AdaCore | Build Software that Matters

Tech Paper

Investing in SPARK:

Formal methods for automotive functional safety

自動車の機能安全を実現するための形式手法への取り組み

概要

最近の自動車リコールでは、ソフトウェアの不具合が原因となるケースが増えています。そのため、安全規格 ISO 26262 を遵守することは、技術的な義務を超えて、企業の信頼や競争力に関わる重要なポイントになっています。

高い安全性が求められる自動車ソフトウェアの開発で、システムの信頼性とセキュリティを向上させるために「形式検証」という手法が注目されています。NVIDIA は、自社の DriveOS に ISO 26262 の最高レベルの安全性を確保するため、Ada 言語と SPARK 言語を使用した効率的な開発プロセスを公開しました。

はじめに

自動車業界では、ソフトウェアが原因であるリコールが増加しており、その割合は近年大幅に上昇しています。この傾向の背景には、車載ソフトウェアの複雑化、とくに先進運転支援システム（ADAS）や電気自動車（EV）の普及が大きく影響しています。

Ars Technica の記事によると現在、自動車リコールの 5 件に 1 件以上がソフトウェアの修正が原因であり、ソフトウェアに関連するリコールは、電装システムや自動緊急ブレーキなどの ADAS 機能、パワートレイン部品に関わることが多いと報告されています。

車の進化はソフトウェアによって支えられていますが、その分、ソフトウェアが複雑になることで、安全性を守るための課題も大きくなっています。特に人命に関わる場面では、確実な安全対策が求められています。

ISO 26262 は、自動車業界における機能安全のための国際規格で、ハードウェアやソフトウェアを含む車両の電気・電子システムに適用されます。安全に関わる機能について、満たすべき要件や、開発プロセスで使用される手法・ツール・工程などが定められています。

ISO 26262 が重要な理由

> 電気・電子（E/E）部品の機能安全を確保することは、人命を守り、システムの故障による事故を防ぐために不可欠となっています。

ISO 26262 の遵守は、単なる技術的な義務ではなく、ビジネス上の重要課題です。車両がますます複雑なソフトウェアシステムに依存するようになる中で、電気・電子（E/E）部品の機能安全を確保することは、人命を守り、システムの故障による事故を防ぐために不可欠となっています。

コンプライアンス（規格の遵守）は、注意義務と責任を果たしていることの証明であり、厳しい世間の目と厳格な責任規定が求められる自動車業界において極めて重要です。ISO 26262 に準拠しない場合、車両のリコール、訴訟、規制当局からの罰則、そして企業イメージに悪影響を及ぼすなど、深刻な結果を招く可能性があります

さらに、開発の進め方を ISO 26262 に適合させることで、エンジニアリングの規律を高めるきっかけになります。
これにより、システム設計が体系化し、作業の履歴や文書化が促進され、世界各地に分散したチームやサプライヤ間でも一貫性を保持することができます。
また、OEM やサプライヤにとっても、ISO 26262 への準拠は、安全性と品質への取り組みを示す重要な差別化要因となり、入札やパートナーシップの競争において有利に働く可能性があります。

ISO26262 の概要

ISO 26262 は、自動車システムのライフサイクル全体を対象としています。これは、構想・設計から製造、運用、廃棄に至るまでのすべての段階を含みます。ISO 26262 の中心となるのが「自動車安全水準（ASIL）」であり、潜在的な危険の重大性、発生頻度、制御可能性に基づいて、リスクを A～D の 4 段階に分類します。ASIL のレベルが高いほど、より厳格な検証・妥当性確認プロセスが求められ、各部品に必要な安全対策の指針となります。

ISO 26262 では、4 つの ASIL（安全度水準）が規定されています。

ASIL（自動車安全度水準）はハザード（危険要因）分析とリスクアセスメント（危険評価）」の結果として決定されます。ISO 26262 において、ハザードは、システムに関連する有害な影響の重大さとその影響が実際に発生する可能性（起こりやすさ）を考慮して評価されます。

それぞれのハザードは、次の 3 つの観点から評価されます。

1. **Severity**：重大度
   致命的な負傷
2. **Exposure**：**発生**頻度
   頻繁に起こる状況
3. **Controllability**：回避可能性
   運転者がその危険を回避できる可能性

これらの要素を総合的に判断することで、ASIL が決定されます

ASIL（自動車安全度水準）は、最も高い自動車の危険度を示す「ASIL D」から、ISO 26262 の安全プロセスにおいて特別な安全要求が不要な「QM（品質管理）」までの範囲で分類されます。ASIL D は、最も厳格な安全要求と検証が必要とされるレベルで、QM は自動車の安全上のリスクがないと判断されたアプリケーションに適用されます。これらの間には、危険度と安全保証の度合いに応じた中間レベルが存在します。

ASIL D（Automotive Safety Integrity Level D）とは、ISO 26262 で定義されている最も高いレベルのハザード分類（負傷リスク）を指し、許容できないリスクを回避するために、最も厳格な安全対策が求められます。特に、ASIL D は重大な生命の危険や致命的な負傷につながる可能性が高い故障や誤動作のケースを想定しています。そのリスクを防ぐために、安全目標（Safety Goals）が十分に設定され、確実に達成されていることを最高水準で保証する必要があります。

ASIL D が必要とされる危険な例として、「すべての車輪のブレーキが効かなくなる」という状況があります。このような重大な故障は、命に関わる事故につながる可能性が高いため、ASIL D に分類されます。

ASIL D の要件に適合している製品は、それより低いレベル（C、B、A）にも自動的に適合しています。

それぞれの ASIL レベルの特徴は以下の通りです：

- **ASIL C**：中～高リスク（例：運転支援機能など）
- **ASIL B**：中程度のリスク（例：ヘッドライトやブレーキランプ）
- **ASIL A**：低リスク（例：後部ライト）
- **QM（Quality Management）**：安全とは直接関係のない部品（例：GPS など）

ISO 26262 への準拠は、単なる規制対応ではなく、製品品質、顧客からの信頼、そして企業イメージへの戦略的な投資です。規格の範囲を正しく理解し、厳密な検証技術を適用し、形式手法を取り入れ、使用するツールの妥当性を確認し、ASIL（自動車安全度水準）を通じて安全目標とリスクレベルを整合させることで、自動車開発者は危険を体系的に低減し、システムの信頼性を高めることができます。

形式手法は ISO 26262 認証にどのように役立つのでしょうか？

自動車業界の進化するニーズに対応するために、開発者は形式検証をプロセスに取り入れることで、システムの信頼性と安全性を大幅に向上させることができます。形式手法は、特に ASIL D や C といった高い安全度水準への対応において、非常に有効です。

形式検証フレームワークは、ハードウェアやソフトウェアの設計が正しく行われているかを、数学的な形式証明を用いて評価する手法です。従来の手法（テスト、レビュー、静的解析、MISRA-C などのコーディング規約）とは異なり、形式手法は、システムが定められた安全性やセキュリティ要件に適合していることを数学的に保証します。テストが限られた入力サンプルからソフトウェアの特性を推測するのに対し、形式手法はすべての可能な入力に対してその条件が成り立つことを数学的に証明できます。

形式手法は、情報の安全な流れ、実行時エラーの回避、形式的に定義された要件に対する機能的正しさなどの条件を検証するのに役立ちます。証明技術やハードウェア支援の進歩により、形式手法は高信頼性システムのソフトウェア開発にとって実践的な構成要素となっています。

NVIDIA が形式手法を導入

高度な ADAS（先進運転支援システム）や自動運転機能への需要の高まりにより、ECU（電子制御ユニット）の数が増加し、それに伴ってソフトウェアの複雑性、通信、配線も増加しています。NVIDIA はこの課題に対し、複数の ECU の機能を統合したハードウェアとソフトウェアのフルスタックプラットフォーム「DRIVE® AGX」で対応しています。このプラットフォームは、ADAS および自動運転をサポートします。

DriveOS が ISO 26262 の最高レベルの安全保証を迅速かつ効率的に達成するために、NVIDIA は Ada 言語と SPARK 言語を採用しました。

DriveOS は、異なる重要度レベルのソフトウェアコンポーネントを分離する役割を担っており、ECU の数を減らし、通信や配線の簡素化を可能にしています。DriveOS が ISO 26262 の最高レベルの安全保証を迅速かつ効率的に達成するために、NVIDIA は Ada 言語と SPARK 言語を採用しました。

Ada 言語と SPARK 言語について

Ada プログラミング言語は、SPARK（Ada 言語向けの演繹的形式検証技術）と組み合わせることで、高信頼性が求められるアプリケーションの開発において、最も信頼性の高いプログラミング言語のひとつとされています。

SPARK 言語と、SPARK Pro ツールによって提供される SPARK 解析は連携して動作し、ソフトウェアのビルドやテストを行う前に、コンポーネントの要件や脆弱性の有無など、ソースコードレベルでソフトウェアの振る舞いの正しさを自動的に検証します。

SPARK Pro は、形式証明による演繹的プログラムの検証力を開発チームにもたらし、メモリの所有権チェックやデータフロー解析から、実行時エラーの排除、さらには機能的正しさの証明に至るまで、スムーズにスケールアップすることを可能にします。このようなスケールで競合できる言語、ツール、手法は、SPARK だけで、欠陥が少ないソフトウェアが実現され、運用後のコスト削減につながります。

SPARK Ada リファレンスプロセスによる ISO-26262 開発

NVIDIA は AdaCore と協力し、Ada と SPARK を活用して ISO 26262 認証ソフトウェアを開発した成功事例を、自動車業界全体で再現できるように、直ちに利用可能なリファレンスプロセスとして公開しました。

NVIDIA は、ソフトウェアの中でも特に重要なコンポーネントの開発に Ada と SPARK を利用しました。これにより、形式手法や Ada/SPARK が持つ安全性の特性を活用できる開発プロセスを構築し、両言語の能力を最大限に引き出すことが可能となりました。

AdaCore と NVIDIA は、このリファレンスプロセスをオープンソースのドキュメントとして公開しました。これにより、Ada と SPARK を採用することが可能になります。ドキュメントは以下のリンクから参照いただけます。

https://github.com/NVIDIA/spark-process
https://nvidia.github.io/spark-process/

安全性だけにとどまらない Ada と SPARK の活用 ： NVIDIA が取り組むファームウェアセキュリティの事例

サイバーセキュリティ環境がますます厳しくなる中、NVIDIA はソフトウェア開発手法を見直し、何を改革する必要があるかを検討しました。そして、重要な組込アプリケーションに対して従来使用していた言語やツールセットのコストについて疑問を持ち始めました。

NVIDIA のソフトウェアセキュリティチームは、測定可能な手法や戦略を幅広く検討しました。その結果、多くの手法の基盤が数学的な形式手法や形式的証明ツールであることに気づきました。また、これらのツールはこの 10 年間に大きく進化していることも見出しました。

そして「形式手法の活用を支援する言語やツールにはどんなものがあるだろうか？」検討し、NVIDIA は SPARK に出会いました。

James Xu 氏は、NVIDIA の GPU ソフトウェアセキュリティ部門のシニアマネージャです。

「SPARK を使う主な理由は、その言語が提供する保証にあります」と Xu 氏は語っています。

「SPARK でコーディングしていると、より自信を持てるようになります。SPARK 言語自体が、C 言語でよくある、誰もが陥りがちなミスを防いでくれるからです。」

「この言語に期待した価値のひとつは、実行時エラーが発生しないことです。コードが一般的な落とし穴を回避できると分かっているのは非常に魅力的です。SPARK でコーディングしていると、より自信を持てるようになります。なぜなら、SPARK 言語自体が、C 言語でよくある、誰もが陥りがちなミスを防いでくれるからです。」

「SPARK でアプリを書き終えたときに、多くのテストやコードの一行ずつの確認をしなくても、メモリのエラーやオフバイワンエラー（off-by-one errors）、型の不一致、オーバーフローやアンダーフローなどの問題が存在しないことが分かるのは、とても素晴らしいことです」と Xu 氏は語っています。「また、MITRE の CWE エラーの一覧表を見たときに、多くのエラーが存在しないことは嬉しいことです。つまり、この言語ではそうしたエラーを起こすこと自体が不可能なのです。」

NVIDIA は、ソフトウェアセキュリティ分野において画期的なリーダーシップと革新性を示してきました。そして、非常に困難な目標を掲げ、半導体業界では前例のないことを成し遂げるために大胆な道を選びました。ここ数年にわたり、SPARK の採用が正しい選択であったことを何度も証明しており、NVIDIA の取り組みに続こうとする人々にとって新たな道を切り開いてきました。

終わりに

SPARK は、検証可能なソフトウェアの安全性を実現するための、実用的で拡張性のある手法を提供します。言語レベルで特定の種類の脆弱性を排除し、正しさを数学的に証明できるため、従来のような後段のテストに頼るだけでなく、システムに対する信頼性を定量的に評価できるようになります。

NVIDIA が SPARK を採用し、それに関連する ISO 26262 のリファレンスプロセスを公開したことは、朗報です。この取り組みによって、形式手法が実現可能なだけでなく、現代の自動車システムに求められる高度な安全性を達成するうえで非常に価値があります。

SPARK に投資することで、規制の要求に対応し、開発リスクを減らし、将来に備えた堅牢なソフトウェアを提供できるようになります。それは、勘や慣習に頼るのではなく、「証明」に基づいて実現されます。

参考資料

https://arstechnica.com/cars/2024/09/more-than-20-of-vehicle-recalls-are-software-fixes-now/#:~:text=In%202022%2C%20almost%2022%20percent,fully%20charging%20to%20100%20percent.

AdaCore

adacore.com

※本資料は、AdaCore の Tech Paper を意訳したものです。正確な内容については、原文をご参照下さい。

https://www.adacore.com/papers/investing-in-spark-formal-methods-for-automotive-functional-safety

本社　〒222-0033　神奈川県横浜市港北区新横浜 3-17-6

TEL:045-474-9095 FAX:045-474-8823

URL: https://www.itaccess.co.jp

IT Access®

アイティアクセス株式会社

本社　〒222-0033 神奈川県横浜市港北区新横浜 3-17-6

TEL:045-474-9095 FAX:045-474-8823

https://www.itaccess.co.jp/service/adv/brand/adacore/

2025/10