【機能安全シリーズ #1】

機能安全にアジャイル開発を適用する際の課題（前半）

近年、自動車業界では SDV（Software Defined Vehicle）や OTA（Over-the-Air）の進展により、ソフトウェアを中心とした開発の在り方が大きく変化しています。これらの変化に対応するため、アジャイル開発、AI 活用、データドリブン開発、クラウドベース開発といった手法の導入が加速し、多くの開発領域で効果を上げています。

本シリーズでは、このような自動車開発の変化に伴い顕在化している「機能安全対応の課題」を取り上げていきます。初回は、自動車業界のソフトウェア開発に関わる技術者が直面する「機能安全にアジャイル開発を適用する際の課題」について解説します。前半となる今回はアジャイル開発適用の課題を中心に、次の機会の後半では解決策を考察していきます。

ソフトウェアの安全分析の複雑性

機能安全にアジャイル開発を適用する際の課題の一つに、複雑性があります。ソフトウェアの安全分析では、単なる内部設計の評価にとどまらず、ソフトウェア異常がシステム全体に与える影響、使用するハードウェアリソースの有効性、さらには他のコンポーネントやユニットとの干渉まで考慮する必要があります。そのため、アジャイル開発のように短期間で繰り返し開発を行う環境では、ソフトウェアの安全分析がボトルネックになることが多々あります。今回は、このソフトウェアの安全分析の複雑性を理解するために、具体例として電動パワーステアリングシステム（以下、EPS）を取り上げ、実際の安全分析の手順を説明します。

他の車載システムのソフトウェアと同様に、EPS のソフトウェアの安全分析は、操舵機能の異常要因の抽出、操舵異常を防止する安全機能の充足確認、これらの安全機能が他の部位から妨げられないことの確認など、複数の目的があります。この中の「操舵異常を防止する安全機能 A が他の部位から妨げられないことの確認」の目的におけるソフトウェアユニットの安全分析の手順を例に説明します。

1. 妨害要因の洗い出し ：安全機能 A を妨害する可能性がある内部と外部の要因をそれぞれ抽出
2. 妨害要因の選別 ：抽出した要因の異常状態毎に安全機能 A へ与える影響を精査
3. 追加の安全機能の検討：妨害要因の影響に対する追加の対策要否を判断
4. 安全論証の作成 ：1~3 の因果関係を整理し安全論証を構築

この 1～4 のステップを、操舵異常を防ぐ安全機能 A を配置した複数のソフトウェアユニットごとに繰り返し、1 つの安全機能 A の「操舵異常を防止する安全機能が他の部位から妨げられないことの確認」が終了します。さらにその他の安全機能 B、安全機能 C についても、同様のステップを繰り返します。これらの作業は EPS のソフトウェアの安全分析の目的の一部にすぎず、ソフトウェア開発の全体では膨大な量の安全分析が必要となります。

もう 1 つの側面は、安全分析の多面的な難しさです。EPS の安全機能を担う 1 つのソフトウェアユニットに着目した場合、安全分析の担当者は次の観点が求められます。

- 上下階層の影響：操舵機能へ与える影響、ソフトウェア OS や lock-step マイコンからの制約
- 同一階層の干渉：同一階層内の他のソフトウェアユニットのインタフェース信号や処理作用の干渉
- 時間進行の影響：内部処理の進行や制御全体の状態遷移などによる影響

ソフトウェアの安全分析では、着目したソフトウェアユニットの設計情報だけでは不十分であり、ソフトウェア全体や EPS 機能、マイコンやモーター制御のハードウェアに関する知見や情報を取り入れた分析が必要です。

上記 2 点の膨大さと難しさが伴う複雑性が、機能安全にアジャイル開発を適用することの阻害要因の一つとなっています。

アジャイル開発にソフトウェアの安全分析を取り入れる際の課題

次は視点を「ソフトウェア開発フロー」に変えて、ウォーターフォール開発をアジャイル開発に置き換えた場合のソフトウェアの安全分析に関わる影響について考察します。

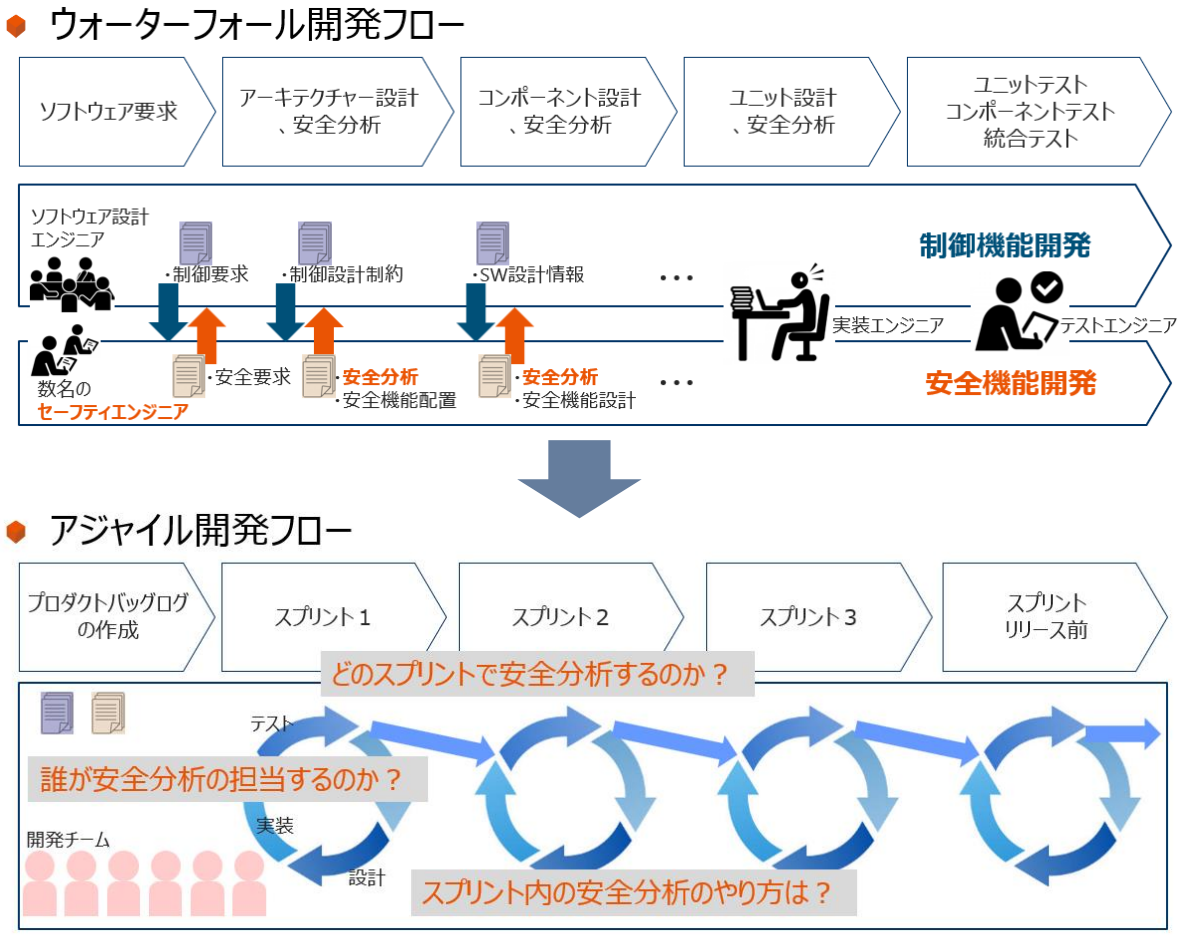

図 1

ウォーターフォール開発では、制御機能の開発と安全機能の開発をすり合わせながら、仕様化・設計・安全分析を進め、安全機構の検証や非干渉性の分析を行います。一方、アジャイル開発では安全分析の工程を加えていく際に、特に以下の点が課題となります。

- 安全分析の担当者は誰か　　：アジャイル開発チームの役割分担
- いつ安全分析を実施するのか　：スプリントに対する実施計画
- 安全分析の実施方法　　：スプリントごとの安全分析の手順化

つまり、機能安全のウォーターフォール開発の各階層で発生するソフトウェアの安全分析を、アジャイル開発の開発フローでどのように取り入れるかが、アジャイル開発の適用時の課題となります。例えば、「アジャイル開発でも、ソフトウェア設計のアーキテクチャ、コンポーネント、ユニットといった安全論証の因果関係を構築するための階層設計を取り入れているか？」「アジャイル開発チームの複数名がセーフティエンジニア相当の安全分析を担当できるか？」といった面への工夫が必要です。

まとめ

今回は、機能安全対象のソフトウェア開発へアジャイル開発を適用する際の課題について、特にソフトウェアの安全分析に焦点を当てて解説しました。アジャイル開発が進展する中、自動車業界の開発手法も変化し続けています。品質や安全を確保しながら、最適な開発スタイルを模索していくことが重要です。また、次の機会では今回取り上げた課題に対する解決方針について掘り下げていく予定です。

今回挙げた課題やソフトウェアの安全分析、アジャイル開発等の詳細については、弊社までお気軽にお問い合わせください。

2025/3/12 吉川 初芽