
セーフティコンセプトの体系的な構築

ISO 26262 で求められているセーフティコンセプトとはどのようなものでしょうか。

セーフティコンセプトとは、ひとことで言うと「安全な商品を作りこむため、開発の着手に先立ち、一連のシナリオを体系的にまとめたもの」というような位置づけになります。
安全の作りこみを行うためには、発生し得るハザードを把握し、リスクを評価した結果、リスク低減が必要なものについてはそれらを抑え込まなければなりません。

また、組織やプロジェクトの観点としては、人に依存する部分の考慮が必要となります。対象製品の開発にはどのような知識、スキルが求められるのか、必要な人材をどのように育成していくのか、個別のプロジェクトにおいてはどのようにスキル不足を補っていくのか、人のミスが混入する要因は何か、隠ぺいできない仕組みになっているかなど考慮しなければなりません。
このような、安全のつくりこみに対して、技術的側面、管理的側面から体系的にまとめておくことが求められます。

セーフティコンセプトには様々なものが含まれますが、代表的なものとしては、技術面ではセーフティメカニズムという技術的にどう安全を達成するかというもの、管理面では機能安全計画書という安全に関する計画、そして安全の達成を主張するための各種エビデンスとしてセーフティケースが求められます。その中でも機能安全としてもっとも重要なのがセーフティメカニズムです。
セーフティメカニズムの中には、個々のハザードに対する安全要件、達成すべきセーフティゴール、故障検出や障害低減の方法、安全状態への遷移方法などがまとめられます。
前回のメルマガでもご説明しておりましたが、これら一連のセーフティコンセプトおよびそれに付随する安全の根拠を示す各種エビデンス（セーフティケース）は、個々の担当者が勝手に構築すれば良いというものではなく、組織としてプロジェクトとして体系的に構築していかなければなりません。

それでは、どうすれば発生し得るハザードに対してリスク低減ができるのでしょうか。
それぞれのシステム、サブシステムがどのように使われるか、その際にどのようなハザードが発生し得るのか、そしてハザードを引き起こす要因は何か、その要因はどのようにして発生するのか、要因を回避する、またはその影響を低減するためにはどのような機能、性能が求められるか、どうすれば必要な機能、性能を実現できるのか、実現できたかどうかどうすれば判断できるのか、例えばこのようなことを考慮しなければならないわけです。

例えば、エンジンに関するハザードとしては、「意図しない急加速」として、運転手の意に反してエンジンが急に吹き上がって暴走してしまうということが考えられます。
その発生要因はいくつか考えられますが、電子制御スロットルの制御に着眼してみると、ECU における PWM の指示値の演算間違いや RAM 化けによって、スロットルセンサーの値がすべて正常であるにも関わらず、ドライブバイワイヤのモータ制御値が突然跳ね上がったために、瞬間的にエンジンの回転数が急上昇してしまったという事例も実際に報告されています。通常、スロットルは各種診断機能によって監視されており、モータに異常が発生したとしてもバネ力によって閉じる方向に動作しますが、ECU がモータを制御している以上、制御値の異常による暴

走の可能性は排除できません。このケースにおける危険状態、安全状態はそれぞれどのように定義されるのでしょうか。危険状態の一例は、「運転手がアクセルを踏んでいないのにスロットルが開く」ということであり、安全状態の一例は、「運転手がアクセルを踏んでいないときはスロットルが開かない」ということが考えられます。ただし、このケースにおいては実際には他にも危険状態、安全状態が存在します。
ISO 26262 では確定論的手法、確率論的手法によって安全性の証明が求められますが、上記の例では「運転手がアクセルを踏んでいないのにスロットルが開く」という事象を引き起こす要因の集合（最小カットセット）を導出し、その要因に対して適切に診断機能が機能することを確認する必要があります。最小カットセットの導出にはFTAのような帰納的分析手法が用いられることが多いですが、FMEAのような演繹的分析手法との組み合わせによって網羅性を確認することも重要です。

信頼性と安全性について、これらは同じような意味に聞こえるかもしれませんが、信頼性は正常機能を維持することを主な目的としているのに対し、一般的には安全性は人（環境、財産などを含む場合もある）への危害や物の破損や誤動作に対する危害発生の防止を目的としています。信頼性では部品故障率の低減や長寿命化が目標であり、安全性は危険要因の除去と回避や危険度低減、発生率の抑制が目標となります。
従って、信頼性向上と安全性向上の設計的な実現方法は異なります。

システムは多くのハードウェア部品やソフトウエアで構成されますが、構成部品はいつか壊れ、ソフトウエアには思わぬ欠陥が内在している可能性があります。こうした障害が表面化したとき、故障状態に陥ることになります。障害による機能失陥の観点から故障状態を分類すると、安全側故障と危険側故障に分かれます。部品等の障害の発生は機能不全を起こし、正常動作を果たせなくなって、多くの機器は停止することになります。このように機能停止することだけに留まり、危害を生ずるような異常な状態を招かない場合、この故障状態を安全側故障と呼びます。これとは異なり、障害が原因で新たな動きを生じて、思わぬ危害発生に及ぶ可能性を持っているものが危険側故障となります。安全性においては、危険側故障状態を発生させない事が最優先ですが、全てを安全側故障とすることは困難です。高信頼性は安全性確保の必要条件であることは間違いありませんが、危険状態を発生させる可能性を残しています。

一般に電子スロットル制御の事例では、スロットル開側は出力増大側であり、意図しないスロットル開は危険事象につながる可能性があります。また、スロットル閉側に対しても意図通りスロットル閉操作が出来ないことは危険事象につながります。以上のことを考慮すると、アクセル開側動作判断は操作入力信号の信頼性確保と出力アクチュエータ動作によるスロットル開度の監視と動作速度制限の付加が必要となります。スロットル閉側動作は電源喪失やアクチュエータロック不作動を想定するとバネ機械力による強制戻り力確保が必要不可欠となります。構造機構による安全確保は機械要素だけでなく、電気接点や回路電位は回路素子の構造構成で障害対応を図っています。このようにアクセルとスロットルバルブの間に電子制御を構成する電子スロットル制御システムでは、ソフトウエアでのエラー処理が主制御より安全上は重要になってきます。特に危険側故障に進展する恐れのある障害モードに対しては、十分なエラー処理が求められることから、機能不全に陥る障害把握の網羅性が問題となります。

従って、商品の安全性を主張するためには、開発開始時のハザード分析が重要となります。まず、潜在する危険事象を運転状況から洗い出します。自動車運転において、意図しない加速（または意図しない減速や停

止）、意図通り曲がれない（意図通り、まっすぐ走れない）、などのハザードをリスト化します。こうした状況の起因となる各種の故障を入力系、演算系、出力系等から抽出します。そして、危険回避操作の困難性や危険回避失敗時の危害の大きさや危険発生率について、運転状況を含め整理します。
従来行われている FMEA は、機能システムの構成部品毎、部品故障の状態毎についてリスクとしてボトムアップ的に整理したものです。FTA は機能システムとして最悪事象につながる要因をトップダウン的に分析析したものです。これらはいずれも重大危害の発生要因を客観的に抽出できる手法として、広く採用されています。ここから得られたリスクシナリオから、危害の発生除去、抑制や危害発生の大きさ低減策等に向けた安全目標の設定、及び、安全対策の具体化につなぐことが可能となるわけです。

こうしたハザード分析に際しては、安全確保の対称範囲の明確化と、商品としての使用や運用上の制約事項を確定することが必要になります。また、類似商品について、品質や誤使用等の市場を通したトラブル情報の蓄積も必要となります。これは、分析作業（故障状態、発生率、危害大きさ等）が単なる推定ではなく根拠ある情報に基づくものになることから、組織開発プロセスに沿ったものとなります。

以上のように安全性実現の開発は、セーフティコンセプトとして、対象とする商品の危険性を把握した上で、許容できるリスク水準を明確化することにあります。こうしてまとめられた安全目標に対して、開発に携わる担当者はリスク低減の技術的な具体化展開が可能であり、商品の安全性確保についての明確な説明につながることになります。
(2011 年 09 月号、10 月号 メルマガ抜粋)

ビジネスキューブ・アンド・パートナーズ株式会社
東京都渋谷区広尾 1-13-1 フジキカイ広尾ビル 5F
TEL：03-5791-2121 / FAX：03-5791-2122 / E-mail：consulting@biz3.co.jp
URL：http://biz3.co.jp