ソフトウェア組込み型デバイス製品のための機能安全活動の実践とその成果

パナソニック株式会社デバイス社　技術本部　機能安全・DR 推進グループ　チームリーダ
安倍　秀二

自動車用の機能安全規格であるISO 26262の発行に伴って実現した機能安全プロセス構築とその実践結果について報告する。規格の要求内容を従来の開発活動に出来るだけ対応付けて割り当てることで作業の追加を避け、従来実施してきた活動の延長として機能安全活動が実施出来るようにした。ここでは、その活動内容とそこから得られた成果等について報告する。

1 機能安全規格　ISO 26262 について

ISO 26262 は、2011 年 11 月に発行された自動車用の機能安全規格である（図 1）。電気、電子、ソフトウェアから構成された安全関連システムにおける、機能不全の振る舞いによって引き起こされる可能性がある潜在的なハザードを取り扱っている。そのハザードにより、安全関連システムが不安全にならないことの説明責任を果たすための論証を確立することが求められている。ある運転状況でのハザードの潜在リスクを ASIL※1 を用いて 4 段階（A ～ D）にレベル付けし、規格の要求事項を実践することにより、許容されるリスクまで低減する。このレベル付けでは、ASIL D の方がより安全を求められる。

機能安全規格では安全関連システムが不安全に至る原因を、システマティック故障とランダムハードウェア故障と定義している。前者は主にソフトウェア、ハードウェアの設計ミスであり、安全ライフサイクルで実施される活動内容の詳細な定義と信頼のある設計原則などによって引き起こさないようにすることが求められている。後者はハードウェア部品の確率的な故障によって引き起されるものであり、製品の各機能に対して設置した安全機構により、故障を検出して安全状態に移行させ、故障をドライバーに通知することが求められている。前述したように ISO 26262 は、自動車を構成している機器が不安全な振る舞いを引き起こさないよう、安全文化を基本にして、安全マネジメント、ソフトウェア・ハードウェアの設計手法、テスト技法、ハードウェアの定量分析活動などの詳細な要求事項を含んでいる。

Part1	用語集
Part2	機能安全の管理
Part3	コンセプトフェーズ
Part4	システムレベルにおける製品開発
Part5	ハードウェアレベルにおける製品開発
Part6	ソフトウェアレベルにおける製品開発
Part7	生産及び運用
Part8	支援プロセス
Part9	ASIL 指向及び安全指向の分析
Part10	ISO 26262：ガイドライン

図1　ISO 26262の概要

2 機能安全規格への対応と取り組みについて

パナソニック株式会社デバイス社（以下当部門）は、パナソニックグループの中で汎用電子、半導体、自動車用などのデバイス開発、製造、販売を担当している。当部門の開発する自動車用デバイス部品の多くにソフトウェアが搭載されており、自動車の ECU※2 などに組み込まれている。

2.1　機能安全プロセス

当部門は、2002 年からパナソニック全社で展開されたソフトウェアプロセス改善活動の一貫として、CMM※3 や CMMI※4、Automotive SPICE※5 を参照し、ソフトウェア開発プロセスの改善を実践してきた。その結果、2008 年には CMMI レベル 3 を達成した。今回報告する機能安全規格に対応したプロセス（以下、機能安全プロセス）は、そのソフトウェア開発プロセスがベースになっている。また、ISO 26262 はソフトウェアの開発だけではなく、システム、ハードウェアも含めた製品の開発プロセス定義を要求している。また、当部門は、自動車用以外

のデバイス開発も行っており、すべての製品が機能安全に対応しているわけではない。そのため、機能安全対応の車載開発、一般の車載開発、一般の開発のすべてに対応出来るように、図2に示すような4層のプロセス構造を取っている。これは、すべての開発の元となる“品質マニュアル”及びソフトウェア搭載デバイス開発の開発イベントを規程した“システム製品開発管理規程”である。この規程は、ISO 26262の要求事項である安全ライフサイクルを内装している。

機能安全プロセスはこの規程を参照して構築され、“基準”と“機能安全ガイドライン”から構成される（図3）。基準は、開発活動、入出力成果物、支援活動を定義したENG系、支援系の20種のプロセスからなる。また、機能安全ガイドライン（14種）はASILが設定された場合に、各プロセスから参照される。図3の各基準、各機能安全ガイドラインの名称に含まれるアルファベットは略式表記を示している。高信頼の製品開発には、厳格なプロセス定義だけでは達成が不十分であり、過去の失敗事例も含む設計ノウハウ、そしてエンジニアが設計ノウハウを確実に設計に織り込んでいることを確認する

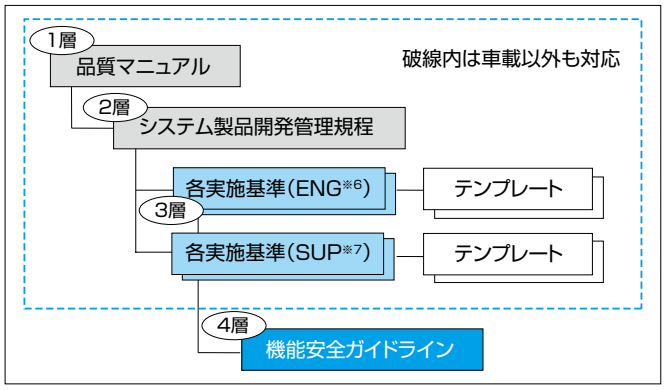

図2　開発に関する4種のプロセス構造（文書構造）

脚注

※1　ASIL：Automotive Safety Integrity Level，自動車安全度レベル
※2　ECU：Electrical Control Unit，電子制御ユニット
※3　CMM：Capability Maturity Model，能力成熟度モデル
※4　CMMI：Capability Maturity Model Integration，能力成熟度モデル統合，CMMIは米国での登録商標
※5　Automotive SPICE：Automotive Software Process Improvement and Capability Etermination
※6　ENG：engineering，エンジニアリング
※7　SUP：support，サポート

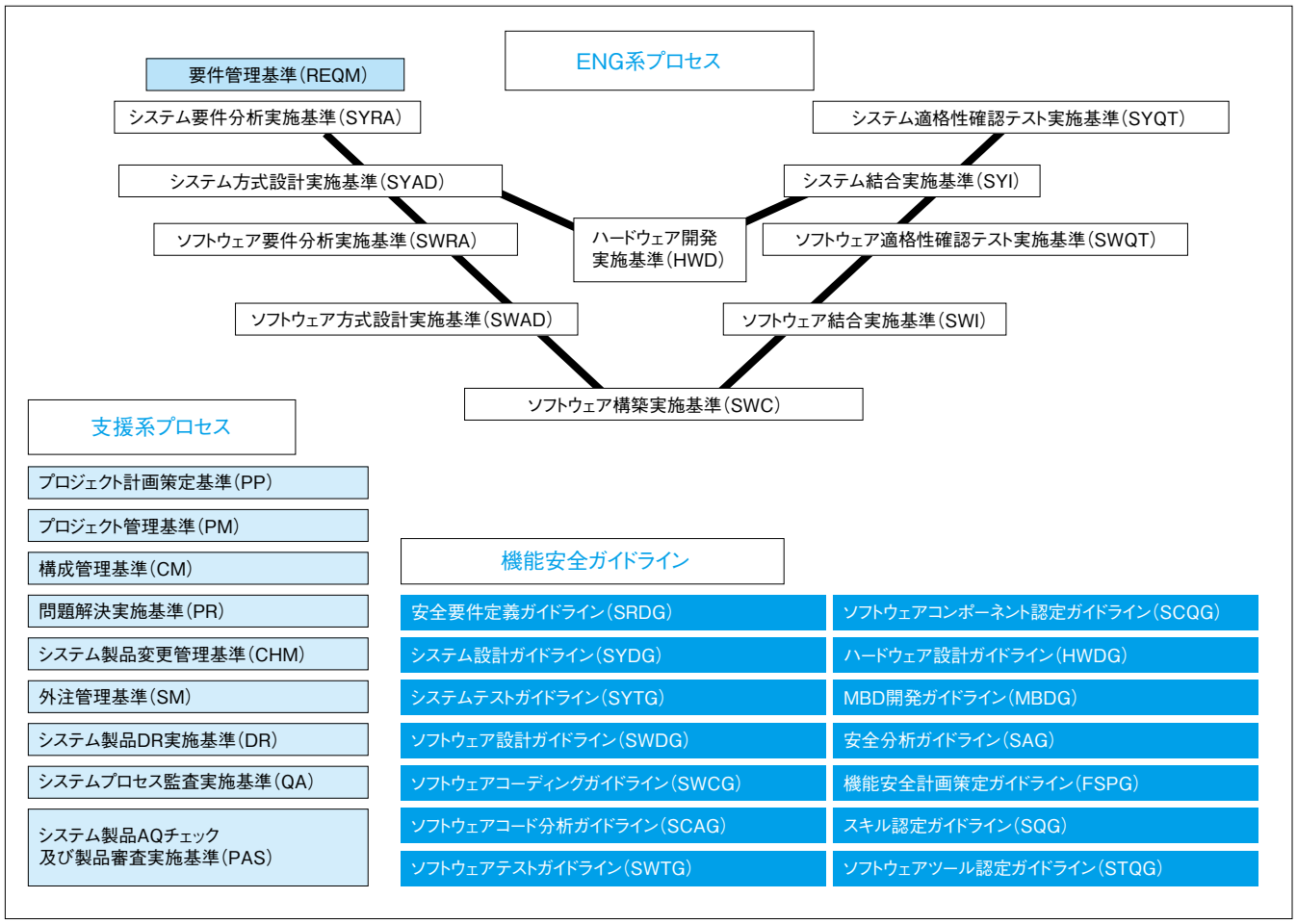

図3　機能安全プロセス体系

チェックリストも含む必要がある。機能安全ガイドラインには、より良い設計技法やテスト方法の解説など、ISO 26262 の規格要求事項への対応だけではなく、エンジニアリングの知識も多数含まれ、また、開発者のスキル認定のしくみも含んでいる。

2.2 プロセスアプローチの導入

一般的に自動車用の部品は、要求や技術の実現可能性検討のために、開発の上流時点で試作をすることが多い。また、モデルを作成し、シミュレーションで確認することもある。多くの部品が車内ネットワーク機能を持っているため、相互の接続検証を行うこともある。そのため、開発期間中に複数のサンプル出荷を行う。このような開発の状況では、“ウォーターフォール”型のライフサイクルを適用した開発手法は使用することが困難なため、それぞれのサンプル出荷の開発目標や品質目標に合わせた、柔軟な開発が必要となる。これに対応するため、機能安全プロセスは“反復”型での計画作成を可能にしている。本プロセスはプロセスアプローチ※8を基本にしており、プロセスには、その入力成果物、出力成果物、開始基準、終了基準と共に、作業手順が定義されている。反復計画の単位は“ステージ”と呼ばれ、必要な複数のプロセスを、入出力成果物を考慮して組み合わせ、1～数週間の計画を作成し、そのステージで実施する作業の到達目標とその品質目標を設定する（図4）。

例えば、機能安全活動の中で重要な技術安全コンセプトの検討は、“システム要件分析実施基準（SYRA）”と“システムアーキテクチャ設計実施基準（SYAD）”を組み合わせ、安全目標の侵害に至る故障モードの分析のためにFTA分析を実施して要求を仕様化し、システムに“意図した機能”と“安全機構”を割り当てる。また、上流でサンプルを出荷する場合は、“ソフトウェアアーキテクチャ設計実施基準（SWAD）”、“ソフトウェア構築実施基準（SWC）”を組み合わせ、品質目標に沿った適切な品質レベルのサンプルを作り上げる。開発の中流では、“ソフトウェアアーキテクチャ設計実施基準（SWAD）”、“ソフトウェア構築実施基準（SWC）”及び“ソフトウェア結合実施基準（SWI）”を組み合わせ、ソフトウェアコンポーネントをしっかり作り込む。“ステージ”は機能単位や担当者ごとに設定することが出来る。それぞれのプロセスの終了基準は、レビューを実施して検出された欠陥を解消することとなっており、上流でしっかり品質を作り込む必要がある。開発の下流では、“システム結合実施基準（SYI）”及び“システム適格性確認テスト実施基準（SYQT）”を組み合わせ、システムのテストを実施し、しっかりと仕様や設計を確認する。下流で仕様変更がある場合には、設計、テストのプロセスを組み合わせた“ステージ”で対応する。このようにプロセスアプローチは、工程といった時間軸に関係なく、開発や品質目標に合わせた適切なプロセスの組み合わせ

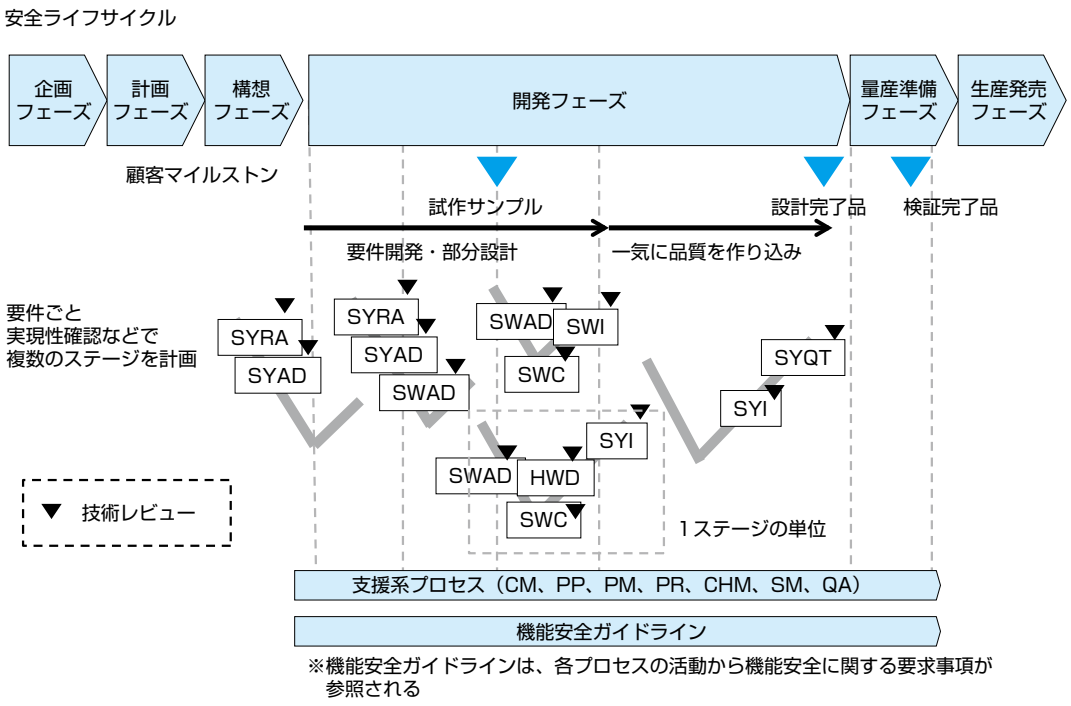

図4　反復計画とステージの例

でいつでも柔軟に対応が出来る。

2.3　安全ケース

安全ケースとは、システムが安全であるということを第三者へ客観的に説明するための作業成果物群である。これは以下のような事柄について、客観的に示すことが出来るものでなければならない。

・システマティック故障を起こさないような設計・検証の実施とその結果。
・ランダムハードウェア故障については、安全目標の侵害に至るハードウェア部品の故障の故障モードの分析を行う。このとき、分析の結果により、それぞれの故障モードに安全機構を設置し、部品の故障を検出し、処置し、通知出来るようになっているか。

安全ケースは、“安全ケース”という成果物を改めて作成するのではなく、各プロセスの出力成果物から構成し、逐次開発の上流から作業成果物を作成するようにしている（図5）。これは安全目標から安全分析により導かれる機能安全コンセプト、及び技術安全コンセプトに基づく各設計書やそれらの検証結果であるレビュー記録やテスト仕様、結果などから構成されている。2.2で述べたプロセスアプローチを使うと、プロセス実施の結果として安全ケースを構成する作業成果物が作成されるので、上流の成果物から一貫した内容にすることが出来る。それらはトレーサビリティツールにより双方向のひも付けを行うことが可能であり、それにより安全要求がもれなく実装され、検証されていることを一覧で示すことが出来る。

2.4　製品の開発ステップと確証方策の組込み

ISO 26262では、システムが安全であることを確認するために“確証レビュー”、“機能安全監査”、“機能安全アセスメント”からなる“確証方策”の実施が必要となっており、それらの内容を表1に示す。

また、確証方策を実施する人員や組織については、“開発人員とは異なる人物によって実施”、“開発人員とは異なるチームによって実施”、“開発人員とは異なる組織の人物によって実施”という実施者の独立性についての要求事項もある。これらの適用については、成果物及びASILによって異なる。

確証方策については追加の活動とせずに、製品開発で既に実施しているイベントや活動に割り当てる方針とし

脚注

※8　プロセスアプローチ：プロセスアプローチとは、“ISO 9001：2008の序文　0.2プロセスアプローチ”に定義されているように、望まれる成果を生み出すために、プロセスを明確にし、その相互関係を把握し、マネジメントと併せて、一連のプロセスをシステムとして適用することである。

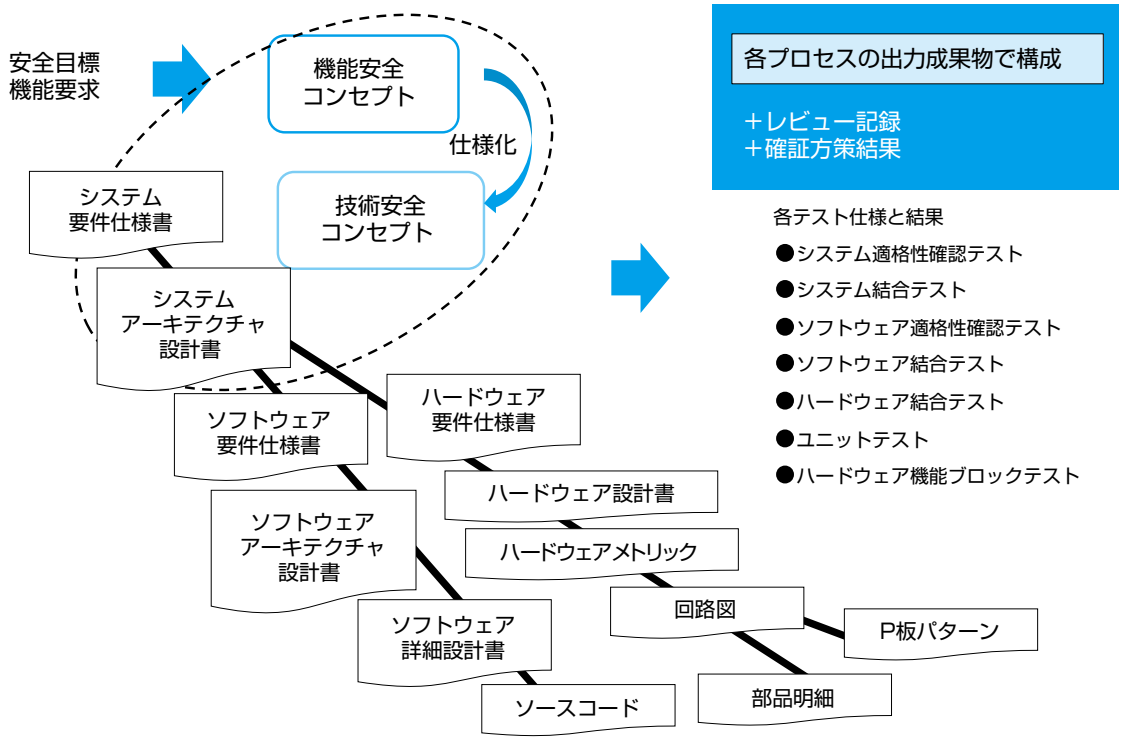

図5　安全ケースとプロセス成果物

表1　確証方策の種類とその内容

確証方策	実施内容	確認成果物
確証レビュー	ISO 26262 の要求内容に対する準拠性	安全ケースを構成する各作業成果物
機能安全監査	組織で定義されたプロジェクトが実施すべき機能安全プロセスに対する準拠性	プロジェクトの作成する作業成果物やプロセスの実施を示す安全計画など
機能安全アセスメント	システムが安全であるかの確認	確証レビューや機能安全監査の結果及びシステムそのもの

（参考：ISO 26262:2011, Part2）

た（図 6）。すなわち以下の方針である。

- 製品の開発フローで実施を計画している品質イベントや DR イベントに割り当てる。
- 確証レビューについては、マイルストンごとの DR イベントで実施する成果物の第三者レビューと同時に、規格の要求事項を正しく実装しているかの視点でもレビューをする。併せて、安全メカニズムの適切性や有効性の確認のため、レビューやテストの実施内容の確からしさも確認する。
- 実施は当部門の機能安全規格に精通しているレビュアーが担当する。独立性については、“開発人員とは異なる組織の人物によって実施”を確保する。
- 機能安全監査は、従来からのプロセス監査と同じであるので、当部門の各事業担当部門の品質部門に所属する SQA※9 担当者により実施する。従来のソフトウェアだけではなくシステムやハードウェアの活動も確認する。
- 機能安全プロセスの要求事項や作成する作業成果物、実施の観点をまとめたチェックリストを作成し、SQA 担当者はそれに沿って実施する。
- 機能安全アセスメントは、生産移行前に実施する製品審査活動に割り当てる。機能安全開発における製品の審査として、製品品質視点と安全視点で評価する。ただし、機能安全アセスメントでは次の内容も確認が必要となる。
  - 安全計画によって要求される作業成果物
  - 機能安全のために要求されるプロセス
  - システムの開発中に実装した安全方策の適切性及び有効性レビュー

機能安全アセスメントを生産移行前に実施すると、手戻りも予想されるので、開発の上流から漸次実施することが望ましい。前述したように、DR に連動した確証レビューの実施時に安全機構の適切性や有効性の確認を実施し、システムが安全であるかどうかを確認するようにしている。機能安全アセスメントでは、確証レビューや機能安全監査の結果についての内容や一貫性を確認することで、一定の目的が達成される。ロバスト性などの観点でのシステムの妥当性確認については、従来より審査活動として実施している。これらの結果を踏まえてシステムの安全を確認し、生産への移行を承認する。

2.5　専門組織の設置とトレーニング提供

当部門では機能安全を取り扱う専門組織として、“機能安全・DR 推進グループ”（以下、当グループ）を設置した。当グループの主な責務は、機能安全プロセスの構築・維持管理やトレーニングプログラム（規格を教える“機能安全製品開発コース”と機能安全プロセスを教える“システム製品開発コース”）の提供と実施、機能安全開発のコンサルティング及び確証レビューの実施である。機能安全プロセスの構築については上記で述べてきた通りである。トレーニングは 2012 年 4 月から実施し、延べ 400 人が受講した。また、トレーニングで取得した“知識”を使える“スキル”にするために OJT によるコンサルティングを実施し、機能安全開発が出来るエンジニアを育成している。

3　機能安全活動の実践とその結果

2011 年は機能安全プロセスの構築を実施してきたが、何よりも困難であったのは、規格要求の解釈である。現場では、規格の実施の相場観が確立しておらず、何をどの深さまで実施すべきかを迷ったこともあった。解釈については、パナソニック全社の機能安全関連活動に携わるメンバーと議論を繰り返し行い、共に納得することで、有効な成果を得ることが出来た。実活動のコンサルティングでは、まさに手探りの活動ではあったが、機能安全の活動の形がおおよそ見えてきた。主な活動は下記の通りである。

- 安全分析と技術安全コンセプト形成
- 故障率の計算と各指標の算出
- 安全プロセスの実施
- 確証方策の実施
- ソフトウェアツールの適格性確認　など

また、機能安全活動の実施を通じた成果と活動に関する感想を、次に列挙する。

- ソフトウェア技術者は、CMMI、Automotive SPICE を参照して作成したプロセスに沿って仕事を進めるこ

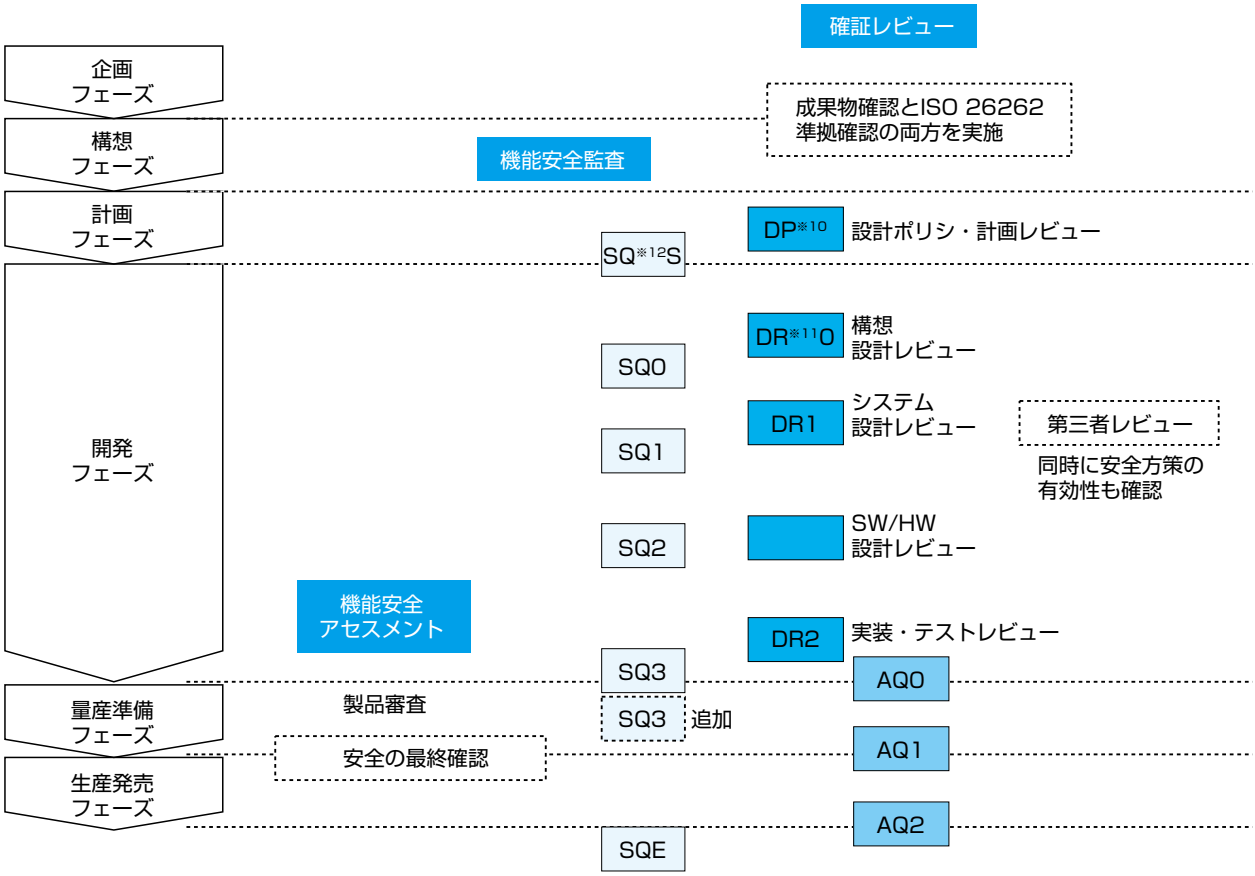

図6　安全を確保するための確証方策の実施タイミング

とにある程度慣れていたので、作業をスムーズに実施出来た。

- ハードウェア技術者の安全分析や安全方策については、フェールセーフ開発にて設計・実装されている。設計書や設計根拠は明示されているものの、多くの文書がエンジニアの視点で具体的に記載されており、それを第三者である非エンジニアへ客観的かつ抽象的に説明することが難しかった。
- システムについては派生開発も多く、物理的に安全関連・非安全関連の部分が混在して実装されている。それらの説明を抽象的に受けたために、論理的に分離することに苦労した。エンジニアは安全方策の実装を当たり前のように意識しているため、コンサルティング時のインタビューで情報や意図を引き出し、“意図した機能”と“安全機構”を分離して説明出来るようにした。それによって、安全分析結果を関連付けた技術安全コンセプトを形成出来た。
- 故障率データベース（IEC 62380 など）を用いた故障率計算やハードウェアアーキテクチャ指標の算出については、テンプレートを作成することで、実施内容の平準化が出来た。

4　おわりに

これまで構築してきた機能安全プロセスを活用し、実開発を通じて、徐々に機能安全活動の形が出来つつある。トレーニングについては、コンサルティング活動で得た機能安全の実開発のノウハウをもとに、“規格を教える”から“現場で使えるスキルを身に付けることが出来る”へと内容を改善する予定である。また、専門組織メンバーも現場と共に学び、その実施結果を元にして機能安全対応プロセスを改善していく。これらの活動によって獲得したノウハウについては広く全社に展開し、機能安全開発活動の高位平準化を目指していきたい。

脚注

※9　SQA：System Quality Assurance，システム品質保証
※10　DP：Design Policy，設計ポリシ
※11　DR：Design Review，設計レビュー
※12　SQ：System Quality Audit，システム品質プロセス監査