安全設計活動の従来製品開発プロセスへの実装について（システム編）

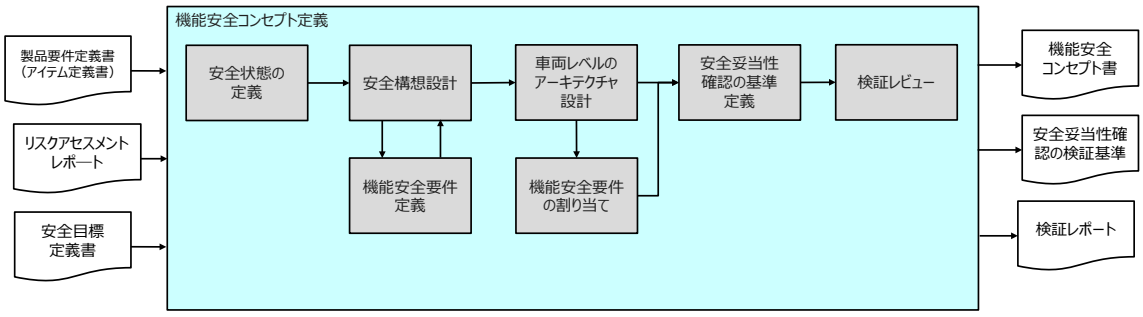
（小西）

2020 年 10 月に出版された「ISO 26262 実践ガイドブック 入門編～機能安全の正しいアプローチ～」では、「安全の基本アプローチ」と安全な製品を開発するための重要な三つの取り組み「安全設計」、「プロセスアプローチ」、「安全文化」を解説しています。

2021 年 2 月 10 日に出版予定の「新 ISO 26262 実践ガイドブック システムエンジニアリング編」では、プロセスアプローチと安全設計の視点で、安全ライフサイクルにおける各システムエンジニアリングの活動の流れと活動内容を具体的な事例（衝突被害軽減ブレーキ機能）を用いて解説しています。本メルマガでは、それらの中から、機能安全コンセプト開発の活動の流れと活動内容の一部を紹介いたします。ガイドブックで扱っているシステムエンジニアリングの領域は、ISO 26262 の Part-3 と Part-4 に該当します。

ISO 26262 では、電気/電子システム（以下、EE システム）の機能不全により引き起こされる安全上のリスクを安全技術や対策によって許容可能なレベルまで低減することを目的としています。この目的を達成するために、EE システム開発では、ランダムハードウエアフォールトに起因して発生する故障を考慮した安全設計だけでなく、ヒューマンエラーに起因して発生する故障も一緒に考慮する必要があります。従来製品開発のプロセスに、安全設計として実施すべき活動を定義し、それに従って実施することで、ヒューマンエラーを回避した安全設計が可能になります。

下図は、機能安全コンセプト開発の目的を達成するための活動の流れを示しています。前工程で、アイテム定義、ハザード分析/リスクアセスメント、安全目標の導出が実施され、そのアウトプットを入力として扱い、機能安全コンセプトを定義する各活動（灰色のボックス）を流れ（矢印）に沿って実施します。その中で、次工程で必要な機能安全コンセプト文書、安全妥当性確認の検証基準、検証レポートを成果物として作成し、レビューによって検証します。



機能安全コンセプト開発で最初に実施する活動は、安全状態の定義になります。前工程で導出された安全目標を達成することが機能安全の達成につながります。しかし、アイテムに生じる故障によって安全目標を達成できない場合は、安全状態に遷移させ、安全状態を維持する安全機構が必要になります。安全目標を導出する際に、誤作動系や不作動系のようにハザードを分類しておくことで、安全目標に一貫した安

全状態を考えることができます。例えば、衝突被害軽減ブレーキアイテムの場合、誤作動系ハザードに対する安全状態は、システムの正常が確認されるまで自動ブレーキ作動が禁止されている状態と定義できます。故障により意図しない自動ブレーキの作動発生の可能性があるため、自動ブレーキ作動が禁止されている状態をシステムの正常が確認できるまで維持することが重要です。

設計しようとする安全機構が、危険事象に至る前に、フォールトや故障、機能不全をコントロールし、安全状態に遷移するまでに与えられる時間（フォールトトレラント時間間隔:FTTI）を定義します。同一フォールトの発生でも、運用状況（例えば、低速走行、または高速走行）が異なれば、与えられるFTTIは異なります。アイテム定義活動で明確にされた開発対象システムの特性、性能、能力を考慮して FTTI を導出します。

次に安全構想設計の活動では、安全目標、または安全状態の達成、FTTI から、安全機構を設計進めていくにあたり、どのような思想で設計するかを最初に決めます。例えば、障害が発生した場合は安全を優先する思想で設計するフェールセーフ、障害を検出した場合は影響範囲を最小化しつつシステムを稼働し続ける思想で設計するフェールソフトなど複数の安全設計思想から、安全目標、または安全状態の内容に相応しい設計思想を選択します。

前述の衝突被害軽減ブレーキの安全状態例（誤作動系）は、自動ブレーキの誤作動が抑制されている状態が目標なので、フェールセーフ設計思想に基づいて、「自動ブレーキ誤作動発生の可能性がある故障は急減速に至る前に検出し、自動ブレーキ作動を禁止すること」が安全構想設計になります。

安全構想設計では、フォールトの検出、検出後のフォールトのコントロールが考慮されているので、これらの構想設計を機能安全要件として個々に定義します。

ここまで説明した各活動は、従来製品開発プロセスにおけるシステム要件定義プロセスに統合していくのが適切です。後続の活動（車両レベルのアーキテクチャ設計、機能安全要件のアーキテクチャ要素への割当て）に関する説明は割愛しますが、従来製品開発プロセスではシステムアーキテクチャ設計プロセスに統合するのが適切です。

開発現場の皆様が、ガイドブックで解説しているシステムエンジニアリング領域のプロセスアプローチと安全設計を理解し、機能安全製品の開発で実践できるようになるためのトレーニングを準備しています。弊社ホームページ、または次号以降のメルマガにて案内いたします。機能安全対応でお困りの際は、弊社コンサルティング事業部にお気軽に、ご相談下さい。

2021/1/25 小西 晃輔