【機能安全シリーズ #2】

機能安全にアジャイル開発を適用する際の課題（後半）

前回（前半）では、自動車業界のソフトウェア開発に携わる技術者が直面する「アジャイル開発にソフトウェア安全分析を取り入れる際の課題」について、課題提起を中心に解説しました。今回（後半）では、機能安全にアジャイル開発を適用する際の解決策を模索していきます。

アジャイル開発にソフトウェアの安全分析を効率的に組み込むための 3 つのアイデア

前回（前半）では、機能安全のソフトウェア開発を全てアジャイル開発に置き換える場合には、いくつかの課題が発生することをお話ししました。今回は、ウォーターフォール開発の中で、業界のソフトウェア開発の主流となっている V モデル開発の階層設計の良い点を活かしながら、アジャイル開発を適用する手段を探ります。

現在、業界で確立されたベストプラクティスは存在せず、アジャイル開発の適用方法は多岐にわたります。以下の 3 つの代表的なアイデアは、ソフトウェアの安全分析の質を確保しつつ、アジャイル開発の効果を発揮する内容です。

1. 並走関係　：図 2 のように、安全機能開発にはウォーターフォール開発を、制御機能開発にはアジャイル開発を適用
    - メリット　：セーフティエンジニアによる安全分析の手順や手法を維持可能
    - デメリット：開発プロセスが二重化し、相互インタフェースが煩雑になる
      安全関連部と非安全関連部の非干渉性の確保が前提となる

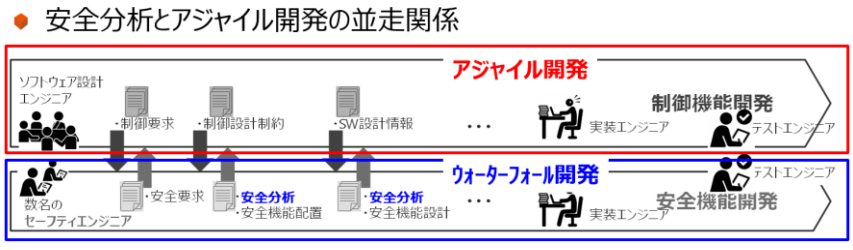

図 2

2. 前後関係　：図 3 のように、安全分析の工程から導出した結果を、アジャイル開発へ引き継ぐ
    - メリット　：ウォーターフォール開発の安全分析と同等のプロセスを適用できる
    - デメリット：安全要求やトレース指示など、アジャイル開発への要件詳細化に工夫が必要
      上流の安全分析情報が確定しないと、アジャイル開発が進められない

● 安全分析 ➡ アジャイル開発 の前後関係

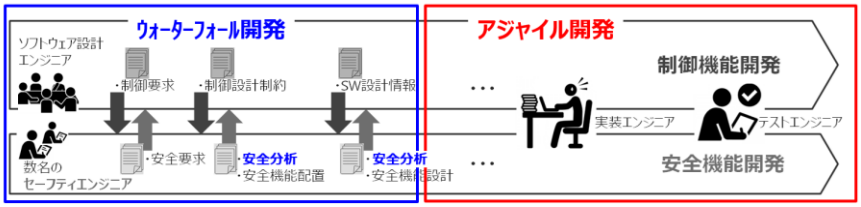

図 3

3. 共存関係 ：図 4 のように、スプリント単位で安全分析を実施
   - メリット ：アジャイル開発の柔軟性を最大限に活かせる
   - デメリット ：アジャイル開発に合わせた安全分析の適用や手順の策定が必要
     多くのエンジニアが安全分析のスキルを身に着ける

● アジャイル開発と安全分析の共存関係

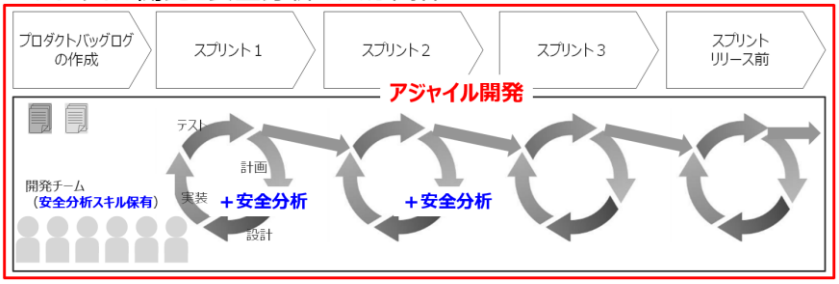

図 4

これらの関係の採用や選択は、対象システムや製品の特長、搭載するソフトウェアアーキテクチャの構造、開発組織の経験や力量を踏まえた総合的な判断が重要です。特に図 4 のアジャイル開発と安全分析の共存関係では、適用するスプリントごとの安全分析の目的と手順、並走するチーム間での役割分担など、ソフトウェア全体のアーキテクチャー設計や安全機能の動作確保の手段を考慮した安全分析の策定が必要です。

EPS ソフトウェア設計へのアジャイル開発の適用事例

ここでは、前半にも登場した電動パワーステアリングシステム（以下、EPS）の事例を取り上げます。EPS のソフトウェア設計において、車両適合領域の 1 つの「車速に連動したステアリングトルク感度調整」に初めてアジャイル開発を適用する事例について考察します。

EPS の制御は安全関連部と非安全関連部の切り分けが難しいため、事例の車両適合領域を非安全関連と位置付けるのは適切ではないと考えられます。このため、「2. 前後関係」と「3. 共存関係」を組み合わせた「車速に連動したステアリングトルク感度調整」のソフトウェア設計事例を解説します。

Step1：ソフトウェアコンポーネント設計 → ソフトウェアユニット設計の階層間で使い分ける

■ソフトウェアコンポーネント設計（従来のウォーターフォール開発工程）

- 「車速に連動したステアリングトルク感度調整」のソフトウェアコンポーネントの全体構造を設計する
- ステアリングトルク制御部とのインタフェースや安全に関する影響を分析する
- 「車速に連動したステアリングトルク感度調整」に必要な安全要求や適合制約を設定する
- 「車速に連動したステアリングトルク感度調整」の安全要求を詳細化し内部へ配置する
- 配置した安全要求や適合制約に影響を与える機能や異常要因を分析する
- 必要な追加の安全要求を検討し、ソフトウェア詳細設計（アジャイル開発）への要件を設定する
- 特に、各スプリントにおいて、安全設計の具体的な活動要件を明示することが重要

■ソフトウェアユニット設計（アジャイル開発を適用する工程）

- 下記 Step2 へ

Step2：アジャイル開発のスプリントに必要な安全分析を取り入れる

- Step1 の安全分析結果に従い、安全要求や適合制約に関係するソフトウェアユニットを特定する
- 特定したソフトウェアユニットとその他のソフトウェアユニットのスプリントを分ける
- 機能安全の経験や知識があるメンバーを加えた開発チームを構成し、特定したソフトウェアユニット設計を担当する
- 特定したソフトウェアユニットのスプリントでは、安全要求や適合制約に関する設計、検証、テストのトレースや因果関係など安全分析が必要な工程を定義する
- その他のソフトウェアユニットは、組織のアジャイル開発ルールに沿ったスプリントを適用する

このように、「車速に連動したステアリングトルク感度調整」には、アジャイル開発の部分的な適用が可能となります。この他の EPS 操舵制御部やセルフステアを防止する安全機構部などの安全関連領域へのアジャイル開発の適用は、ソフトウェアの安全分析の量や複雑さの規模が大きくなるため、開発チームのスキルや経験を考慮し、メリットとデメリットを総合的に検討する必要があります。

まとめ

２回にわたって、機能安全対象のソフトウェア開発にアジャイル開発を適用する際の課題と解決策について、EPS の事例を交えて解説しました。アジャイル開発を適用する領域の検討と、開発組織が機能安全設計とアジャイル開発の両方の知識や経験を積むことが重要です。品質と安全を確保しつつ、最適な開発スタイルを模索することが、今後のソフトウェア開発の強化や効率化につながります。

本記事で紹介した解決策やソフトウェアの安全分析、アジャイル開発に関する詳細な情報については、弊社までお気軽にお問い合わせください。

2025/3/26 吉川 初芽