R-30-RC-01

平成３０年度

電子部品信頼性調査研究委員会
研究成果報告書

人工知能（AI）技術と安全性、及び
ハードウェア開発における ASIL 評価方法と例

―　　―

付録 A：　IEC CD 63162/TR/Ed1:電気部品－信頼性
－基準条件における基準故障率
付録 B：自動車用半導体デバイスロバストネス検証
ハンドブック（ZVEI：第３版）

平成３１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

一般財団法人日本電子部品信頼性センター（RCJ）では、自動車電子制御に関わる機能安全規格 ISO 26262:2011「自動車－機能安全」及び基本機能安全規格である IEC 61508:2010（翻訳 JIS C 0508）等の理解を深めて機能安全活動を効果的に実践するため、平成 25 年度に「電子部品信頼性研究委員会」を設置した。平成 30 年度では、平成 29 年度に引き続い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）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とになった。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を作成し、システムの信頼性向上に資することを目的としている。本年度では、次の調査を企図した。

（１） 機能安全規格（IEC 61508、ISO 26262）の特にハードウェアを中心とする理解
（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係る調査
（３） 外部専門家を招いての講演と討論

その結果、平成 30 年度では第 1 回から第 8 回までの研究委員会を実施して、次のような成果・知見を得ることができた。

・ 自動運転の安全について検討－IRPS（信頼性物理国際会議）で、Riccardo Mariani 氏（Intel、イタリー）より発表された“An Overview of Autonomous Vehicles Safety”の内容について検討した。自動運転の安全では、ISO 26262 に基づくハードウェア（H/W）及びソフトウェア（S/W）の安全機構の他に、サイバーセキュリティ、企図機能の安全（safety of intended functionality（SOTIF））、義務遂行能力由来の安全（responsibility-sensitive safety（RSS））など大きな課題がある。

－ サイバーセキュリティ対策を ISO 26262 第 2 版で要求している。サイバーサイバーセキュリティの脅威及び対策は、以下のようなものである。
  ① 機能安全に影響を及ぼすセキュリティの脅威（安全機構が機能喪失する。）
  ② ハッカーによる安全機構への攻撃
  ③ H/W ランダム故障の検出可能なセキュリティ対策（例：コード）
  ④ セキュリティアタックを検出する安全対策（例：チェッカー）
－ 企図機能の安全（SOTIF）は、環境のセンシングに信頼を置いているシステムで、企図機能の性能限界による安全目標の侵害に関係する。これには例えば次の要因があげられる。
  ① 状況を正確に把握する機能の性能不足
  ② センサー入力のばらつきや環境条件に対応する機能の性能不足
－ 義務遂行能力由来の安全（RSS）とは、マルチエージェント安全とも呼ばれる。例えば、人間が運転する車が、急に自動運転車（AV）の車線に割り込んだ時に、AV は衝突の回避ができない（AV の衝突回避義務性能が不足している）。このような場合のライアビリティ（利用者、自動車会社、保険会社）リスクの明確化が必要である。

・ 現在開発中の IEC TR 63162「電子部品－信頼性－基準条件における基準故障率（CD）」について検討した。本文書は、新たに規格化が提案された基準条件における基準故障率を取り上げた技術報告（TR）で、IEC 61709「電子部品－信頼性－故障率の基準条件及び換算のためのストレスモデル」を補完す

ることを意図する。次の特徴をもつ。

－　基準使用条件（IEC 61709 と同じ条件）に対する基準故障率を提供する。

－　故障率の値は、各種モデルの平均値としているが、数値を見ると、SN 29500 を基にしていると思われる。

－　電子部品の種類は、IEC 61709 と同じ種類を取り上げている。但し、約半分の種類について、故障率は検討中として現在のところ記載が無い。

この内容については、附属書に示している。

・　自動車産業分野で最近活用され始めたハザード分析技法”STAMP（Systems Theoretic Accident Model and Processes）”について、独立行政法人情報処理推進機構（IPA）が発行している「はじめての STAMP/STPA」を題材に、STAMP の概要について検討した。STAMP は、HW の不具合よりも SW の不具合に起因するシステム不具合分析に向いているようである。

・　IEC TC 65 A（工業用プロセス計測制御、システム一般）WG18 で、新たに防衛システムの機能安全規格を開発することになり、パリで最初の開発会議が開催された。その概要が報告された。

－　規格番号とタイトルは、IEC 63187（Functional safety - Framework for safety critical E/E/PE systems for defense industry applications）である。

－　陸上及び海上に係る防衛システムへの IEC 61508 の応用を目的として、規格を開発する。空軍が入っていないが、理由は不明である。（理由の一つとして、航空・宇宙産業ではすでに機能安全規格と類似の規制等が実施されていることが考えられる。例えば、機能安全の SIL に類似した DAL（Development Assurance Level）を用いた、不具合へ対応する設計開発フレームワークがあげられる。）

・　ISO 26262 では、部品の信頼性も記載されているが、部品供給者が開発した車載用電子部品の信頼性規格もあり、それらを検討した。

－　代表的な規格は、AEC 規格、SAE 規格、ZVEI 規格（ドイツ）などがある。

－　AEC 規格は、各種試験条件と試料数を指定し、故障 0 であれば、合格と判定する規格である。一般に、「緩い試験規格であり、これらの試験で合格しても、車載用として使用できるとは限らない。」というのが一般的な見解である。

－　SAE 規格及び ZVEI 規格は、ロバスト性検証試験の規格であり、寿命検証を目的にしており、故障に至るまでの試験を行うことを基本にしている。設計・開発段階で行い、目標寿命達成には有効な試験方法と考えられる。この ZVEI 規格（自動車用半導体デバイスのロバストネス検証ハンドブック（ZVEI、第 3 版：2015））を付録に掲載している。

・　外部専門家（竹市正彦氏・ナブテスコ（株））により、鉄道関連のサイバーセキュリティ規格の開発状況が紹介された。

－　サイバーセキュリティ規格の開発が IEC TC 9「鉄道用電気設備とシステム」の AHG 20 で進行中

である。
- 安全とセキュリティの両方の幅広い分野を考慮する必要があり、またどこに焦点を絞るかが課題である。
- アジャイル（AGILE）思考（要求のすりあわせを行いながら開発し、常に見直しを行う）が必要ではとの議論があった。

・ IEC 61508 3rd edition に向けた規格改定状況の報告があった。
- IEC 61508 3rd edition の CD は、2020 年 1 月の予定である。
- 仏グルノーブル会議で審議された IEC 61508（3rd Ed.）Part 6（Guidelines on the application of IEC 61508-2 and IEC 61508-3）附属書 B（Example of technique for evaluating probabilities of hardware failure）の WD（CD になる前の素案）について説明があった。
- Part 6 中の多数の信頼性関連公式が修正されている。
- 日本提案の「共通要素を持つ多重防護層の安全分析方法とその事例」が当該附属書 B に採録予定となっている。

・ ISO 26262-5 : 2018 の仮訳（附属書 D は省略）、及び 2018 年版と 2011 年版との比較資料を検討した。
- 本文の要旨に大きな修正は無いが、語句の修正は多い。
- 備考及び事例が多く追加された（解説が多くなった）。
- 附属書が追加された。

・ ISO 26262-5 : 2018 のシングルポイントフォールトメトリック、レイテントフォールトメトリック、ランダムハードウェア故障の確率的メトリック（PMHF）の評価方法と事例（図 E）について議論した。
- PMHF の算出式

$$PMHFest = \lambda_{SPF} + \lambda_{RF} + \lambda_{DPF\_det} \times \lambda_{DPF\_latent} \times T_{Lifetime}$$

の導出根拠について議論した。IEC 61508-6、または佐藤吉信著「機能安全の基礎（日本規格協会）」を参照するとよい。

・ 2019 年 3 月中旬にパリフランス規格協会本部（AFNOR）で開催される MT 61508 会議において、日本が提案予定の「人工知能（AI）に関する要求事項の機能安全規格への採録」について説明があり、議論した。

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。