安全の基本に立ち返って、安全な製品を開発する

前回のメルマガでは、新 ISO 26262 ガイドブックシリーズの出版時期をお知らせいたしました。2020年 10 月に出版される「ISO 26262 2nd 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」を具体的な例を用いて解説しています。

本メルマガでは、それらの中から安全アプローチおよび機能安全の概念に基づき許容できないリスクを識別し、リスク低減を行う「安全設計」のポイントについて例を用いて紹介いたします。

ISO 26262 では、電気/電子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。その目的が達成できていることを確証方策によって評価します。

開発現場は、どこまでやったら製品が安全であると言えるか、製品が安全であることをどのように説明するかの方針が明確でない中で機能安全対応に取り組んでいませんか。ISO 26262:2011 への対応では、確証方策は規格の要求事項を満たしていることが評価の観点であると受け取られています。

このことから、開発現場が機能安全アセスメントへの適合を機能安全達成の要件であると捉えて、規格対応に取り組んでいる状態が見られます。

その結果、表層的に規格要件の目的や意味を理解せず要件適合を行うため、その設計・技法・手法が安全な製品開発にどのような効果をもたらしているかが説明できない状態になります。

それは、製品の安全上のリスクを許容可能なレベルまで低減するという目的が、規格の要求事項に適合することに置き換わっているからです。これによって、本来達成すべき安全上のリスク低減がおろそかになる状況に陥ってしまいます。

安全な製品を開発するためには、規格の要求事項に盲目的に適合するのではなく、製品、組織、プロジェクトの特性を考慮し、起こり得る安全上のリスクを識別、評価し、リスク低減のために必要な活動を計画し、実施することが機能安全活動の基本です。安全上のリスクのうち、システムが稼働中に起こって欲しくない技術的なリスクを識別し、そのリスクを回避するための方策を設計し、故障の影響を正しく把握し方策の有効性を保証することが「安全設計」です。

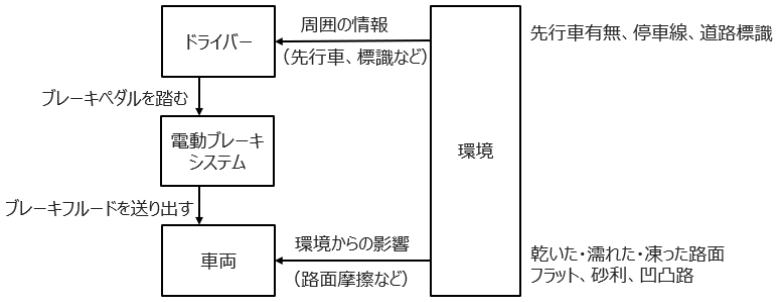
以下で、電動ブレーキシステムを例に、リスクアセスメントの結果に基づいて設定する安全目標を取り上げます。

下図に示すように電動ブレーキシステムの範囲、機能（ドライバーのブレーキペダル操作量に応じたブレーキ圧力を出力）、性能、他システムエレメントとの相互作用の有無などをアイテムとして定義します。

アイテムに対してハザード分析、シチュエーション分析、危険事象に対するリスクを評価し、ASIL を決定します。この分析に沿って、例えば、以下の電子ブレーキのリスク評価を得ることができます。

- ハザード：ブレーキが利かない（例えば、HAZOP でガイドワード No Entry：機能しない）
- シチュエーション：市街地を 50km/h で走行、晴天、前方の信号が赤信号、歩行者が横断している（路面状況、天候、周囲環境、走行状態を組み合わせて運用状況を分析）
- 危険事象：減速、停車しなければならない状況でブレーキが利かない

- 見積り：危害度 S3（重症・死亡）、遭遇確率 E4（頻繁にある）、制御可能性 C3（回避困難）
- 評価：ASIL D



リスクの評価結果から、シチュエーションにおいて回避すべき危険事象を考慮して安全目標を定義します。機能の誤作動で危険事象となる場合は、危険事象が起こり得るシチュエーションで機能の誤作動を回避することが安全目標として考えられます。また、機能の不作動で危険事象となる場合は、危険事象が起こり得るシチュエーションでの機能動作を保証することが安全目標として考えられます。

安全目標は最上位の安全要求となり、技術的な解決策の観点ではなく、機能上の目的の観点で定義します。前述の電動ブレーキのリスク評価例では、危険事象（機能の不作動）に対して、例えば、「車両走行中は、最低でも-2m/s^2 で減速可能なブレーキトルクが発生することを保証しなければならない」と定義することができます。

リスク低減活動で、安全目標を達成する安全方策を検討する上で、どのような状態が安全かも安全目標と合わせて定義します。誤作動系ハザードの場合は、機能が停止している状態、不作動系ハザードの場合は、ドライバーが不作動故障を認識し、残存リスクを制御可能とみなせる状態が安全な状態です。電動ブレーキシステムの例では、走行中にブレーキが利かなくなると危険です。「故障がドライバーによって認識され、車両を停車している状態」が安全状態と考えられます。

安全目標、安全状態を明確に定義できれば、安全の構想設計（止めれば安全なのか、継続しないと危険なのか、縮退でも大丈夫なのかなど）が明確に考えられるようになります。

機能安全コンセプト以降の安全設計のポイントについても、新ガイドブックにて前述の例を活用しながら、解説しています。

開発現場の皆様が、ガイドブックで解説している機能安全の重要な取り組みを理解し、製品開発で実践できるようになるためのトレーニングも準備しています。機能安全対応でお困りの際は、弊社にお気軽にご相談下さい。

2020/9/18 小西 晃輔