれば故障状態を維持し、アップ状態にはならない」という条件を満たすシステムの FT を意味する。
  - コヒーレントＦＴでは、最小カット集合という理論が適用できて、容易に FT の定量化が可能である。
  - ノンコヒーレント FT では、上記の条件が満たされず、最小カット集合の理論が適用できないため、インプリカント及びプライムインプリカントの理論を用いて定性的/定量的に解析する必要があり複雑になる。
  - 信頼性の FT ではコヒーレント FT が多く、安全性の分野ではノンコヒーレントの FT が必要な場合が多い。
  - 現実には、ノンコヒーレント FT を適用すべきところであっても、誤ってコヒーレント FT を用いている場合が多い。
  - ノンコヒーレント FT の例として、交差点での 3 台の車 A、B、C と信号との考えられる状態と事故との関係が示された。状態は 8 通り（A（停止・動作）×B（停止・動作）×C（停止・動作））あり、各状態での事故との関係の分析が必要となる。これらを FT 図にまとめ、確率も計算できることがわかった。

- IC 顧客返品からの学習と返品の低減に関する論文を検討した。
  - NXP セミコンダクター社が、2016 IRPS tutorial で発表した自動車用 IC のフィールドでの返却品の分析結果についての内容である。
  - 製品の故障率はバスタブ曲線にのり、10 年以内の故障率は、0.01～0.1 FIT レベルである。
  - 製造年が最近に近いほど、返却率（故障率）は小さくなる（習熟効果）。
  - 故障モード分類で、比率が高いのが EOS/ESD が約 55%、NOT（No Trouble Found）が約 17%である

- ヒューマンファクタを安全関連系に組み込む案について検討した。
  - 「ヒューマンファクタを安全関連系に組み込む案」を検討した。
  - 人間を介さないロボットを介した安全システムが主流であるが、人間が関与する場合もあるので、人間が関与する場合を想定している。
  - ヒューマンエラーの内容に応じたクラス分けと得点付けを行い、SIL の求め方を提案している。

- TI（Texas Instruments）の機能安全対応半導体の開発状況について資料を検討した。

- TI が公表している機能安全対応半導体の開発状況について記述されている。
- 機能安全対応製品には、機能安全対応製品（Functional Safety-Capable）、機能安全品質管理製品（Functional Safety Quality-Managed）、機能安全準拠製品（Functional Safety-Compliant）の 3 種類がある。機能安全準拠製品は、認定された機能安全プロセスに従って開発した製品である。
- いずれの製品にも、故障率計算と故障モード分布が示されている。但し、高集積化 IC 製品の情報については、開示条件が厳しい（米国政府の許可が必要）。故障率計算は、IEC/TR 62380 と SN29500 を基に計算している。但し、トランジェント故障（ソフトエラー）率は、TI が独自に試験した結果が掲載されている。
- 故障モード分布は、故障モードの内容と発生比率が提示されている。

- ゲストより、JEITA で検討している半導体集積回路信頼性認定ガイドラインにつて講演があり、質疑応答を行った。
  - LSI と個別半導体別々に作成している。LSI は EDR-4708C（半導体 LSI 認定ガイドライン）、個別半導体（主にパワーデバイス対象）は EDR-4711 A（個別半導体認定 ガイドライン）である。
  - 耐用期間（常用期）の故障率の求め方として、LSI では 2 種類の方法、個別半導体では、5 種類の方法を提示している。LSI では、(1)指数分布を仮定した方法（多くの規格で採用している）、(2)ワイブル分布（m<1）を仮定した平均故障率を求める方法（JEITA 提案）である。スクリーニングのデータが必要であるが、(2)の方法が推奨される。

- ゲストより多状態を持つ要素を含むシステムの S-A プロセスチャートを用いたハザードの分析について講演があり、質疑応答を実施した。
  - 多状態(相反状態)を持つシステムのハザード分析には、S-A プロセスチャートを用いる手法が有効である。
  - 例として、(1) 環境試験槽の停止起因のハザードの同定とその抑制策の導出、（2）ガス爆発による危害発生、（3）修理系 2 冗長電源システムの故障プロセスの同定の 3 例を示し、S-A プロセスチャートを用いる手法の解説とその有効性が説明され、質疑応答を行った。

- 故障物理アプローチ（ロバストネス検証）について検討した。
  - ISO 26262-5：2018 の第 3 番目の故障率の見積もり方法として「エキスパートの判断」がある。
  - エキスパートの判断の際に用いる基準として提示されている SAE J1211（ E/E モジュールのロバストネス検証（同内容の規格が ZVEI（第 2 版: June 2013））について検討した。
  - ロバストネス検証（RV）は、製品が、指定されたライフタイムの間、定義されたミッションプロファイルの下で十分なマージンを持って意図された機能を実行できることを示すプロセスである。
  - そのため、ミッションプロファイルの適用方法、故障の知識マトリックスの活用、分析・モデリング・シミュレーション（AMS）の活用、インテリジェントテスト方法、製造プロセスのロバストネスとその評価方法、及びロバストネスインジケーターフィギュア（RIF）によるロバストネスの判断など、詳細な手法が文書化されている。

- IEC 63142-CD（56/1912/CD）の概要について検討した。
  - IEC TC 56 で 2021 年 1 月に提案された IEC 63142-CD（A global methodology for reliability data prediction of electronic components）の概要が説明された。
  - 本文書は、FIDES　Ed. A：2010 も基にしており、第 1 部（予測方法論）と第 2 部 （IEC 63142 用の基礎故障率とその他の入力パラメータ）に分割されている。今回提案の CD は第 1 部である。
  - FIDES ed. A の前半（I、II、III：電子部品等の故障率予測算出式）は、本文になり、後半（IV、V：信頼性プロセスのコントロールと監査のガイドと推奨、質問表）は、附属書（informative）になっている。
  - 採用している故障率予測算出式は、FIDES と同じである。

以上のように、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。